УДК 621.391.8

Р.В. Сергієнко

Академія сухопутних військ імені гетьмана Петра Сагайдачного, Львів

АНАЛІЗ СУЧАСНИХ МЕТОДІВ ПОРУШЕННЯ РОБОТИ АПАРАТУРИ КОРИСТУВАЧА СУПУТНИКОВИХ РАДІОНАВІГАЦІЙНИХ СИСТЕМ ТА МОЖЛИВІ ШЛЯХИ ЇХ ВИЯВЛЕННЯ

Проаналізовано загрози, які можуть привести до порушення нормальної роботи апаратури користувача супутникових навігаційних систем та істотних помилок у відпрацюванні ними навігаційної інформації. Наведено шляхи виявлення атак зловмисників з метою недопущення використання невірної інформації.

Ключові слова: *супутникова навігація, заглушування сигналу, фальсифікація сигналу, навігаційна інформація.*

Вступ

Постановка проблеми. Навігаційна інформація, отримана апаратурою користувачів супутникових радіонавігаційних систем (СРНС), дедалі активніше використовуються у різних сферах діяльності людини, у тому числі у системах, що забезпечують керування посадкою літаків, керування транспортними засобами, роботою базових станцій стільникового зв'язку, визначення місць пошкоджень силових електромереж тощо. У військовій сфері супутникові навігаційні приймачі використовуються для визначення місцеположення та точного часу [2]. Програмне забезпечення апаратури користувачів СРНС стає дедалі складнішим та багатофункціональним. Аналіз наведених у відкритих джерелах результатів досліджень свідчить, що це обумовлює значну уразливість цих систем до потенційних атак зловмисників. Тому питання захисту навігаційної інформації не повинно бути поза увагою розробників та користувачів приладів, залежних від систем глобального позиціонування.

Аналіз останніх досліджень і публікацій. Питання безперебійного забезпечення навігаційною інформацією останнім часом досить активно обговорюється у відкритих джерелах інформації. Однією з найбільш докладних публікацій результатів своїх досліджень є стаття «Атаки на програмне забезпечення GPS» (GPS software attacks) [1]; в цій роботі запропоновано класифікацію відомих загроз функціонуванню приймачів СРНС, проаналізовано можливі причини їх уразливості. Опубліковано роботи, в яких запропоновано криптографічну аутентифікацію цивільного С/А-сигналу [3], інші засоби протидії фальсифікації цього сигналу [4], [5]. Однак необхідно зазначити, що запропоновані в цих роботах заходи більшою мірою орієнтовані на архітектуру та програмне забезпечення супутникових навігаційних систем у цілому, а також частково – на виробника апаратури користувача СРНС. Тому актуальним є пошук шляхів виявлення факту здійснення атаки безпосередньо особами, які використовують приймачі супутникової навігаційної інформації, а також ефективних та малозатратних модернізацій виробниками цих приймачів.

Формулювання мети статті. Метою статті обрано аналіз основних загроз коректній роботі засобів супутникової навігації від атак зловмисників чи природних явищ, що впливають на розповсюдження електромагнітних хвиль у діапазоні, який використовують СРНС, а також визначення заходів, які допоможуть користувачам виявити некоректну роботи приймача інформації від СРНС.

Виклад основного матеріалу

Відповідно до відкритих джерел, найбільшого успіху в оцінці нових загроз та вразливостей вдалося досягти дослідникам з університету Карнегі-Меллон та компанії Coherent Navigation (США). За результатами своєї роботи було опубліковано статтю «Атаки на програмне забезпечення GPS» [1], де автори звернули увагу на зростання ролі програмної компоненти у функціонуванні супутникових навігаційних систем, дали класифікацію загроз та атак. Відповідно до поданої класифікації, розглянуті ними під час дослідження атаки можна поділити на наступні групи [1].

1. Атаки на рівні даних: ці атаки подібні до спуфінгу (перехват сигналу та передача його у зміненому вигляді непомітно для користувача), але можуть завдати шкоди високотехнологічним приймачам навігаційної інформації.

