Підроблено (spoofed) чи заглушено (jammed)?

Розвіюємо міфи про перешкоди та послаблення GNSS

Якщо ваша діяльність на робочому місці вимагає точного знання того, де ви знаходитесь і куди збираєтеся, ви, безсумнівно, покладаєтеся на глобальні навігаційні супутникові системи (GNSS) для точного позиціонування, навігації та визначення часу (PNT). GNSS - це загальний термін для будь-якого супутникового угруповання, яке передає дані для позиціонування, навігації та визначення часу. На рис. 1 показані глобальні та регіональні супутникові угрупування та їх сигнали. Радіочастотні (RF) сигнали GNSS використовуються для PNT у різних галузях промисловості та військовій сфері (від наземних до бортових і морських застосувань) які вимагають високої точності, надійності та доступності.

Критичною проблемою, з якою стикаються ті, хто покладається на гарантований PNT (APNT), є загрози для сигналів GNSS, особливо при роботів в середовищах GNSS із забороною, перервами або обмеженнями (D/DIL). До них належать військові театри та морські прибережні регіони. Чорне та Середземне моря, береги яких охоплюють країни з високою комерційною тапромисловою активністю, а також військовими заворушення, черезприбережну та наземну діяльність мають переповнені зони RF спектру. Стратегічні регіони, такі як Скандинавія, також часто піддаються загрозам в роботі GNSS з боку протилежних режимів.

Будь-який збій у передачі сигналу GNSS може призвести до часткової або повної втрати PNT, тобто ви фактично керуєте автомобілем, літаєте або плаваєте наосліп. Загрози для сигналів GNSS можуть бути ненавмисними або навмисними (див. вставку нижче). Було задокументовано багато випадків ненавмисного втручання, починаючи від несправних телевізійних передавачів і закінчуючи іншими джерелами передачі, не пов'язаними з GNSS, які проникали у діапазони частот GNSS. Якщо заважаючий сигнал навмисно передається в діапазоні частот GNSS, це називається глушінням (jamming).

Іншою загрозою для позиціонування GNSS є підробка (spoofing). Це навмисне надсилання підроблених сигналів GNSS на приймач, він обчислює хибне положення, змушуючи користувача вважати, що він знаходиться в іншому місці або в інший час, ніж насправді. Цей тип загрози викликає особливе занепокоєння в критично важливих для безпеки програмах у всіх галузях промисловості — комерційних чи військових — які покладаються на точні PNT із підтримкою GNSS.

Чому сигнали GNSS схильні до глушіння та підробки?

Радіочастотний спектр розділений для використання у різних цілях, тому діапазони сигналів GNSS є фіксованими та мають відомі частоти (рис. 1). Це робить їх сприйнятливими до глушників і спуферів, що випромінюють сигнали в тому самому діапазоні частот.

Що ще гірше, до того часу, коли сигнали GNSS проходять 20 000–25 000 км від супутників на середній навколоземній орбіті (MEO) до приймача на поверхні Землі, вони мають дуже низький рівень потужності (-130 dBm або 1E-13 мВт) — у 600 квадрильйонів (це 15 нулів) разів слабкіше, ніж лампочка на 60 Вт!

Цей низький рівень потужності робить сигнали GNSS сприйнятливими до перешкод від більш потужних сигналів, що передаються в тому ж діапазоні частот. Ось чому потужні перешкоди можуть заглушити приймач GNSS, і чому слід розглянути захист і посилення.

