УДК 621.391

М.В. Думанський

ПІДМІНА НАВІГАЦІЙНИХ ДАНИХ ЯК МЕТОД ПРОТИДІЇ НЕСАНКЦІОНОВАНОМУ ВИКОРИСТАННЮ БЕЗПІЛОТНИХ ПОВІТРЯНИХ СУДЕН. СПУФІНГ

Описано теорію захоплення безпілотного повітряного судна (БПС(А) та керування ним через глобальну систему позиціонування (GPS), проаналізовано сигнали підміни. Мета цієї статті полягає у вивченні уразливості підмінених сигналів GPS. БПС(А) вважається захопленим, коли спуфер отримує можливість в кінцевому підсумку вказати положення і швидкість БПС(А). Під час контролю після захоплення спуфер маніпулює справжнім положенням БПС(А), що приводить до польотів БПС(А) далеко від плану завдання, не піднімаючи тривоги.

Ключові слова: *безпілотне повітряне судно, GPS спуфінг, протидія БПС(А).*

Описана теория захвата беспилотного воздушного судна (БВС(А) и управления им через глобальную систему позиционирования (GPS), проанализированы сигналы подмены. Цель этой статьи заключается в изучении уязвимости подмененных сигналов GPS. БВС(А) считается захваченным, когда спуфер получает возможность в конечном итоге указать положение и скорость БВС(А). При контроле после захват спуфер манипулирует настоящим положением БВС(А), что приводит к полетам БВС(А) далеко от плана задания, не поднимая тревоги.

Ключевые слова: *беспилотное воздушное судно, GPS спуфинг, противодействие БВС(А).*

The theory of unmanned aerial vehicle (UAV) capture and control via Global Positioning System (GPS) signal spoofing are analyzed. The goal of this work is to explore UAV vulnerability to deceptive GPS signals. UAV is considered captured when a spoofer gains the ability to eventually specify the UAV's position and velocity estimates. During post-capture control, the spoofer manipulates the true state of the UAV, potentially resulting in the UAV flying far from its flight plan without raising alarms.

Keywords: *unmanned vehicle security, GPS spoofing, Counter-UAV.*

Вступ

Спуфінг − атака на GPS навігацію (англ. *Spoofing* − підміна) − атака, яка намагається підмінити дані, що сприймаються GPS-приймачем, цілі, широкомовно передаючи більш потужні сигнали, ніж отримані від супутників GPS, такі сигнали, щоб вони були подібні до ряду нормальних сигналів GPS. Ці сигнали змінені в такий спосіб, щоб змусити одержувача не уточнювати своє місце розташування, вважаючи його таким, яке відправив атакуючий. Оскільки системи GPS працюють, вимірюючи час, який потрібен для сигналу, щоб дійти від супутника до одержувача, успішний спуфінг вимагає, щоб атакуючий точно знав, де знаходиться його ціль − так, щоб імітований сигнал міг бути структурований з належними затримками.

Для автономної або напівавтономної експлуатації безпілотних літальних суден (апаратів) (БПС(А)) потрібно використовувати надійну навігацію. До найбільш поширених систем забезпечення надійної навігації БПС(А) належать системи інерціальної навігації та глобальні системи супутникової навігації (Global Navigation Satellite System – GNSS) [1]. Але з огляду на нестабільну роботу GNSS систем в умовах створення перешкод на їх робочих частотах, в цей час існує великий інтерес до розробки навігації і управління системами БПС(А), які можуть працювати в GNSS-відмовних середовищах. Системи роботизованого зору автоматизованої навігації є практичною альтернативою GNSS для замкнутого контуру БПС(А) в безконтрольному (непідключеному) середовищі. Проте, на відміну від GNSS, системи роботизованого зору неминуче будуть накопичувати величину відхилення від курсу в ході розвідки на великих відстанях, потребують карти руху з позначеними на ній об'єктами (маркерами), і вони можуть бути застосовані тільки в сприятливих погодних умовах та при відповідному освітленні. Отже, можна очікувати, що більшість навігаційних систем для БПС(А) будуть базуватися на GNSS, а роботизований зір та інші не GNSS системи будуть використовуватися короткочасно в місцях неможливої роботи GNSS.