2. Атаки на програмне забезпечення приймача навігаційної інформації GPS: небезпечні тим, що підвищують рівень привілеїв користувача та дозволити доступ до конфіденційної інформації;

3. Атаки на GPS-залежні системи: використовують той факт, що ці системи сприймають надану GPS-інформацію як інформацію достовірного джерела.

Для цього застосовувались наступні прийоми [1, 3, 4]:

- фальсифікація даних про параметри орбіт навігаційних супутників;

- передача спотвореної інформації про дату та час;

- атака на системне програмне забезпечення;

а також раніше відомі атаки:

- фальсифікація сигналу – псевдовипадкового коду (спуфінг – spoofing);

- заглушка сигналу (джаммінг – jamming).

Як приклад останнього можна зазначити факт його використання кримінальними бандами для блокування протиугінних систем на базі GPS-навігації.

Відомий також інцидент з використанням заглушування GPS-сигналу Північною Кореєю проти Південної. Було не тільки унеможливлено морську навігацію, а й роботу базових стацій стільникового зв'язку, деяких військових систем.

Цікавий і той факт, що для виготовлення необхідного апаратного забезпечення для здійснення атак використано складові, які виробляються серійно (апаратура імітації GPS-сигналів); їх вартість приблизно дорівнює вартості ноутбука [1]. В ході описаного в [1] експерименту було з'ясовано, що з семи пристроїв, які залучалися до перевірки, кожен з них був уражений як мінімум двома видами атак.

Необхідно зазначити, що подібну апаратуру імітації сигналів СН-3810 виробляє вітчизняне Державне підприємство "Оризон-навігація", м. Сміла Черкаської області. Ця апаратура дозволяє формувати радіочастотний сигнал, що імітує навігаційне поле повного сузір'я космічних апаратів ГЛОНАСС (Росія), GPS (США) та GALILEO (загальноєвропейська система), при чому передбачена можливість моделювати рух приймача навігаційної інформації [6].

В умовах сьогодення неприпустиме сприйняття приймача навігаційного сигналу як пристрою, а не як комп'ютера: тобто ігнорування можливості розробки та встановлення «патчів» у відповідь на виявлені загрози [8, 9]. Характерним прикладом використання «лазівок» у програмному забезпеченні є присвоєння нульового значення довжині *A* великої півосі орбіти супутника у навігаційному повідомленні, що є складовою частиною навігаційного сигналу супутника.

У процесі обчислень приймач розраховує середній рух супутника за формулою

$$n_0 = \sqrt{\frac{\mu}{a^3}}$$

де м – гравітаційна константа для системи WGS-84, $a = \left(\sqrt{A}\right)^2$ – значення, що залежить від довжини А великої півосі орбіти супутника.

Після помилки ділення на нуль система перевантажується, однак для повторення обчислень використовує дані з кешу (пам'ять для забезпечення «гарячого» старту приймача), де знаходяться ті ж помилкові дані. Це призводить до нескінченного циклу перевантажень [1].

Іншим прикладом є атака де-синхронізації дати. Вона використовує особливість представлення приладом дати. При цьому використовується номер тижня, що займає 10 біт у навігаційному повідомленні. Поступово змінюючи номер тижня від більшого до меншого, досягають зміни дати початку епохи номерів тижня, фальсифікуючи дату майже на 20 років. Це виводить прилади з ладу, оскільки повернення дати початку епохи у «минуле» є неможливим [1].

Перелік загроз не обмежується наведеними вище атаками; кожна з цих атак може уразити лише окремі зразки приймачів, програмне забезпечення яких не виконує перевірок вхідних даних, що надходять від супутника.

Наведені вище загрози говорять про актуальність підвищення захищеності навігаційних систем від розглянутих кібер-атак. Першими кроками для виробників навігаційних приймачів може стати наступне: ретельна розробка програмного забезпечення з застосуванням обмежень, які б унеможливлювали прийняття явно невірних даних у якості достовірних [1] (наприклад, велика піввісь орбіти супутника не може дорівнювати нулю); передбачення виробниками можливості самостійного оновлення користувачами програмного забезпечення; використання ретрансляторів істинного сигналу для приймачів навігаційної інформації. Одним з шляхів запобігання подібним атакам є комплексування навігаційних систем: автономних систем та приймачів супутникової навігаційної інформації, а також удосконалення системи, що корегує налаштування вбудованого пристрою збереження часу приймача відповідно до інформації, отриманої з супутника, з метою недопущення введення неадекватних поправок до часу внутрішнього годинника.