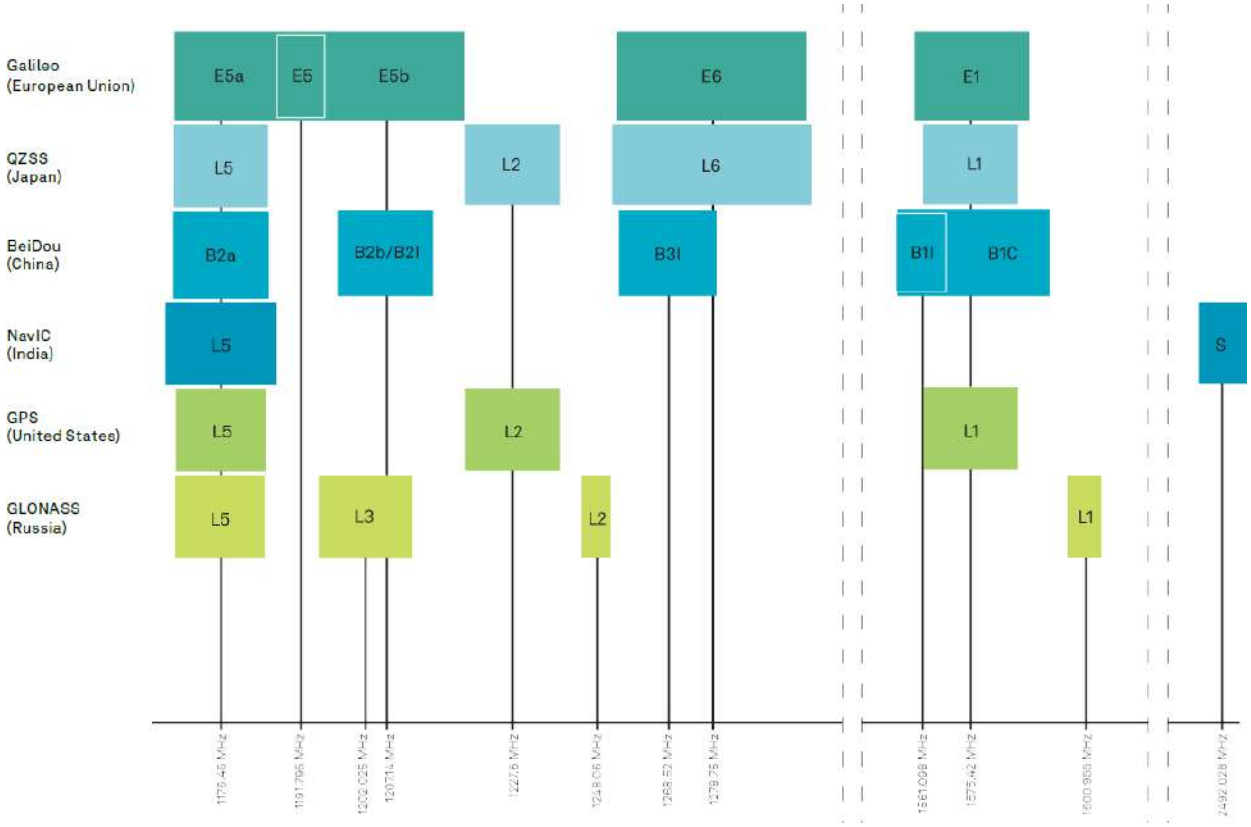


Рисунок 1. Супутникові навігаційні системи та сигнали GNSS.