GNSS вразливість виходить далеко за межі недоступності сигналів із супутників. Спуфінг – атаки, в яких підроблені GNSS сигнали, генеруються з метою маніпулювання про місцезнаходження, швидкість, цілі, а також час, було продемонстровано за допомогою недорогого обладнання над широким спектром GPS приймачів. Тоді як побудова та форма військового GPS сигналу непередбачувана і тому стійка до підміни, цивільні GPS-сигнали та сигнали інших цивільних GNSS не зашифровані і відкрито вказані в публічно доступних документах. Поєднання відомої структури сигналу і бітової передбачуваності даних робить цивільні GNSS сигнали легкою ціллю для спуфінгу [2].

Ряд перспективних методів нині розробляється для захисту від атак підміни цивільних GNSS.

Вони можуть бути класифіковані як:

1) методи обробки сигналів, основані на автоматичному прийманні сигналу, з використанням нерухомих спеціалізованих антен;

2) методи обробки сигналів, основані на автоматичному прийманні сигналу, з використанням рухомих спеціалізованих антен;

3) криптографічні методи, які вимагають модифікації специфікацій сигналів цивільних GNSS;

4) методи, які використовують існуючі військові сигнали GPS.

На жаль, миндуть роки, перш ніж ці технології будуть допрацьовані і набудуть поширення. Водночас не існує іншого захисту від GNSS підміни.

У цій статті розглядається ступінь уразливості БПС(А) до підмінних сигналів GNSS, а саме створення необхідних умов для захоплення БПС(А) за допомогою GPS-спуфінга.

Проте заяви [2], зроблені щодо вразливості сигналів цивільного GPS, широко застосовуються щодо інших існуючих цивільних GNSS, чиї характеристики були опубліковані, в тому числі модернізовані GPS L2C і L5 і сигнали Galileo Open Service.

1. Компоненти системи, геометричні розміри, затримки

У цій статті розглядається спуфінг на відстані, як показано на рис. 1. Через приймальну антену та приймач спуфер отримує справжні сигнали від усіх видимих супутників GPS. Вектори Δr_{TX} і Δr_t представляються, відповідно, у 3-вимірних координатах, відносно антени передавача спуфера, яка позначена як ***TX*** і GPS антени цілі відносно антени приймача спуфера. Відповідно розраховується відстань від приймача спуфера та GPS антени цілі відносно кожного супутника GPS, сигнали від яких приймаються спуфером.

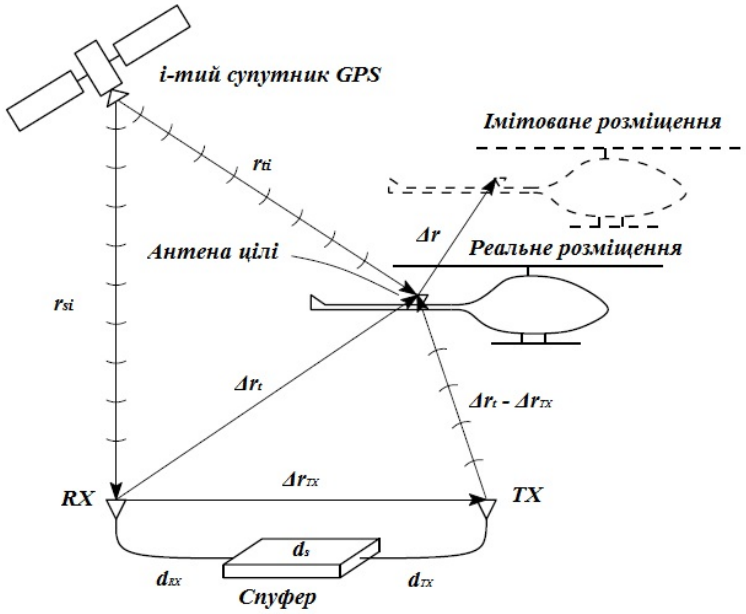

Рис. 1. Ілюстрація компонентів, відстаней і затримок, пов'язаних із спуфінгом GPS систем

Спуфер створює фальшиві сигнали для кожного справжнього сигналу відповідно. Підроблений сигнал зі спуфера передається на антену цілі таким чином, що кожен сигнал є аналогічним (розбіжність у межах декількох метрів) з її справжнім аналогом. Після захоплення цілі за допомогою спуфера можливо поступово проводити підміну реального розміщення цілі шляхом зміни координат, що передаються.

Вдала атака можлива, тільки якщо спуфер виконав всі особливості стандарту відповідної GNSS, опрацював сигнали та передав їх до антени цілі. Як наслідок, звичайно, виникає затримка, яка не може бути більша ніж декілька наносекунд, тому спуфер повинен компенсувати ці затримки, випромінюючи сигнал, в якому час зміщений у майбутнє відносно сигналу, який він отримує. Для цивільних сигналів GPS це є тривіальним завданням, тому що сигнал, що передається, незашифрований і відомий алгоритм кодування, супутники пересуваються по фіксованих орбітах і передають дані відповідно до стандартів.

