White Paper

Підміна чи глушіння?

Розвінчання міфів про завади та послаблення GNSS

Якщо ваша професійна діяльність вимагає точного знання того, де ви перебуваєте і куди рухаєтесь, ви без сумніву покладаєтесь на глобальні навігаційні супутникові системи (GNSS) для точного визначення положення, навігації та часу (PNT – positioning, navigation and timing). GNSS — це сукупність супутникових навігаційних систем або сузір'їв різних країн і регіонів (рисунок 1). Радіочастотні сигнали GNSS використовуються для PNT у багатьох галузях промисловості та військових сферах — від наземних до авіаційних і морських застосувань — багато з яких вимагають високої точності, надійності та доступності.

Критичним викликом для тих, хто покладається на гарантовані PNT (APNT), є загрози сигналам GNSS, особливо в середовищах із забороненим, порушеним, переривчастим або обмеженим доступом GNSS (D/DIL). До них належать театри воєнних дій та прибережні морські регіони з перевантаженими RF-зонами через прибережну та берегову діяльність — такі як Чорне та Середземне моря, узбережжя яких охоплюють країни з високою комерційною та промисловою активністю, а також військовою нестабільністю. Регіони зі стратегічним положенням, як наприклад Скандинавія, також часто зазнають загроз GNSS з боку протиборних режимів.

Будь-яке порушення передачі сигналів GNSS може призвести до часткової або повної втрати PNT, тобто ви фактично здійснюєте навігацію (керуєте автомобілем, літаком або судном) «наосліп». Завади сигналам GNSS можуть бути ненавмисними або навмисними (див. вставку). Існує багато задокументованих випадків ненавмисних завад — від несправних телевізійних приймачів до інших не-GNSS джерел випромінювання, що «просочуються» у частотні діапазони GNSS. Якщо завадний сигнал навмисно передається в частотному діапазоні GNSS, це називається глушінням (jamming).

Ще однією загрозою GNSS-позиціонуванню є спуфінг (spoofing), який означає навмисну передачу фальшивих GNSS-сигналів до приймача, внаслідок чого він обчислює хибне положення, змушуючи користувача вважати, що він перебуває в іншому місці або в інший час, ніж насправді. Такий тип завад викликає особливе занепокоєння у критично важливих для безпеки застосуваннях у всіх галузях — як цивільних, так і військових — які покладаються на точні GNSS-орієнтовані PNT.

Чому сигнали GNSS схильні до глушіння та спуфінгу?

Радіочастотний (RF) спектр поділений на визначені сфери використання, тому смуги сигналів GNSS є фіксованими та мають відомі частоти (рисунок 1), що робить їх уразливими до глушників і спуферів, які випромінюють сигнали в тому ж частотному діапазоні.

Ситуація ускладнюється тим, що до моменту, коли сигнали GNSS проходять 20 000–25 000 км від супутників середньої навколоземної орбіти (MEO) до приймача на поверхні Землі, вони мають дуже низький рівень потужності (−130 dBm або 10^{-13} мВт) — у 600 квадрильйонів разів (це 15 нулів) слабші за лампу розжарювання потужністю 60 Вт!

Цей низький рівень потужності робить сигнали GNSS уразливими до завад від потужніших сигналів, переданих у тому ж частотному діапазоні. Саме тому потужні завади можуть перевантажити GNSS-приймач, і саме тому слід розглядати захист та підсилення сигналів.