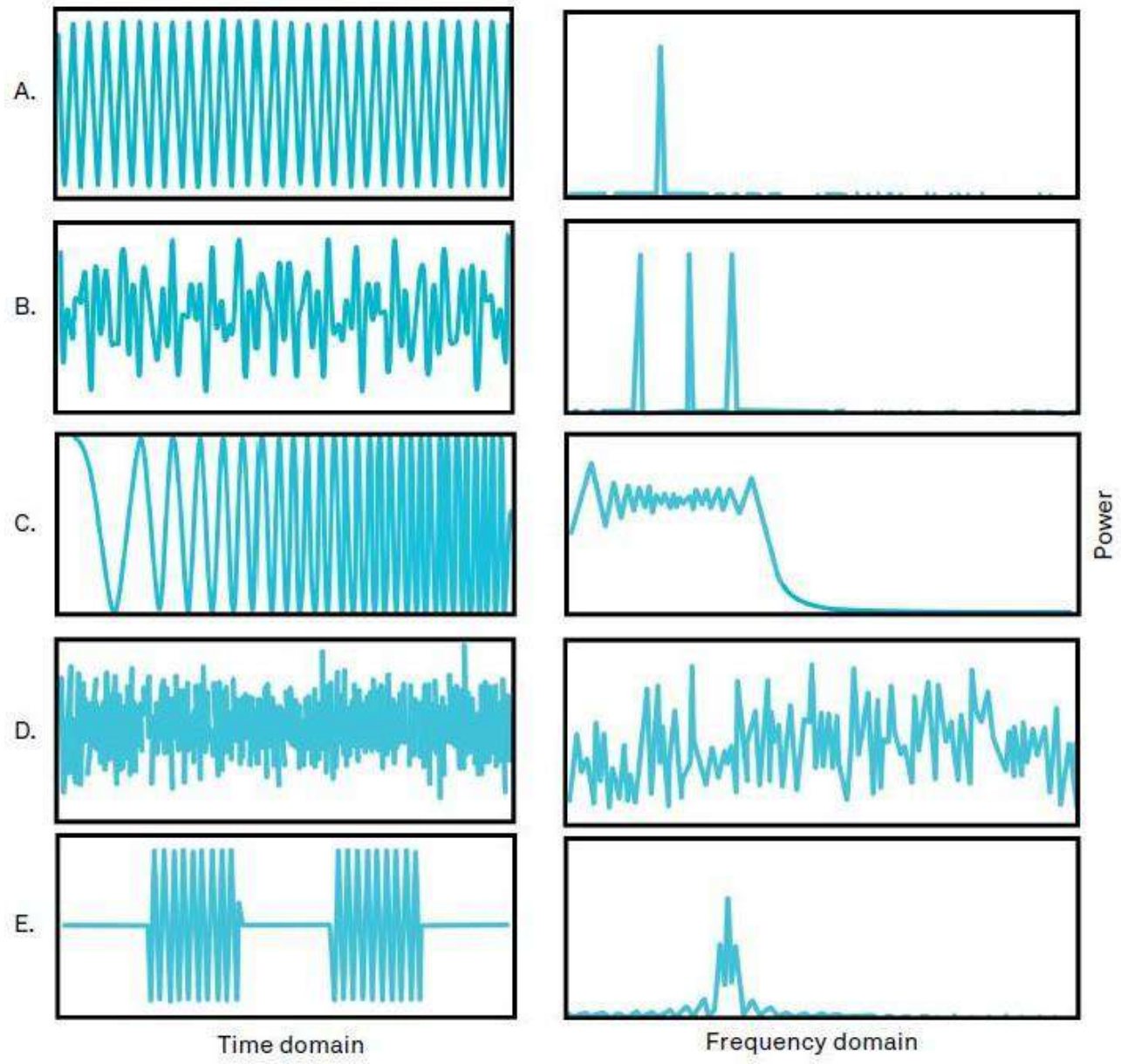


Рисунок 2. Типи глушіння. A. Суцільна вузькосмугова хвиля. B. Безперервна багатотональна хвиля. C. Chirping. D.Wideband. E. Pulse. (Jahromi et al., 2015)

Яка різниця між глушінням і спуфінгом?

Головним відмінним фактором між глушінням і спуфінгом з точки зору користувача є вплив, який він має на здатність приймача надавати PNT. Перешкоди проявляються як втрата інформації PNT, оскільки корисний сигнал перекривається сигналом перешкод. З іншого боку, підробка призводить до отримання неправильної інформації PNT.

Аналогія для порівняння різниці між глушінням і спуфінгом полягає в тому, що грабіжник перериває трансляцію камери відеоспостереження, тому охоронець бачить сірі статичні плями на екрані монітора (глушення), або грабіжник замінює трансляцію відео, яке показує те саме зображення з іншого часу, створюючи охоронець вважає, що все добре (спуфінг). Ось чому з точки зору користувача GNSS спуфінг викликає більше занепокоєння. На відміну від глушіння, ви можете не знати, що вас обманюють.

З точки зору суб'єкта, який здійснює глушіння або підробку, обладнання та процес дещо відрізняються.

Глушіння здійснюються шляхом перевантаження приймача GNSS радіочастотними сигналами більшої потужності. Незважаючи на те, що в більшості юрисдикцій це незаконно, малопотужні передавачі перешкоди, відомі як «пристрої конфіденційності», можна придбати в Інтернеті та використовувати для цієї мети. Навіть простий малопотужний передавач перешкод може подавити сигнали GNSS на великій території, зриваючи PNT.

Ефективність засобів перешкод в першу чергу залежить від їх вихідної потужності та відстані до GNSS приймача. Перешкоди малої потужності поблизу можуть мати такий самий ефект, як потужні перешкоди, що передають з більшої відстані. Іншими характеристики передавачів перешкод є їх сигнали. Передають вони вузькосмугові або широкосмугові завади, чи вони передаються увигляді безперервної хвилі (на вибраній частоті, або у виді розгортки на заданому спектрі), або пульсують з певною швидкістю на нижчому рівні потужності (тріскотіння). На рисунку 2 показано приклади кількох типів сигналів перешкод.

Спуфінг часто є двоетапним процесом. На першому етапі використовуються перешкоди які заважають приймачу здійснювання відстеження автентичних сигналів GNSS, а потім використовується радіопередавач для надсилання хибних сигналів цільовому приймачу. Помилкові сигнали можуть бути створені генератором сигналів або ретрансляцією записаних сигналів GNSS, що називається meaconing. Якщо приймач не почав відстежувати автентичні сигнали GNSS (наприклад, після запуску), для спуфінгу знадобиться лише другий крок.

Простим прикладом спуфінгу є використання недорогого програмно-визначеного радіо (SDR), яке дозволяє передавати генеровані потоки даних сигналу базової смуги GNSS щоб змусити смартфон думати, що він надворі в парку, коли він ще вдома. Концептуально більш серйозні атаки спуфінгу з використанням складних симуляторів сигналу GNSS є такими ж, але наслідки можуть бути жахливими — наприклад, якщо літак приземлився там, де йому не слід, або корабель, який запливе в недружні води. Атаки підробки можна додатково класифікувати за їхньою відносною потужністю порівняно з автентичними сигналами GNSS і тим, чи синхронізовані фальшиві сигнали з різними аспектами автентичних сигналів GNSS чи ні (див. праву вставку). Якщо ціль рухається, спуфер також повинен знати її швидкість і курс, щоб відрегулювати рівень переданого сигналу спуфінгу (і допплерівський зсув), щоб одурити цільовий приймач.

З цього вступу легко зрозуміти, чому захист від перешкод і спуфінгу став критично важливим компонентом обладнання GNSS. Зараз ми обговоримо, що ви можете зробити, щоб запобігти глушінню чи підробці — або обом!