Для кожного *i*-го GPS супутника загальна затримка відстані еквівалентної системи, яка повинна бути компенсована, розраховується за формулою:

$$cd_i = r_{si} - r_{ti} + c(d_{RX} + d_{TX} + d_s) + |\Delta r_t - \Delta r_{TX}|, \quad (1)$$

де $\boldsymbol{d_{RX}}$ і $\boldsymbol{d_{TX}}$ є, відповідно, затримки сигналу в кабелях антен приймача і передавача, $\boldsymbol{d_s}$ − затримка обробки сигналу спуфером, $\boldsymbol{c}$ − швидкість світла. Відстані $\boldsymbol{r_{si}}$ і $\boldsymbol{r_{ti}}$ легко обчислюються за допомогою даних, що передаються супутниками, обчислення проводяться миттєво, оскільки спуфер знає положення кожного супутника, місце розташування власної приймальної антени та відносні координати $\boldsymbol{\Delta r_t}$ цілі. Затримки $\boldsymbol{d_{RX}}$ і $\boldsymbol{d_{TX}}$ легко обчислюються з наносекундною точністю для кабелів відомих довжин і стандартних типів. Для представленого методу спуфінгу обчислення $\boldsymbol{d_s}$ є більш складним, за рахунок виникнення затримка при роботі алгоритмів та буферизації даних. Щоб подолати цю затримку, одноразово проводять калібрування за допомогою опорного сигналу, що подається на вхід приймача спуфера та заміряється час до початку отримання сигналу з виходу передавача спуфера, при цьому спуфер має функціонувати в режимі ретранслятора. Також проводиться калібрування за допомогою переміщення спуфера, при цьому порівнюються передані та отримані дані в один момент часу, приблизно $\boldsymbol{d_s}$ становить 5 мс, в межах декількох наносекунд.

Для генерування фальшивих сигналів кожного і-го супутника спуфер має обчислювати для кожного сигналу:

1) три координати розміщення в просторі на момент часу отримання даних антеною цілі (зміщення значення часу в майбутнє) − модульоване значення навігаційних даних;

2) зміщення частоти за ефектом Допплера.

Ці прогнозовані дані опираються на швидкість переміщення супутників (прогнозована позиція супутника) і синхронізації годинника реального часу спуфера. Типова швидкість і прискорення БПС(А) досить малі, тому немає необхідності прогнозувати рух цілі, поточної оцінки $\boldsymbol{\Delta r_t}$ і її похідної за часом буде достатньо для вирівнювання частоти сигналу, яку передає спуфер на антену цілі.

2. Захоплення навігаційної системи

Навігаційна система БПС(А) вважається захопленою за допомогою GPS спуфера, коли спуфер диктує БПС(А) його розміщення на рівні шестимірного фазового простору та швидкості (ПШ) з оцінкою $\hat{x} = \left[\hat{r}^T; \hat{v}^T\right]^T$. Також при спуфінзі буде отримано контроль над частотою оновлення даних із супутників $\boldsymbol{\delta t}$, але основна увага буде приділятися саме контролю $\hat{r}$ і $\hat{v}$. У цьому контексті слово "контроль" використовується для опису генерації сили $\hat{x}$, що призводить до переміщення БПС(А) в просторі до запропонованих спуфером координат у межах точності GPS позиціонування, яка на цей час має похибку ±3 м в просторі та 10 см/с у швидкості, за умови що приймач має доступ лише до служби звичайного місцезнаходження (Standard Positioning Service (SPS) [4].

Стан захоплення спуфером доречно розглядати як аналог нелінійного контролю стабільної системи в розрізі ПШ: при початковому положенні $\hat{x}(t_0)$ після підміни буде існувати $t_1 > t_0$ і йому буде відповідати $\hat{x}(t_1) = x^*$. Значення t_1 обмежене в динаміці, тобто не може бути набагато більше, ніж значення t_0, оскільки БПС(А) порівнює дані, отримані з GPS навігації, з даними не GPS навігаційних датчиків. Захоплення навігаційної системи передбачає, що спуфер отримав контроль над цільовим GPS-приймачем і над періодом оновлення координат цього приймача, і в межах цих обмежень передає навігаційні дані, кожен цикл передачі виконується GPS-приймачем БПС(А) [3].