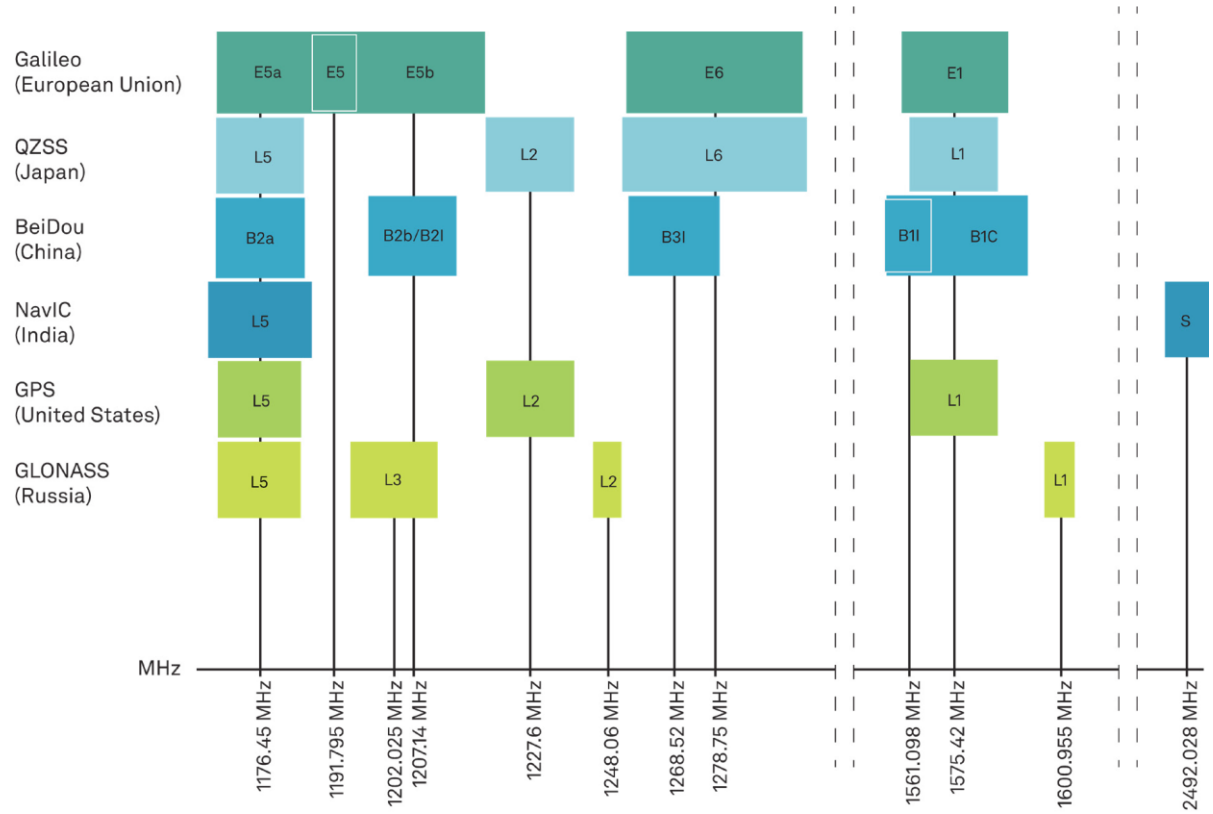


Рисунок 1. Сузір'я та сигнали ГНСС.

Яка різниця між глушінням і спуфінгом?

Основною відмінністю між глушінням і спуфінгом з точки зору користувача є вплив, який вони мають на здатність приймача надавати PNT. Глушіння проявляється як втрата інформації PNT, оскільки сигнал GNSS пригнічується завадним сигналом. Спуфінг, з іншого боку, вводить приймач в оману, змушуючи його повідомляти неправильну інформацію PNT.

Аналогією для порівняння різниці між глушінням і спуфінгом є грабіжник, який перерізає відеосигнал камери спостереження, унаслідок чого охоронець бачить сірі перешкоди на екрані монітора (глушіння), порівняно з грабіжником, який замінює відеопотік записом, що показує той самий вигляд з іншого часу, змушуючи охоронця вважати, що все гаразд (спуфінг). Саме тому, з точки зору користувача GNSS, спуфінг є більшою загрозою. На відміну від глушіння, ви можете навіть не знати, що вас спуфлять.

Глушіння здійснюється шляхом перевантаження GNSS-приймача радіочастотними сигналами вищої потужності. Хоча в більшості юрисдикцій це є незаконним, дуже малопотужні глушники, відомі як «пристрої персональної конфіденційності», можна придбати в Інтернеті та використовувати з цією метою. Навіть простий малопотужний глушник може пригнічувати сигнали GNSS на великій території, позбавляючи PNT.

Ефективність глушників головним чином залежить від їх вихідної потужності та дальності дії (відстані до цільового приймача). Малопотужний глушник поблизу може мати такий самий ефект, як і потужний глушник, що передає сигнал з більшої відстані. Інші характеристики глушників включають те, чи націлені вони на вузькосмугові або широкосмугові частоти, а також чи передаються вони як безперервна хвиля (на вибраній частоті або з розгорткою по спектру) чи імпульсно з певною частотою на нижчому рівні потужності – чирпінг (chirping). На рисунку 2 наведені приклади кількох типів завадних сигналів.

Переклад українською – ТОВ «Є.П.С.»