Які існують типи спуфінгу?

Незалежно від джерела спуфінгу їх можна класифікувати як неперекриваючі або перекриваючі, а також за їхньою відносною потужністю порівняно з автентичними сигналами GNSS. На рисунку 3 показано чотири типи атак спуфінгу.

Атаки спуфінгу без перекриття – це випадки, коли код і фаза несучої (затримка та допплерівська частота) сигналів спуфінгу не синхронізовані з автентичними сигналамиGNSS. Атаки підробки, що перекриваються, є більш складними, оскільки фаза коду та допплерівська частота сигналів підробки синхронізовані з автентичними сигналами GNSS. Цей тип атаки вимагає, щоб спуфер знав поточний час, спостережувані супутники, місцезнаходження та параметри цільового приймача.

Стаття "Nobody's Fool: Spoofing Detection in a High-Precision Receiver" з July/August 2020 issue of Inside GNSS містить більш детальний погляд на виявлення різних типів атак спуфінгу .

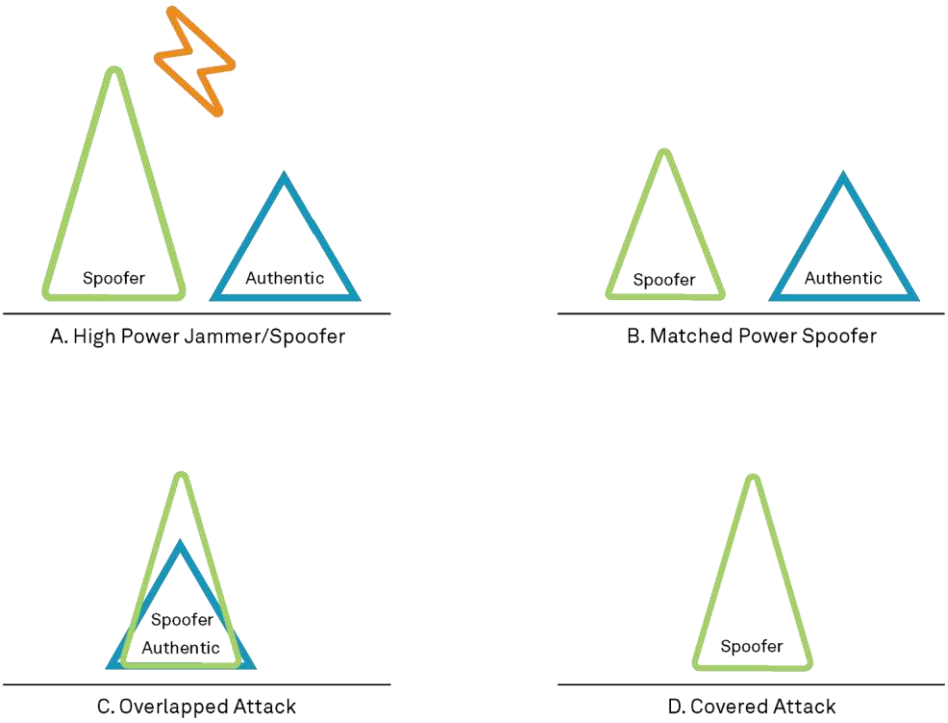


Рисунок 3. Типи атак спуфінгу.
A. Jam/Spoof: сигнал глушіння високої потужності, за яким слідує сигнал спуфінгу. B. Відповідна потужність: потужність підробки відповідає автентичному сигналу. C. Перекривається: кореляційна функція автентичного та підробленого сигналів накладається. D. Покритий: спуфер маскує прийом автентичних сигналів. (Broumandan et al., 2020)

Як пом’якшуються перешкоди та підробка?

Першою лінією захисту від перешкод у будь-якій системі GNSS є виявлення та відхилення або придушення якомога більшої кількості перешкод, перш ніж вони вплинуть на PNT. На базовому рівні система GNSS включає супутникові сигнали, антену та приймач. На кожному з цих трьох рівнів розроблено стратегії пом’якшення глушіння та спуфінгу, як описано нижче. Кожен із цих компонентів працює разом, створюючи додатковий ефект проти перешкод. Разом вони дають користувачеві спокій, що його PNT захищено, і вони можуть безпечно виконувати свої операції.

Сигнальний захист

Для військових застосувань існують зашифровані коди сигналу GNSS які запобігають перешкодам і підробці. Наприклад, код GPS P(Y) — це зашифрований двійковий код 1 та 0, що передається на частотах L1 і L2. Код P(Y) змінюється 10,23 мільйона разів на секунду та складається з унікальної послідовності з 6,18 трильйонів 1 та 0 на супутник, яка оновлюється щотижня. Для коду P(Y) потрібен приймач із модулем захисту від фальсифікації вибіркової доступності (SAASM) із дійсним ключем розшифрування (експортний товар у багатьох країнах, включаючи Канаду та Сполучені Штати).