Обмежений варіант повного захоплення відбувається, коли спуфер може тільки контролювати $\hat{\chi}$ з m<6-мірним фазовим ПШ. Зокрема, БПС(А) навігаційна система може ігнорувати положення GPS навігації у вимірюванні швидкостей у вертикальному напрямку, покладаючись виключно на висотомір. Такий вид захоплення розглядається як підсистеми більш великої некерованої системи.

Доцільність розробки системи повного або часткового захоплення вимагає, щоб більшість видів піддавалися спуфінгу. Ця умова виконується для більшості, яка оснащена приймачем при роботі в активному режимі GPS навігації, оскільки, як правило, оцінка стану розміщення БПС(А) датчиками не GPS навігації здійснюється у разі неможливості отримання координат GPS. Це стосується таких систем: з інерційними датчиками, з магнітометрами, з барометричними висотомірами із електрооптичною навігацією на основі пошукової одночасної локалізації і відображення. Тільки системи останнього типу, які суворо обмежують похибки при отриманні координат з GPS, або системи, які орієнтуються по завантаженій карті з високою роздільною здатністю, будуть захищенні від спуфінгу.

Таким чином, слід очікувати, що більшість систем БПС(А) не будуть захищені і піддаватимуться керуванню за допомогою спуфера.

2.1 Неприховане захоплення

У неприхованому захопленні спуфер не робить жодних спроб приховати свою спробу підпорядкувати собі цільову систему. Отже, спуферу не потрібно вирівнювати свої змодельовані сигнали з їх справжніми відповідними сигналами з супутників GPS навігації на цільовий приймач на початку атаки; він може замість цього просто заглушити смуги частот цільового GPS супутника, в результаті чого приймач вимкне блокування і спроби повторного придбання всіх сигналів. Після такого заглушення спуфер успішно отримує контроль над цільовим GPS приймачем, якщо його змодельовані сигнали надходять з достатньою силою, якщо вони перевищують встановлений поріг чутливості, і потужність справжніх сигналів нижче від порогу чутливості, поріг чутливості цільового приймача змінюється під дією передавача спуфера як наслідок роботи автоматичного регулювання підсилення (АРП) цільового приймача. Нехай $\eta = \frac{P_s}{P_a}$ – число, яке відповідає за можливість приймання сигналу спуфера цільовим приймачем, або відношення потужності P_s отриманого від спуфера сигналу до потужності сигналу P_a, який відповідає рівню чутливості приймача. Експерименти з різними типами приймачів показують, що $\eta = 10\,dB$ досить, щоб задовольнити ці умови.

Також для спуфера необхідно вирівняти імітацію стану x^* з істинним станом x або по-іншому стан ПШ $\hat{x} \approx x$ для відвертого захоплення. Далі спуфер забезпечує поступовий перехід і переміщення цілі в заплановане місце простору. Однак у деяких БПС(А) різкий перехід прийнятний, оскільки упродовж тривалого часу система навігації цілі не отримувала інформації, тому не визначала свого місцезнаходження.

2.2 Приховане захоплення

У прихованому захопленні передбачається, що навігаційна система БПС(А) оснащена засобами виявлення спуфінгу. Спуфер для позитивного результату

атаки повинен своїми діями не ініціювати заходи виявлення спуфінгу. Як зазначалося у вступі, постійний розвиток БПС(А) спровокував появу методів виявлення підміни. Однак ці методи далекі від широкого застосування, і деякі з них занадто дорогі в реалізації або важкі для практичного використання на БПС(А). Захоплення навігаційної системи буде вважатися прихованим, якщо спуфер задовольняє всі умови для неприхованого захоплення й ухиляється від наступних методів виявлення: аналізатор відношення заглушення/шум (J/N), вбудований у приймач GPS, аналізатор частоти зміни оновлення координат, вбудований у приймач GPS, та метод оцінки стабільності роботи та отримання даних GPS приймачем. Нижче наводиться короткий опис методик виявлення спуфінгу. Уникнення простих стратегій виявлення підміни, таких як моніторинг інформаційних біт даних про шум та автономний контроль цілісності стандартного приймача також буде вважатися прихованим захопленням, але вони згадуються лише побіжно, враховуючи, що вони не становлять проблеми для інтелектуального спуфера [5].