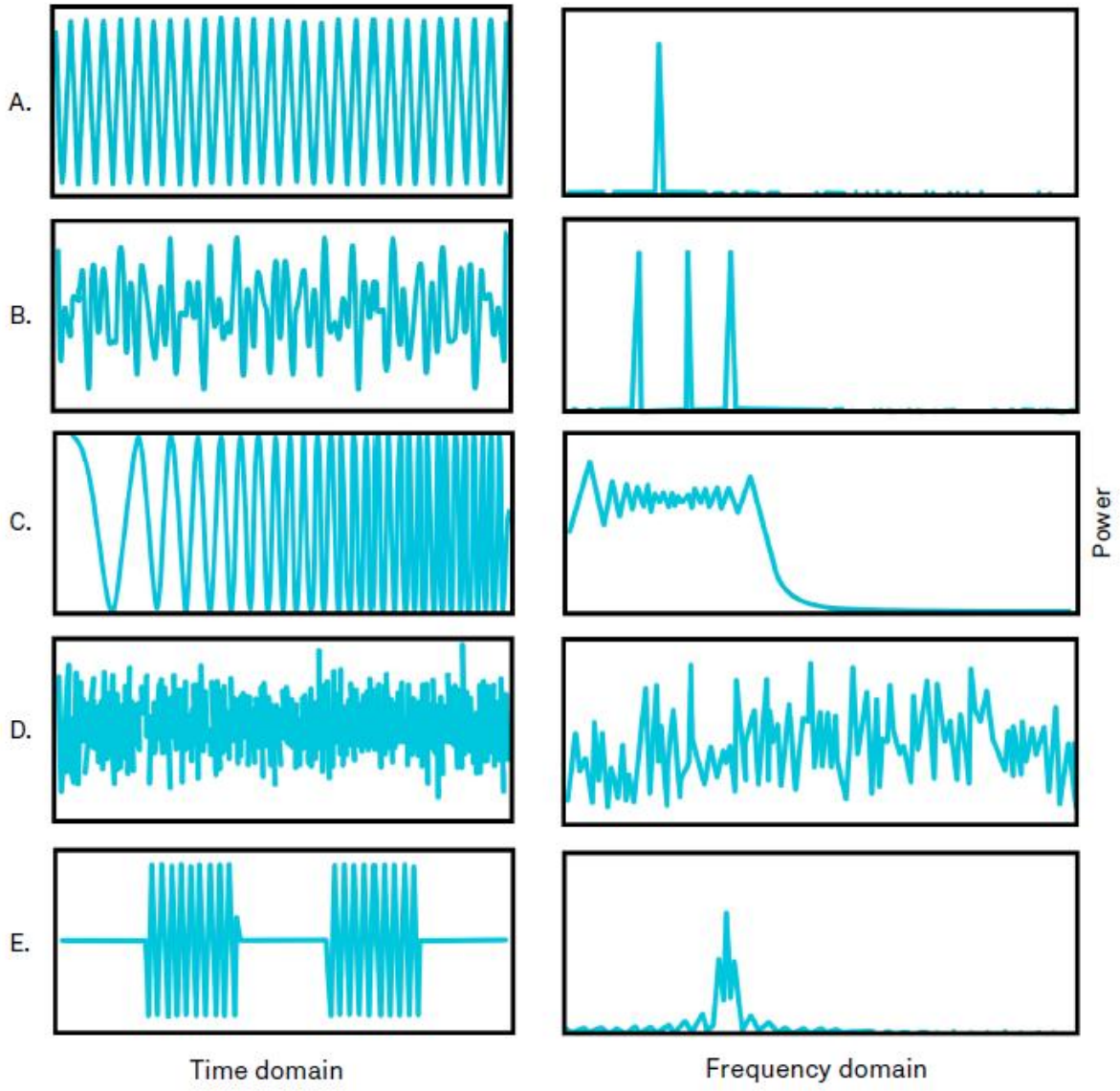


Рисунок 2. Типи перешкод. A. Вузькосмугові безперервні хвилі. B. Багатотональні безперервні хвилі. C. Чирпінг. D. Широкосмугові. E. Імпульсні. (Jahromi et al., 2015)

Які існують типи спуфінгу?

Незалежно від джерела спуфінг-атак, їх можна класифікувати як **неперекриті**, **перекриті**, а також за **відносною потужністю** порівняно з автентичними сигналами GNSS. На рисунку 3 зображено чотири типи спуфінг-атак.

Неперекриті спуфінг-атаки — це атаки, за яких кодова фаза та фаза несучої (затримка та доплерівська частота) спуфінг-сигналів не синхронізовані з автентичними GNSS-сигналами.

Перекриті спуфінг-атаки є більш складними, оскільки кодова фаза та доплерівська частота спуфінг-сигналів синхронізовані з автентичними GNSS-сигналами. Такий тип атаки вимагає, щоб спуфер знав поточний час, видимі супутники, місцезнаходження та параметри цільового приймача.

Стаття **«Nobody's Fool: Spoofing Detection in a High-Precision Receiver»** з випуску *Inside GNSS* за липень/серпень 2020 року надає детальніший огляд методів виявлення різних типів спуфінг-атак.

Спуфінг часто є **двоетапним процесом**, який вимагає використання глушника для початкового порушення відстеження автентичних GNSS-сигналів приймачем, а потім використання радіопередавача для передачі фальшивих сигналів до цільового приймача. Фальшиві сигнали можуть бути створені або за допомогою генератора сигналів, або шляхом повторної трансляції записаних GNSS-сигналів, що називається **меконінгом (meaconing)**. Якщо приймач ще не почав відстежувати автентичні GNSS-сигнали (наприклад, під час запуску), для захоплення приймача потрібен лише другий етап.

Простим прикладом спуфінгу є використання недорогого програмно-визначуваного радіо (SDR), щоб змусити смартфон «думати», що він перебуває надворі в парку та ловить персонажів Покемон, хоча насправді він усе ще знаходиться в будинку. Концептуально серйозніші спуфінг-атаки з використанням складних симуляторів GNSS-сигналів є такими ж самими, але наслідки можуть бути катастрофічними — наприклад, літак може здійснити посадку не там, де потрібно, або судно може зайти у ворожі води.

Спуфінг-атаки також можна класифікувати за їх відносною потужністю порівняно з автентичними GNSS-сигналами, а також за тим, чи синхронізовані фальшиві сигнали з різними аспектами автентичних GNSS-сигналів чи ні (див. вставку). Якщо ціль рухається, спуферу також необхідно знати її швидкість і курс, щоб коригувати рівень переданого спуфінг-сигналу (та доплерівський зсув) для введення цільового приймача в оману.

З цього вступу легко зрозуміти, чому захист від глушіння та спуфінгу став критично важливим компонентом GNSS-обладнання. Далі ми розглянемо, що можна зробити, щоб запобігти глушінню або спуфінгу — або обом завадам одночасно.