M-Code — це новий військовий сигнал GPS L1/L2, призначений для подальшого покращення захисту від перешкод. M-Code розроблений як автономний, тобто користувачі можуть обчислювати свої позиції, використовуючи лише сигнал M-Code. Навпаки, для того, щоб приймачі використовували P(Y)-код, вони, як правило, повинні спочатку заблокувати загальнодоступний код C/A, а потім перейти до блокування за P(Y)-кодом. Сигнал M-коду розміщує більшу частину своєї енергії по краях спектру, подалі від існуючих P(Y) і C/A несучих. Крім того, M- Code буде передаватися з антен з більшим коефіцієнтом посилення, які збільшують потужність сигналу, роблячи його менш схильним до впливу перешкод.
На рисунку 4 показано коди сигналу GPS.

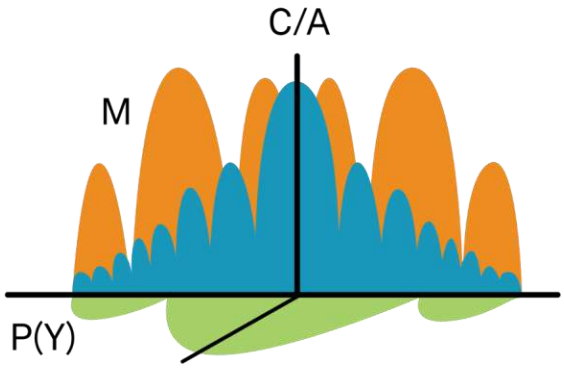


Рисунок 4. Коди сигналу GPS

Захист на основі антени

Високоякісні GNSS-антени забезпечують ще один рівень захисту від перешкод, оскільки вони збільшують потужність отриманого сигналу в частотному діапазоні GNSS, водночас не пропускаючи сигнали, які діють поза діапазоном. Деякі антени GNSS, що запобігають перешкодам, що діють на лінії горизонту, зменшують посилення сигналу на заданій висоті від лінії горизонті, однак цей підхід також блокує сигнали від діючих супутників на низькій висоті. Захист, який забезпечують ці антени, є обмеженим, оскільки їх все ще можна заглушити, якщо джерело перешкод відходить від заданої висоти горизонту або якщо є кілька джерел перешкод.

Адаптивні антенні решітки, такі як антени з контрольованим прийомом діаграми спрямованості (CRPA), і відповідна електроніка для захисту від перешкод забезпечують вищий рівень захисту, постійно контролюючи кількість сигналів, отриманих з будь-якого напрямку. Використовуючи кілька окремих елементів антени, електроніка CRPA адаптовано змінює коефіцієнт підсилення антенної решітки, створюючи «нульові значення» меншого посилення в напрямку джерела перешкод (формування нуля).

Система CRPA може створювати нулі в діаграмі спрямованості в n-1 напрямках, де n – кількість елементів. Отже, 7-елементна система може створювати нулі в 6 напрямках і так далі. Але це не так просто, і інші фактори, такі якгеометрія CRPA та алгоритм обробки сигналущовикористовується (див. вставку на стор. 7), можуть мати велике значення. Для розширених застосувань, таких як військові літаки, яківикористовують додаткові датчики для визначення розташування супутників GNSS, позиції та курсу платформи, система також може спрямовувати максимальне посилення до законних сигналів GNSS (керування променем).

Деякі рішення для захисту від перешкод додатково використовують методи обробки сигналів, щоб розрізняти пеленг і кут місця заважаючого сигналу, форма ситуаційної обізнаності, яка називається пеленгацією, що використовується в критично важливих програмах. Залежно від типу спуфінгу, CRPAта пов’язана з ними електроніка також надають допоміжну функцію захисту від спуфінгу, оскільки вони виявляють аномальні сигнали ті, що перевищують певний поріг потужності та пом’якшують їх шляхом обнулення.

Захист на основі приймача

Окрім використання GNSS-приймачів, які можуть відстежувати зашифровані коди, удосконалені GNSS-приймачі містять фірмові алгоритми мікропрограм або цифрові фільтри, які можуть виявляти та видаляти заважаючі сигнали, зменшуючи їх потужність (див. вставку на стор. 7). Це включає позасмугові сигнали, а також сигнали внутрішньосмугових перешкод більшої потужності.

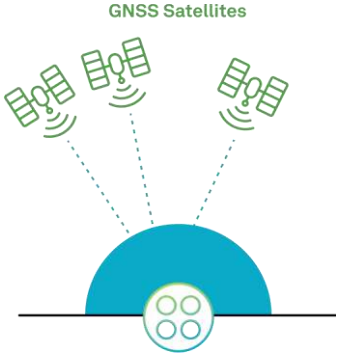
Багаточастотні приймачі які одночасно відстежують кілька сузір’їв GNSS (Multi-constellation, multi-frequency - MCMF) ефективні проти деяких спуферів. Щоб обдурити цільовий приймач доводиться виробляти та передавати всі можливі сигнали GNSS одночасно. Хоча це можна зробити в лабораторії, це дуже важко зробити в польових умовах, особливо якщо ціль рухається.