Одним з видів боротьби з заглушкою чи втратою сигналу є встановлення радіомаяків – по типу псевдосупутників. Подібна система «eLoran» встановлюється в Великобританії, її призначення – забезпечення навігації у Дуврській протоці [9].

Що ж можна порекомендувати користувачу, що має на озброєнні навігаційний приймач типу СН-3003 «Базальт», СН-3003М «Базальт-М», чи інший доступний зразок? Ефективним шляхом виявлення прийняття до обробки даних від імітатора навігаційного сигналу є відстеження його потужності [4]. В реальних умовах розташування потужність сигналів від навігаційних супутників не буде сталою величиною, це обумовлено наявністю пе-

решкод, змінами значень затримок проходження сигналу через шари атмосфери. В більшості приймачів передбачено режим роботи, в якому у вигляді гістограми відображаються потужності сигналів супутників. Сигнал від супутників, висота (кут піднесення) яких є незначною (≈15-35°), є менш потужним. Апаратура імітації формує однаково потужний сигнал для всіх супутників, і якщо користувач спостерігає незмінно потужні сигнали незалежно від умов місцевості, то це з високою імовірністю означає проведення атаки фальсифікації сигналів супутників [4].

Найбільш доступним шляхом виявлення фальсифікації сигналу може стати «комплексування» отриманої навігаційної інформації з даними, що користувач з'ясував під час орієнтування по карті. При діях на рівнинній місцевості необхідно звіряти значення висоти, зняте з карти, зі значенням, обчисленим приймачем навігаційної інформації. Розбіжність у значеннях не повинна перевищувати величини, зазначеної у технічних характеристиках приладу в даних умовах роботи, з урахуванням похибки визначення висоти по карті. При наявності двох та більше приймачів один з них необхідно встановити на пункті з достовірно відомими координатами та слідкувати за величиною розходження координат, отриманих приймачем, та істинних координат пункту.

Враховуючи можливість користувача виявити фальсифікований сигнал за його потужністю чи відношенням сигнал-шум, імітатор сигналів навігаційних супутників можна налаштувати також і на імітацію зміни цих показників, тобто штучно довільним чином змінювати потужність імітатора. У цьому випадку доцільно спробувати визначити напрям на джерело сигналу і порівняти його з очікуваним положенням супутника. Це можна реалізувати із застосуванням відбиваючих чи екрануючих поверхонь.

Розглянемо можливість розрізнити хибний сигнал від істинного порівнянням прямого та відбитого сигналу за умови використання відбиваючої поверхні. Результати обчислень координат антени СРНС-приймача будуть відрізнятися зі зміною взаємного розташування навігаційного супутника, антени та відбивача [7].

Аналіз результатів обчислення місцеположення при різних варіантах розташування антени та відбивача дадуть змогу визначити напрям на джерело сигналу та зробити висновок про його істинність. Необхідно зазначити, що поряд з просторовими методами врахування багатошляховості значна кількість виробників широко використовує методи цифрової кореляційної обробки сигналів. Вони дозволяють виявити відбитий сигнал та відкинути його. Подібні технології можна використати для виявлення хибного сигналу. Оскільки вплив наявності відбиваючої поверхні на визначення координат антени приймача не є значним, – за віддалі поверхні від антени 2-3 м спотворення координат сягає лише 4-7 мм, – його можна використовувати тільки при виконанні високоточних вимірів.

Продовжуючи тему впливу аналізу розповсюдження сигналів, необхідно згадати дослідження способу визначення азимута з використанням екрануючої поверхні [10].

Його сутність полягає у обертанні екрануючої поверхні навколо антени приймача навігаційних сигналів та вимірюванні при цьому рівня сигналу (рис. 1).