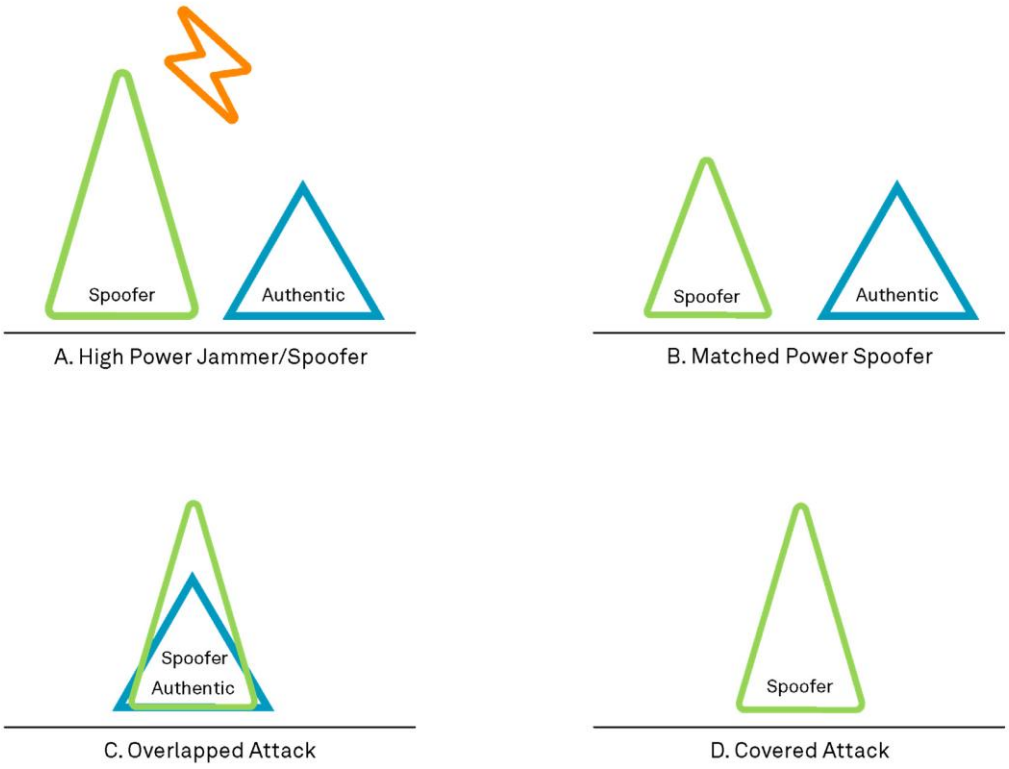


Рисунок 3. Типи спуфінг-атак. A. Jam/Spoof: глушильний сигнал високої потужності, за яким слідує спуфінг-сигнал. B. Matched power: потужність спуфінг-сигналу узгоджена з автентичним сигналом. C. Overlapped: кореляційні функції автентичних і спуфінг-сигналів перекриваються. D. Covered: спуфер маскує прийом автентичних сигналів. (Broumandan et al., 2020)

Як здійснюється протидія глушінню та спуфінгу?

Першою лінією оборони від завад у будь-якому GNSS-рішенні позиціонування є **виявлення та відхилення або пригнічення** якомога більшої кількості завад до того, як вони вплинуть на PNT. На базовому рівні GNSS-рішення включає супутникові сигнали, антену та приймач. Стратегії протидії глушінню та спуфінгу були розроблені на кожному з цих трьох рівнів, як описано нижче. Усі ці компоненти працюють разом, створюючи сумарний ефект проти завад. У сукупності вони забезпечують користувачеві впевненість у захищеності його PNT і можливість безпечно виконувати свої операції.

Захист на рівні сигналу

Для військових застосувань існують зашифровані коди GNSS-сигналів для протидії глушінню та спуфінгу. Наприклад, **GPS P(Y)-код** є зашифрованим двійковим кодом із одиниць і нулів, що передається на частотах L1 і L2. P(Y)-код змінюється 10,23 мільйона разів на секунду та складається з унікальної послідовності з 6,18 трильйона одиниць і нулів для кожного супутника, яка оновлюється щотижня. P(Y)-код вимагає використання приймача з модулем **Selective Availability Anti-Spoofing Module (SAASM)** з дійсним ключем дешифрування (експортно контрольований виріб у багатьох країнах, зокрема в Канаді та Сполучених Штатах).

M-Code — це ще один військовий GPS-сигнал L1/L2, розроблений для подальшого підвищення стійкості до глушіння. M-Code спроєктований як автономний, тобто користувачі можуть обчислювати свої координати, використовуючи лише сигнал M-Code. На відміну від цього, для використання P(Y)-коду приймачі зазвичай спочатку повинні зафіксувати публічний C/A-код, а потім перейти до фіксації P(Y)-коду. Сигнал M-Code розміщує більшу частину своєї енергії на краях спектра, подалі від існуючих носіїв P(Y) та C/A. Крім того, M-Code передаватиметься з антен з більшим коефіцієнтом підсилення, що збільшує потужність сигналу та робить його менш уразливим до пригнічення глушником. **На рисунку 4** показано коди сигналів GPS.

Другим методом захисту на рівні сигналу є **автентифікація**, яка передбачає використання криптографічних методів для захисту GNSS-сигналів від використання неавторизованими користувачами або маніпуляцій з боку підроблених передавачів. Це включає нещодавно розроблену **Galileo E1-B Open Service Navigation Message Authentication (OSNMA)**, а також майбутній сигнал **GPS L1C Chimera (Chips Message Robust Authentication)**.

Захист на рівні антени

Високоякісні GNSS-антени забезпечують ще один рівень захисту від завад, оскільки вони підвищують рівень прийнятого сигналу в частотному діапазоні GNSS, одночасно відхиляючи сигнали поза діапазоном. Деякі GNSS «anti-jam» антени зменшують підсилення сигналів з малими кутами піднесення, щоб зменшити вплив глушників, які знаходяться поблизу горизонту; однак такий підхід також блокує легітимні супутники з малими кутами піднесення. Захист, який забезпечують ці антени, є обмеженим, оскільки вони все ще можуть бути нейтралізовані, якщо глушник зміститься з горизонту або якщо присутні кілька глушників.