Оскільки підроблені сигнали не завжди можна відрізнити від автентичних сигналів GNSS на основі частоти або рівня потужності, щоб попередити користувача алгоритми цифрового фільтра на приймачі зосереджені на метриках виявлення, це ще одна форма ситуаційної обізнаності. Таким чином, незважаючи на те, що рішення приймача може бути підробленим, користувача не введуть в оману фальсифіковані вимірювання PNT і він зможе приймати обґрунтовані рішення, щоб захистити себе.

Додаткове обладнання

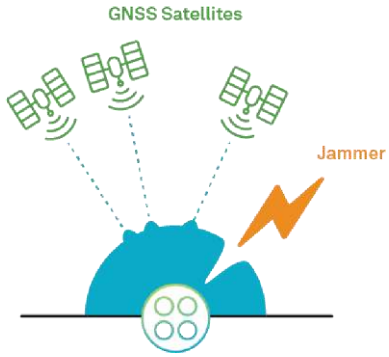
Окрім CRPA та високоточних приймачів GNSS, користувачі можуть використовувати альтернативні датчики як додатковий рівень захисту. Типовим підходом є використання інерційних навігаційних систем (INS), які забезпечують позиціонування за допомогою інформації, наданої акселерометрами та гіроскопами в інерційному вимірювальному пристрої (IMU), оскільки ці вимірювання не залежать від зовнішніх перешкод.

В ідеалі INS «глибоко комплексована» із приймачем GNSS через об'єднання датчиків дозволяє здійснювати надійне, постійно доступне визначення 3D-положення, швидкості та орієнтації навіть у періоди відсутності сигналу GNSS. Глибоке комплексування описує як використовуються необроблені інерційні вимірювання для покращення відстеження сигналу для алгоритмів позиціонування GNSS. Завдяки глибокому зв'язку вимірювання INS дозволяють швидко отримувати сигнали GNSS для підвищення точності позиціонування. Крім того, вихідні дані різних типів датчиків руху, таких як камери, радар, LiDAR і одометричні інструменти для вимірювання відстані (DMI), можна використовувати в алгоритмі для доповнення GNSS PNT.



Спокійний

Близько-півсферична схема посилення



Jammer атака

Нуль формується в напрямку джерела перешкод, а промені підсилення спрямовуються на супутники.

Рисунок 5. Графічне представлення шаблону підсилення масиву CRPA до та під час jammer-атаки

Як працюють алгоритми обробки сигналів і цифрового фільтра?

CRPA електроніка

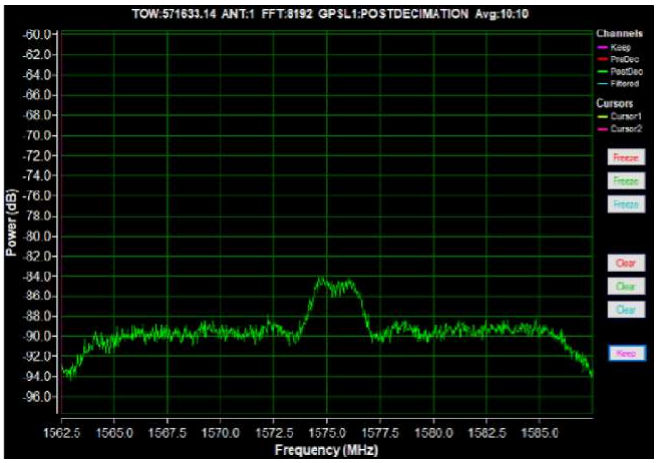
Антенна електроніка решіток CRPA використовує адаптивне формування променю, техніку обробки сигналу просторової фільтрації, щоб формувати нулі в спрямованості решітки (ігнорувати заважаючі сигнали з певного напрямку) і, з додатковими датчиками, керувати променем (посилювати автентичних сигналів з іншого напрямку) (Рисунок 5).