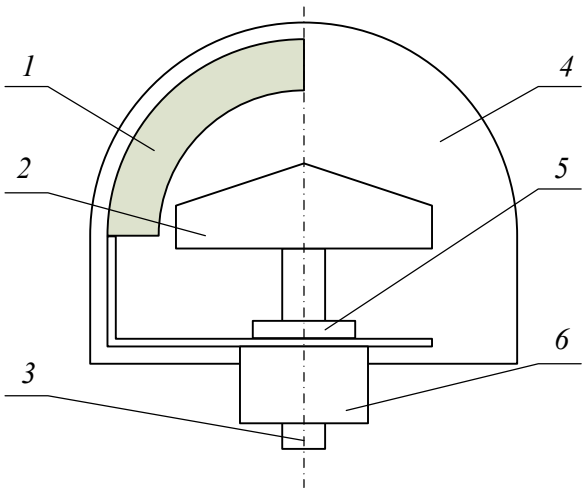

Рис. 1. Загальна будова пристрою виміру азимута супутника (Kahlmann, Ingensand, – 2007):
1 – екрануюча поверхня; 2 – антена приймача навігаційних сигналів; 3 – вертикальна вісь; 4 – радіопрозорий корпус; 5 – пристрій кодування кута повороту; 6 – двигун обертання екрануючої поверхні

Відповідно до положення екрану, при якому потужність прийнятого сигналу мінімальна, можна зробити висновок про азимут напряму на супутник та порівняти його з азимутом, обчисленим відповідно до ефемерид супутника. На рис. 2 приведено графік залежності рівня прийнятого сигналу від кута повороту екрануючої поверхні, отриманий в результаті експериментальних досліджень [10]. Порівняння рівнів опорного та прийнятого сигналів дає змогу визначити напрям на джерело сигналу.

Перелічені вище шляхи дозволяють виявити факт фальсифікації навігаційного сигналу. Заглушування ж повністю унеможливлює прийом навігаційної інформації, і у цьому випадку відновити його можна відшуканням та виведенням з ладу приладу для заглушування. Локацію джерела заглушувального сигналу можна здійснити за допомогою різницево-фазової системи.

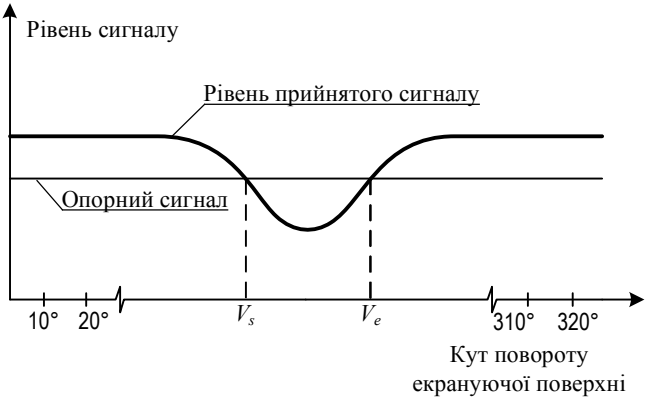

Рис. 2. Рівень прийнятого сигналу як функція кута обертання екрану навколо вертикальної осі GPS-антени (Wiklund – 1992)

Наприклад, може бути використаний фазовий детектор типу AD8302. Це – широкосмуговий детектор сигналів з функцією визначення амплітуди та фази, який працює у діапазоні частот до 2,7 ГГц і забезпечує нелінійність фазового детектування не більше, ніж 1 град у діапазоні від 30 до 140°. При цьому рівень вхідного сигналу – 60,0 дБ, діапазон вимірюваної різниці фаз ±90°, діапазон вихідних напруг - 0..1,8 В і крутизна характеристики – 10 мВ/°.

Висновки

Таким чином, реалії сьогодення вимагають розробки підходів щодо захисту інформації, що використовується супутниковими навігаційними системами. Крім технічних заходів, що пропонується вжити виробникам, користувачам необхідно зважено підходити до прийняття рішення щодо достовірності даних, отриманих приймачем навігаційної інформації, використовуючи наведені у цій роботі підходи.