Адаптивні антенні решітки, такі як **Controlled Reception Pattern Antennas (CRPA)**, та пов’язана з ними антиглушильна електроніка забезпечують вищий рівень захисту шляхом безперервного керування кількістю сигналу, що приймається з будь-якого напрямку. Використовуючи кілька окремих антенних елементів, електроніка CRPA адаптивно змінює уявне підсилення антенних решіток, створюючи зони зниженого підсилення («нулі») у напрямку джерела завад (**формування нулів**).

Система CRPA може формувати нулі в *n-1* напрямках, де *n* — кількість елементів. Таким чином, система з 7 елементів може формувати нулі в 6 напрямках тощо. Однак усе не так

просто, і інші фактори, такі як геометрія CRPA та використовуваний алгоритм обробки сигналів (див. вставку), можуть мати суттєвий вплив. Для передових застосувань, таких як військова авіація, із залученням додаткових датчиків для визначення розташування супутників GNSS, положення та курсу платформи, система також може спрямовувати максимальне підсилення у бік легітимних GNSS-сигналів (**керування променем, beam steering**).

Деякі системи CRPA додатково використовують методи обробки сигналів для визначення азимута та кута місця завадного сигналу — форму ситуаційної обізнаності, відому як **визначення напрямку (direction-finding)**, що є важливим для критично важливих місій. Залежно від типу спуфінгу, CRPA та пов’язана електроніка також забезпечують побічні можливості протидії спуфінгу, оскільки вони виявляють аномальні сигнали — тобто сигнали, потужність яких перевищує певний поріг, — і пригнічують їх шляхом формування нулів.

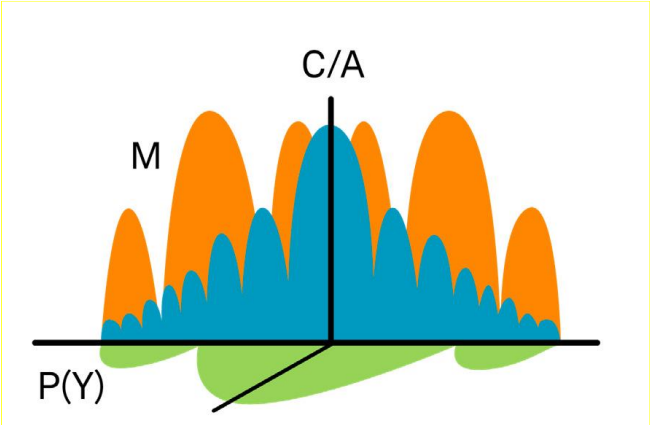


Рисунок 4. Коди сигналів GPS.

Захист на рівні приймача

Окрім використання GNSS-приймачів, здатних відстежувати зашифровані коди, сучасні GNSS-приймачі включають власні алгоритми мікропрограмного забезпечення або цифрові фільтри, які можуть виявляти та усувати завадні сигнали шляхом зменшення їхньої потужності (див. вставку). Це охоплює як позадіапазонні сигнали, так і високопотужні внутрішньодіапазонні глушильні сигнали.

Багатосузірні та багаточастотні приймачі (**multi-constellation, multi-frequency — MCMF**), які одночасно відстежують кілька GNSS-сузір'їв, є ефективними проти деяких спуферів, оскільки їм довелося б генерувати та передавати всі можливі GNSS-сигнали одночасно, щоб ввести в оману цільовий приймач. Хоча це можливо в лабораторних умовах, у польових умовах це зробити дуже складно — особливо якщо ціль рухається.

Оскільки спуфінг-сигнали не завжди можна відрізнити від автентичних GNSS-сигналів за частотою або рівнем потужності, алгоритми цифрової фільтрації в приймачі зосереджуються на **метриках виявлення**, щоб попередити користувача — ще одна форма ситуаційної обізнаності. Таким чином, навіть якщо приймач зазнає спуфінгу, користувач не буде введений в оману фальсифікованими вимірюваннями PNT і зможе ухвалювати обґрунтовані рішення для захисту персоналу та активів.

Допоміжне обладнання

Окрім CRPA та високоточних GNSS-приймачів, користувачі можуть застосовувати альтернативні датчики як додатковий рівень захисту. Типовим підходом є використання **інерціальних навігаційних систем (INS)**, які забезпечують позиціонування на основі даних від акселерометрів і гіроскопів у складі інерціального вимірювального блоку (**IMU**), оскільки ці вимірювання не можуть бути ціллю для глушників.

В ідеальному випадку INS є **глибоко з'єднаною (deeply coupled)** з GNSS-приймачем через злиття датчиків для забезпечення надійного, безперервно доступного тривимірного положення, швидкості та орієнтації навіть у періоди недоступності GNSS-сигналів. Глибоке з'єднання описує спосіб, у який сирі інерціальні вимірювання використовуються для покращення

Переклад українською – ТОВ «Є.П.С.»

відстеження сигналів у GNSS-алгоритмах позиціонування. Завдяки глибокому з'єднанню вимірювання INS забезпечують швидке повторне захоплення GNSS-сигналів для досягнення високої точності позиціонування. Крім того, вихідні дані різних типів датчиків руху — таких як камери, радар, LiDAR та одометричні вимірювачі відстані (**DMI**) — можуть використовуватися в алгоритмі для доповнення GNSS-PNT.

Як працюють алгоритми обробки сигналів і цифрові фільтри?