Для керування променем потрібен приймач та IMU, а також додаткові обчислення, що сприяють вимогам до розміру, ваги та потужності (SWaP) і вартості. Існує два основних типи алгоритмів формування променю: ***просторово-часова адаптивна обробка (STAP)*** і ***просторово-частотна адаптивна обробка (SFAP).***

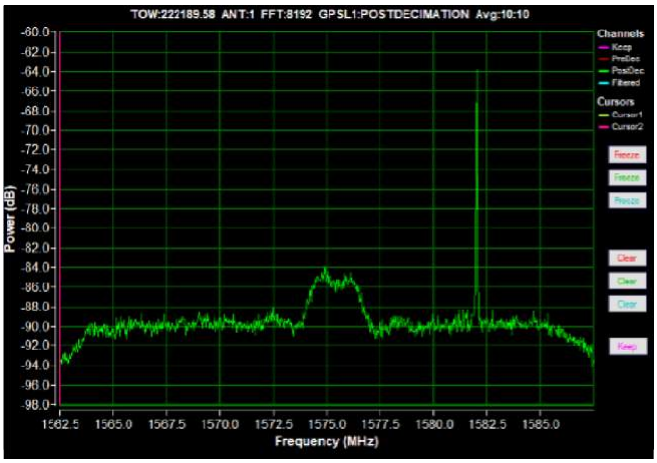
STAP виявляє та пом'якшує перешкоди на основі просторової (напрямок) і часової (період) областей. Виявлення SFAP базується на напрямку та частоті, що розширює здатність створення нулів решітки шляхом додавання частотних ступенів свободи за межі n-1 просторових ступенів свободи, наданих кількома елементами антени.

На практиці це означає, що SFAP може вибірково нулювати вузькосмугові перешкоди без ослаблення інших частот у тому ж напрямку. Досконаліші запатентовані алгоритми використовують комбінацію методів STAP і SFAP для пом'якшення дії цілого ряду типів перешкод.

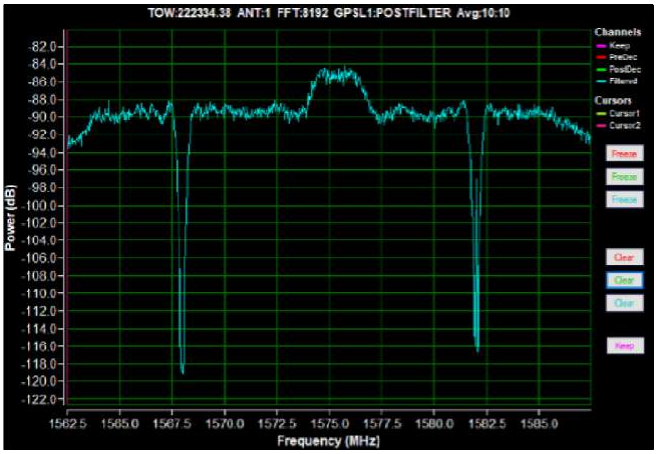
A.



B.



C.



D.

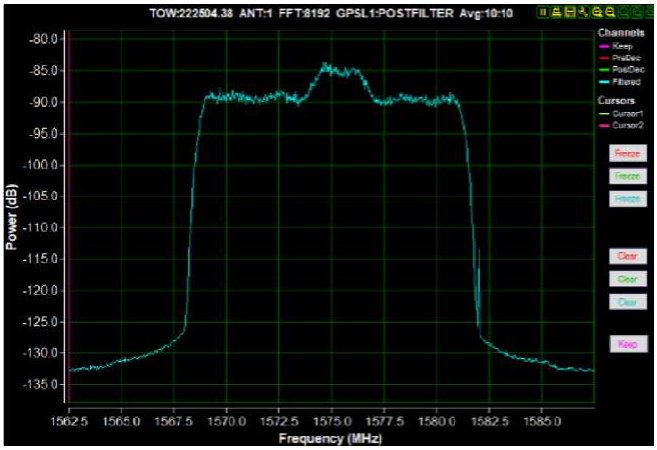


Рисунок 6. Приклади спектральних графіків, що показують спектр смуги GPS L1 без перешкод (A), смугу GPSL1 з перешкодами (B) і використання режекторного (C) і смугового (D) фільтрів для блокування перешкод.

Як працюють алгоритми обробки сигналів і цифрового фільтра? (продовження)

Прошивка приймача

У випадках, коли не можна використовувати CRPA через обмеження на контрольовані товари, розмір, вагу та потужність (SWaP) або обмеження вартості, високопродуктивні приймачі GNSS використовують власні алгоритми мікропрограми для виявлення перешкод і підробки сигналів і сповіщення користувача що їх PNT під атакою. Це дозволяє користувачеві контролювати, кількісно визначати та усувати джерела перешкод. Ці алгоритми включають аналіз радіочастотного спектру, щоб показати яка потужність сигналу визначається в діапазонах частот GNSS (рисунок 6A). Перешкоди можна побачити на графіку вихідних даних спектрального аналізу (рисунок 6B). Обробка сигналів і цифрові фільтри, такі як режекторний або смуговий фільтр (рис. 6C і D), можуть бути застосовані для пом'якшення перешкод, дозволяючи приймачу продовжувати відстежувати автентичні сигнали GNSS і забезпечувати захищений APNT.

Стаття "Try to spoof us. But fool us? Not a chance." з 2021 issue of Velocity надає більш детальний погляд на алгоритми прошивки приймача

Як вимірюється ефективність anti-jam?