Список літератури

1. GPS Software Attacks / T. Nighswander, B. Ledvina, J. Diamond, R. Brumley, D. Brumley. – CCS'12, October16–18,2012, Raleigh, NorthCarolina, USA.

2. Навігація основи визначення місцеположення та скеровування / Б. Гофманн-Велленгоф, К. Легат, М. Візер, Пер. з англ. за ред. Я.С. Яцківа. – Львів: Львівський національний університет імені Івана Франка, 2006. – 443 с.

3. Practical Cryptographic Civil GPS Signal Authentication. Kyle Wesson, Mark Rothlisberger, Todd Humphreys – NAVIGATION, Journal of the Institute of Navigation, Vol 59, Num 3, 2012, pp 177-193; [Електронний ресурс]. – Режим доступу до журналу: http://chromium.ae.utexas.edu/images /stories/files/papers/nma.pdf.

4. GPS Spoofing Countermeasures. Jon S. Warner, Ph.D. Roger G. Johnston. [Електронний ресурс] . – Режим достпупк: http://lewisperdue.com/ DieByWire/GPS-Vulnerability-LosAlamos.pdf.

5. On the Requirements for Successful GPS Spoofing Attacks. Nils Ole Tippenhauer, Christina Popper, Kasper B. Rasmussen, Srdjan Capkun. [електронний ресурс] http://www.syssec.ethz.ch/ research/ccs139-tippenhauer.pdf.

6. Кривов'яз А.Т. Створення і виробництво супутникової навігаційної апаратури ДП «Оризон-Навігація» / А.Т. Кривов'яз. – X Міжнародна науково-технічна конференція "ABIA-2011".– К.: 2011.

7. Глотов В. Оцінка впливу багатошляховості поширення GPS-сигналів на точність визначення координат об'єктів / В. Глотов, К. Третяк, О.Полець. Сучасні досягнення геодезичної науки та виробництва: Збірник наукових праць Західного геодезичного товариства УГГК. – Львів: НУ «ЛП» - 2007. – С.103-108.

8. «Ахиллесова пята» системы GPS. [Електронний ресурс]. – http://www.ixbt.com/news/soft/index.shtml?16/40/85.

9. M. Tolentino. GPS Still Vulnerable To Attacks Show Researchers at University of Texas [електронний ресурс] http://siliconangle.com/blog/2012/12/15/gps-still-vulnerable-to-attacks-show-researchers-at-university-of-texas/.

10. David Grimm. GPS direction finding. – 2nd Baltic Swiss Geodetic Science Week, Lithuania – 2007.

Надійшла в редколегію 21.01.2013

Рецензент: д-р техн. наук, проф. О.О. Кузнецов, Харківський національний університет радіоелектроніки, Харків.

АНАЛИЗ СОВРЕМЕННЫХ МЕТОДОВ НАРУШЕНИЯ РАБОТЫ АППАРАТУРЫ ПОЛЬЗОВАТЕЛЯ СПУТНИКОВЫХ РАДИОНАВИГАЦИОННЫХ СИСТЕМ И ВОЗМОЖНЫЕ ПУТИ ИХ ОБНАРУЖЕНИЯ

Р.В. Сергиенко

Проанализированы угрозы, которые могут привести к нарушению нормальной работы аппаратуры пользователя спутниковых навигационных систем и существенных ошибок в отработке ними навигационной информации. Приведены пути выявления атак злоумышленников с целью недопущения использования неверной информации.

Ключевые слова: *спутниковая навигация, заглушка сигнала, фальсификация сигнала, навигационная информация.*

ANALYSIS OF MODERN METHODS OF GPS RECEIVER FUNCTIONING VIOLATION AND POSSIBLE WAYS OF THEIR DETECTION

R.V. Serhiienko

Possible threats which can cause incorrect functioning of GPS receiver and information handling errors are analyzed. The possible ways of attack detection and prevention of incorrect information use are given.

Keywords*: satellite navigation, jamming, spoofing, navigational data.*