2.3 Протидія спуфінгу

Аналізатор відношення заглушення/шум J/N видає сигнал тривоги, коли потужність сигналу, яка виникає в деякій смузі частот, значно перевищує звичайну потужність в цій смузі пропускання. Кілька комерційних приймачів, включаючи ublox Lea-6N, тепер пропонуються з J/N моніторингом. J/N моніторинг може виконувати роль детектора спуфінгу, якщо потужність, яка приймається від спуфера, перевищує поріг спрацьовування, також коли приймач продовжує відстежувати сигнали GPS при великих коефіцієнтах відношення несучої до шуму, незважаючи на згадану перешкоду. Таким чином, з точки зору спуфінгу, для уникнення J/N моніторингу потрібно обмежувати та контролювати потужність сигналу, що передає спуфер. Для u-blox Lea-6N в конфігурації за замовчуванням, лабораторні тести показали, що збереження $\eta = 12\,dB$ на всі підмінні сигнали досить, щоб уникнути спрацювання J/N моніторингу.

Використання J/N моніторингу також запобігає атаці з попереднім глушінням сигналів, що згадане в попередньому розділі. Без цієї опції спуфер повинен вдатися до більш складної атаки, відповідно, щоб отримати контроль над цільовим БПС(А).

Розблокування частоти моніторінгу в приймачеві GPS може бути ефективною стратегією виявлення підміни, тому що відповідно в середовищі без завади спуферу, розблокування частоти відбувається дуже рідко, за винятком випадків блокування сигналу або важкої іоносферної сцинтиляції і воно є складним завданням для спуфера, щоб запобігти розблокуванню частоти під час захоплення вихідного контуру відстеження, оскільки це вимагає точного знання про швидкість цільового БПС(А). Фаза розблокування, більш чутливе відстеження аномалії також є ефективним показником підміни, але не розглядається, тому що це відбувається занадто часто в середовищі без спуфера.

Інноваційне тестування використовується для більш стабільної роботи навігаційної системи цільового БПС(А). Використання цього методу легко реалізує захист від підміни. Підміна навігаційних даних виявляється системами захисту БПС(А) при захопленні, якщо дані ПШ від приймача GPS не відповідають даним ПШ не GPS навігаційної системи БПС(А). Чутливість виявлення підміни

залежить від якості цих датчиків. Більш стабільні датчики, наприклад, призводить до поліпшення чутливості.

Висновки

З широким розповсюдженням БПС(А) на території України існує загроза використання їх для вчинення протиправних дій. Тому застосування технологій перехоплення керування та, як наслідок, фізичного захоплення БПС(А) є пріоритетною темою і має бути використане в роботі органами виконавчої влади, діяльність яких спрямовується та координується Кабінетом Міністрів України через Міністра внутрішніх справ України.

Описані методи дозволять протидіяти БПС(А) під час антитерористичних операцій, охорони особливо важливих об'єктів, державного кордону та ін.

Також описані методи протидії спуфінгу можуть бути використані під час проектування БПС(А), які будуть використовуватися правоохоронними структурами для виконання поставлених перед ними завдань. Це зменшить можливість витоку інформації та збільшить відсоток позитивно завершених операцій, під час виконання яких будуть використовуватися БПС(А).

Отже, застосування описаних методів протидії БПС(А) та захист від спуфінгу на цей час є пріоритетним напрямом досліджень у сфері боротьби з тероризмом.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Kendoul, F.* (2012). Survey of advances in guidance, navigation, and control of unmanned rotorcraft systems. Journal of Field Robotics, 29(2):315–378.

2. *Chowdhary, G., Johnson, E. N., Magree, D., Wu, A., and Shein, A.* (2013). GPS-denied indoor and outdoor monocular vision aided navigation and control of unmanned aircraft. Journal of Field Robotics, 30(3):415–437.

3. *Humphreys, T. E., Ledvina, B. M., Psiaki, M. L., O'Hanlon, B.W., and Kintner, Jr., P. M.* (2008). Assessing the spoofing threat : development of a portable GPS civilian spoofer. In Proceedings of the ION GNSS Meeting, Savannah, GA. Institute of Navigation.

4. *Misra, P. and Enge, P.* (2012). Global Positioning System : Signals, Measurements, and Performance. Ganga-Jumana Press, Lincoln, MA, revised second edition.

5. *Shepard, D. P., Humphreys, T. E., and Fansler, A. A.* (2012b). Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks. International Journal of Critical Infrastructure Protection, 5(3-4):146–153.

Отримано 22.05.2017
Рецензент Циганов О.Г., к.т.н.