Електроніка CRPA

Електроніка антенних решіток CRPA використовує адаптивне формування променя, метод обробки сигналів просторової фільтрації, для спрямування решітки на формування нульових сигналів (ігнорування перешкод з певного напрямку) та, з додаванням датчиків, керування променем (підсилення автентичних сигналів з іншого напрямку) (Рисунок 5). Керування променем вимагає приймача та IMU, а також додаткових обчислень, що впливає на вимоги до розміру, ваги та потужності (SWaP) та вартість.

Існує два основних типи алгоритмів формування променя: просторово-часова адаптивна обробка (STAP) та просторово-частотна адаптивна обробка (SFAP). STAP виявляє та зменшує перешкоди на основі просторової (напрямок) та часової (період) областей. Виявлення SFAP базується на напрямку та частоті, що розширює можливості нульового регулювання решітки, додаючи частотні ступені свободи понад n-1 просторових ступенів свободи, що надаються кількома елементами антени.

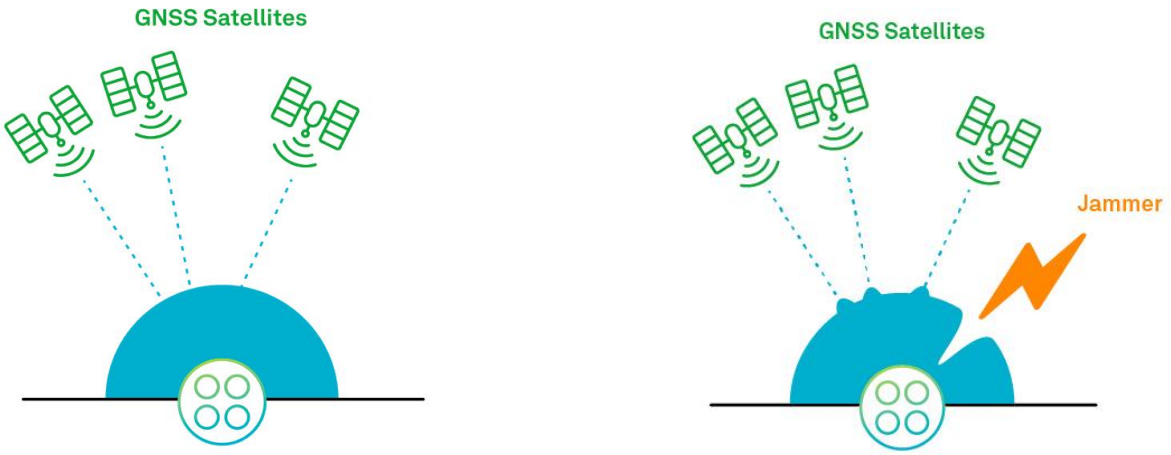
На практиці це означає, що SFAP може вибірково усувати вузькосмугові перешкоди, не послаблюючи інші частоти з того ж напрямку. Більш просунуті власні алгоритми використовують комбінацію методів STAP та SFAP для кращого зменшення впливу різних типів перешкод.

Прошивка приймача

У випадках неможливості використання CRPA через обмеження SWaP або обмеження вартості, високопродуктивні приймачі GNSS використовують власні алгоритми прошивки для виявлення сигналів глушіння та спуфінгу, а також для сповіщення користувача про те, що його PNT знаходиться під атакою. Це дозволяє користувачеві контролювати, кількісно визначати та видаляти джерела перешкод.

Ці алгоритми включають аналіз радіочастотного спектру, подібний до того, що забезпечується аналізатором спектру, щоб показати, яка потужність сигналу визначається в усіх діапазонах частот GNSS (Рисунок 6A). Перешкоди можна побачити на графіку вихідного спектрального аналізу (Рисунок 6B). Потім можна застосувати обробку сигналів та цифрові фільтри, такі як режекторний або смуговий фільтр (Рисунок 6C та D), для зменшення перешкод, що дозволяє приймачу продовжувати відстежувати автентичні сигнали GNSS та забезпечувати захищений APNT.

У статті «Try to spoof us. But fool us? Not a chance» з випуску журналу Velocity за 2021 рік детальніше розглядаються алгоритми прошивки приймача.



Спокійний

Діаграма посилення майже напівсферична

Атака глушилки

Нульовий сигнал формується в напрямку глушилки, а промені посилення спрямовуються на супутники

Рисунок 5. Графічне представлення діаграми посилення решітки CRPA до та під час атаки глушилки.