Якщо ви переглядали специфікації anti-jam продуктів, ви, ймовірно, бачили кілька термінів, які використовуються для визначення ефективності захисту. Приклади термінології включають захист від перешкод, придушення перешкод, пом'якшення/придушення/стійкість до перешкод і співвідношення перешкод до сигналу (J/S). Деякі з цих термінів використовуються як взаємозамінні, і нюанси у значенні цих вимірювань можуть заплутати.

Для порівняння наведемо два загальних показника, **придушення перешкод** та **співвідношення перешкод до сигналу (J/S)**, обидва вимірюються в децибелах (дБ).

Придушення перешкод визначається як різниця в потужності перешкод необхідна для порушення роботи незахищеного приймача в порівнянні з приймачем захищеним антенною системою з захистом проти перешкод. Вимірюється ключовим показником, таким як втрата позиції або 10-метрова помилка.Наприклад, коефіцієнт поліпшення в 40 дБ означає, що приймач, захищений антенною системою проти перешкод, може витримати потужність перешкод на 40 дБ більше, перш ніж він буде придушений, порівняно з тим самим незахищеним приймачем.

J/S визначається як відношення потужності перешкод до потужності сигналу до того, як приймач буде придушений, якщо він захищений антенною системою з захистом від перешкод. J/S має абсолютне значення і сильно залежить від приймача в парі з антенною системою з захистом від перешкод. Крім того, значення J/S також залежить від сценарію у якому воно вимірюється, включаючи кількість джерел перешкод і типи їх сигналів, смугу пропускання та розташування, а також тип приймача тасигнали, що відстежуються (C/A, P(Y) або M-код).

Як обговорювалося в попередньому розділі, здатність GNSS рішення придушувати перешкоди залежить від атакуючого сигналу, антенної системи захисту від перешкод і використовуваного приймача.

Таким чином, будь-який захід пом'якшення перешкод повинен враховувати окремі компоненти. Аналогією може бути стереосистема з програвачем компакт-дисків, ресивером і колонками. Аудіопродуктивність систем залежить від якості всіх компонентів окремо.

Наприклад, виробник системи захисту від перешкод може вказати J/S антени та приймача як єдине значення (загальна система, рис. 7), не вказуючи, що це значення включає продуктивність приймача. Якщо користувач порівнює це значення із заявленим іншим виробником захистом від перешкод лише для антенної системи проти перешкод, він може припустити, що остання має нижчу продуктивність.

Зрештою, найкращий спосіб оцінити можливості захисту від перешкод або спуфінгу — це перевірити рішення у вашій конкретній програмі та середовищі.

Рисунок 7. Можливість відношення перешкод до сигналу (J/S) загальної системи дорівнює сумарним можливостям антени проти перешкод і приймача GNSS

Чи є обладнання GNSS, яке не може глушити?

Проста відповідь - ні. За наявності достатньої потужності та/або кількості перешкод будь-якій системі позиціонування GNSS можна створювати перешкоди. Це як броня — танк дає більше захисту, ніж позашляховик, але з достатньо великою зброєю ви можете перемогти танк.

Мета стійкої системи позиціонування полягає в тому, щоб зробити її достатньо надійною, щоб логістика та обладнання, необхідні для втрати APNT, були дорогими та непрактичними.

Оскільки пом'якшення перешкод залежить від повної спроможності системи, найкращим способом боротьби з перешкодами та спуфінгом є багаторівневий захист із використанням антени проти перешкод (CRPA) та INS із глибоким зв'язком із приймачем GNSS та альтернативними датчиками. Для військових користувачів використання військового шифрованого приймача з ключем (M-Code) забезпечує додатковий рівень захисту.

Використані джерела

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." Velocity, 2021, pp 10-15.

Зовнішній вигляд візуальної інформації Міністерства оборони США не означає або не є підтримкою Міністерства оборони США.

Hexagon є світовим лідером у сфері рішень цифрової реальності, що поєднує датчики, програмне забезпечення та автономні технології.
Ми використовуємо дані, щоб підвищити ефективність, продуктивність, якість і безпеку в промисловості, виробництві, інфраструктура, державний сектор і програми мобільності.
Наші технології формують виробничі та пов'язані з людьми екосистеми, щоб вони ставали все більш зв'язаними та автономними, забезпечуючи масштабоване та стійке майбутнє.
NovAtel, частина Hexagon, є світовим технологічним лідером, що розробляє наскрізні рішення для гарантованого позиціонування на землі, морі та повітрі. NovAtel розробляє, виробляє та продає високоточну технологію позиціонування, розроблену для ефективної та швидкої інтеграції. Її рішення розширюють можливості інтелектуальних екосистем позиціонування в життєве важливих галузях, які залежать від здатності вирішувати найскладніші виклики в найвимогливіших середовищах. Дізнайтесь більше на novatel.com.

Переклад українською мовою ТОВ «Є.П.С.» 11.06.2024 https://eps.com.ua/