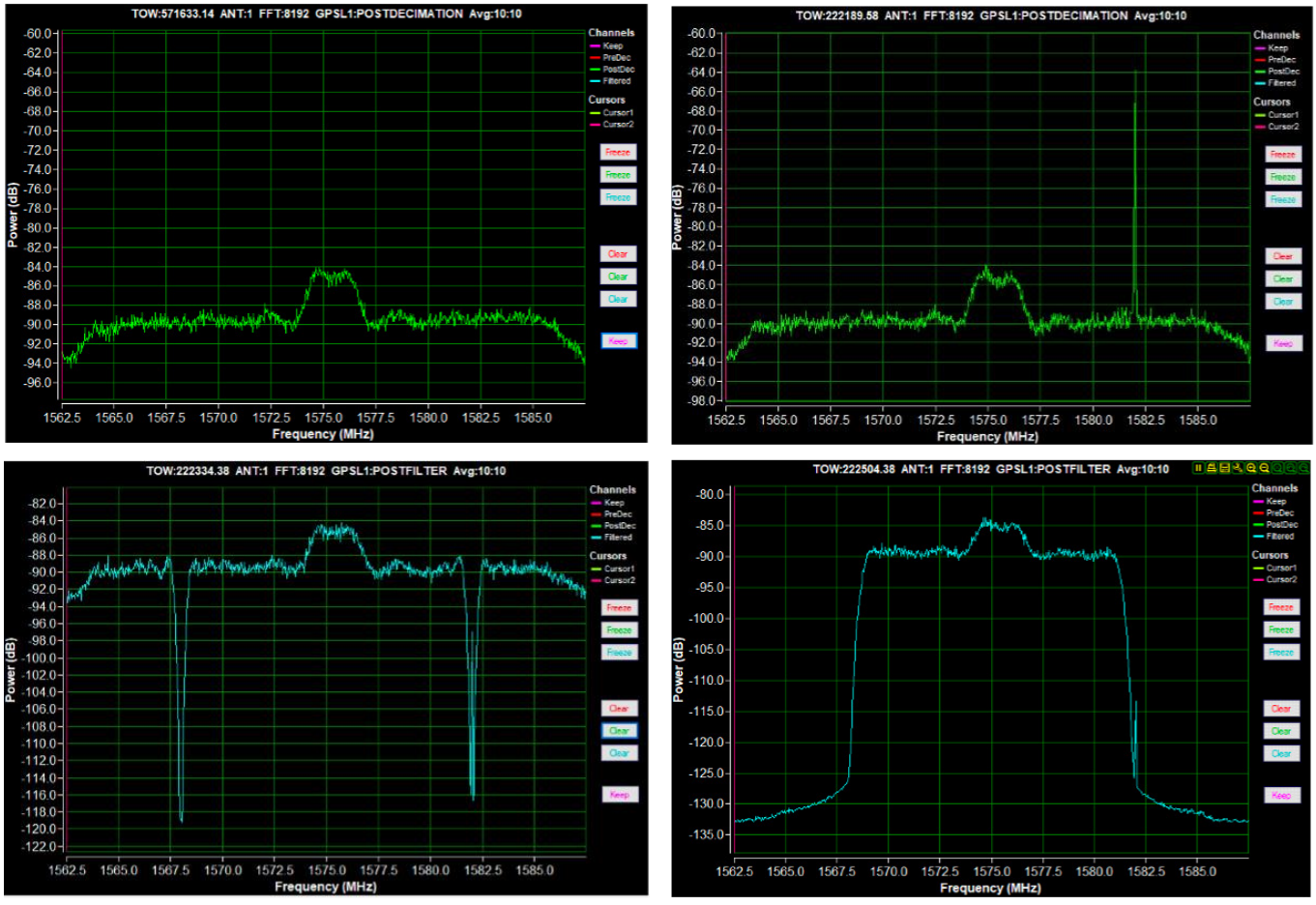


Рисунок 6. Приклади спектральних графіків, що показують спектр діапазону GPS L1 без перешкод (A), діапазону GPS L1 з перешкодами (B) та використання режекторного (C) та смугового (D) фільтрів для блокування перешкод.

Як вимірюється ефективність протидії глушінню?

Якщо ви переглядали специфікаційні листи продуктів протидії глушінню, ви, ймовірно, бачили кілька термінів, що використовуються для опису ефективності протидії глушінню. Прикладами такої термінології є захист від глушника (jammer protection), придушення інтерференції (interference suppression), пом'якшення/відхилення/стійкість до глушіння (jamming mitigation/rejection/resistance) та відношення глушника до сигналу (jammer-to-signal ratio, J/S). Деякі з цих термінів використовуються взаємозамінно, і нюанси значень цих вимірювань можуть бути заплутаними.

Для порівняння, двома поширеними вимірюваннями є придушення інтерференції та J/S, обидва з яких вимірюються в децибелах (дБ).

Придушення інтерференції (IS) кількісно визначає здатність антенної системи протидії глушінню зменшувати рівень сигналу глушника до того, як він досягне приймача. Воно вимірюється як різниця в потужності глушіння, необхідній для порушення роботи приймача, захищеного антенною системою протидії глушінню, порівняно з незахищеним приймачем. Наприклад, придушення інтерференції на рівні 40 дБ означає, що приймач, захищений антенною системою протидії глушінню, може витримати на 40 дБ більшу потужність глушіння до порушення його роботи порівняно з тим самим незахищеним приймачем. Метрикою порушення роботи приймача може бути повна втрата позиції, похибка положення 10 метрів або інша релевантна метрика для застосування інтегратора.

J/S — це відношення потужності глушника до потужності сигналу до моменту порушення роботи системи позиціонування. Під час роботи з GNSS-антеною, що не є CRPA, значення J/S системи позиціонування визначається переважно характеристиками приймача, оскільки GNSS-антена забезпечує обмежений захист від глушіння. Однак у поєднанні з антенною системою протидії глушінню значення J/S загальної системи позиціонування (рисунок 7) є поєднанням придушення інтерференції, яке забезпечується антенною системою протидії глушінню, та власного значення J/S приймача. Крім того, значення J/S є динамічним і залежить від сценарію глушіння, такого як кількість глушників та типи їхніх сигналів, смуги пропускання і розташування, а також тип приймача та сигнали, що відстежуються (C/A, P(Y) або M-Code).

Як обговорювалося в попередньому розділі, здатність GNSS-рішення придушувати глушіння залежить від атакувального сигналу, використовуваної антенної системи протидії глушінню та приймача. Тому будь-яке вимірювання ефективності протидії глушінню повинно враховувати окремі компоненти. Аналогією може слугувати стереосистема з CD-програвачем, підсилювачем і динаміками. Аудіо-ефективність системи залежить від якості всіх компонентів окремо.

Наприклад, виробник антенної системи протидії глушінню може наводити значення J/S, не уточнюючи, що воно стосується загальної системи позиціонування — включно з внеском приймача. У такому разі складається враження, що антена протидії глушінню забезпечує весь захист. Якщо користувач порівнюватиме це значення з показником придушення інтерференції, заявленим іншим виробником антенних систем протидії глушінню, він може припустити, що остання має нижчу ефективність.

На жаль, не існує єдиної загальноприйнятої методології випробувань для вимірювання J/S протидії глушінню або коефіцієнта покращення. Змінні, які впливають на ці значення, включають: 1) спарений приймач, 2) кількість глушників, 3) глушильний сигнал, 4) напрямок глушника та 5) антену. Таким чином, найкращим способом оцінки можливостей протидії глушінню або спуфінгу є випробування рішень у вашому конкретному застосуванні та середовищі.

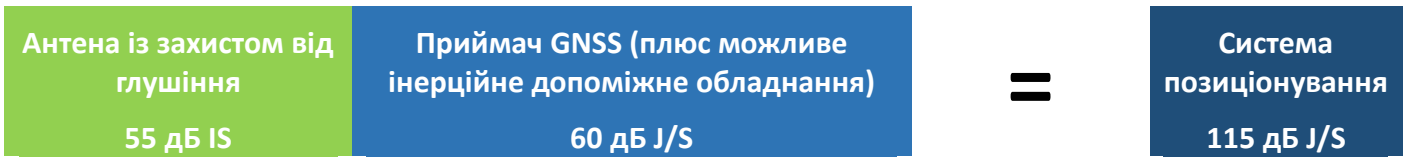


Рисунок 7. Співвідношення рівня перешкод до рівня сигналу (J/S) системи позиціонування в цілому дорівнює сумарним можливостям системи протишумової антени та приймача GNSS.

Чи існує GNSS, яке неможливо заглушити або заспуфити?

Проста відповідь — **ні**. За наявності достатньої потужності глушника та/або достатньої кількості глушників будь-яку систему GNSS-позиціонування можна заглушити. Це схоже на броню — танк забезпечує більший захист, ніж позашляховик, але за наявності достатньо потужної зброї можна вразити й танк. Метою стійкої системи позиціонування є зробити її настільки надійною, щоб логістика та обладнання, необхідні для спричинення втрати забезпечених PNT (APNT), були дорогими та непрактичними.

Оскільки протидія інтерференції залежить від можливостей системи в цілому, найкращим способом протидії глушінню та спуфінгу є багаторівнева оборона з використанням антени протидії глушінню (CRPA) та інерціальної навігаційної системи (INS) з глибоким з’єднанням із GNSS-приймачем і альтернативними датчиками. Для військових користувачів застосування ключованого військового зашифрованого приймача (M-Code) забезпечує додатковий рівень захисту.

Посилання (References)

• A. Broumandan, S. Kennedy and J. Schleppe, “Nobody’s Fool: Spoofing Detection in a High-Precision Receiver,” Inside GNSS+, July/August 2020, pp 36-42.

• A. Broumandan, S. Kennedy and J. Schleppe, “Demonstration of a Multi-Layer Spoofing Detection Implemented in a High Precision GNSS Receiver,” 2020 IEEE/ION Position, Location and Navigation Symposium (PLANS), Portland, OR, USA, 2020, pp. 538-547, doi: 10.1109/PLANS46316.2020.9109842.

• Jafarnia-Jahromi, Ali, Broumandan, Ali, Daneshmand, Saeed, Lachapelle, Gérard, “Vulnerability Analysis of Civilian L1/E1 GNSS Signals Against Different Types of Interference,” Proceedings of the 28th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2015), Tampa, Florida, September 2015, pp. 3262-3271.

• “Try to spoof us. But fool us? Not a chance. Jamming and spoofing detection and mitigation in a commercial receiver.” Hexagon’s Autonomy & Positioning division’s Velocity MagazineVelocity, 2021, pp 10-15.

• Pirsiavash, A., Broumandan, A., & Kennedy, S. (2024). OSNMA: Necessary But Not Sufficient for GNSS Security. Inside GNSS+, Sept/Oct 2024, pp 20-28.

• Pirsiavash, A., Broumandan, A., & Kennedy, S. (2024). Galileo Open Service Navigation Message Authentication (OSNMA) Benefits, Challenges, and Limitations. Proceedings of the 37th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2024), 16-20 September, Baltimore, Maryland.

• Pirsiavash, A., Broumandan, A., & Kennedy, S. (2024). OSNMA: A Step Toward Multi-Layered GNSS Security. Hexagon’s Autonomy & Positioning division’s Velocity Magazine 2024.

Novatel Inc.

Hexagon Calgary Campus | 10921 14th St. NE | Calgary, Alberta, Canada T3K 2L5

US & Canada 1-800-NOVATEL or +1-403-295-4900

China +86-21-68882300 | Europe +44-1993-848-736 | SE Asia & Australia +61-400-883-601

Website: novatel.com | Email: sales.ap@hexagon.com

Version 2

May 2025

Переклад українською – ТОВ «Є.П.С.»