Scientific Journals
Maritime University of Szczecin

Zeszyty Naukowe
Akademia Morska w Szczecinie

2014, 37(109) pp. 28–33
ISSN 1733-8670

2014, 37(109) s. 28–33

Применение спутникового компаса для обнаружения ГНСС-спуфинга

The application of satellite compass for GNSS-spoofing detecting

Larisa Dobryakova[1], Łukasz Lemieszewski[2], Eugeniusz Lusznikov[2], Evgeny Ochin[2]

[1] West Pomeranian University of Technology, Faculty of Computer Science and Information Technology
71-210, ul. Żołnierska 49, e-mail: ldobryakova@wi.zut.edu.pl
[2] Maritime University of Szczecin, Faculty of Navigation
70-500 Szczecin, ul. Wały Chrobrego 1–2, e-mail: e.ochin@am.szczecin.pl

Ключевые слова: спуфер, спуфинг, ГНСС, компас

Резюме
В статье рассматривается новый подход к детектированию ГНСС-спуфинга, основанный на применении спутникового компаса. Сравниваются результаты измерения ГНСС-приёмников компаса в двух режимах (в режиме нормальной ГНСС-навигации и в режиме спуфинга). Исследования показали, что в режиме спуфинговой атаки в обоих приёмоиндикаторах спутникового компаса имеет место равенство полученных координат, что в свою очередь в алгоритме определения координат порождает математическую неопределённость вида 0/0. Это означает выход из рабочего состояния спутникового компаса, что может быть использовано в качестве сигнал тревоги "спуфинговая атака" для принятия соответствующих мер безопасности ГНСС-навигации.

Key words: spoofer, Spoofing, GNSS, compass

Abstract
The article discusses a new approach to the detection of GNSS spoofing, based on the use of satellite compass. Comparing the results of measurements of GNSS receivers of compass in two modes (normal mode of GNSS navigation and spoofing mode). The studies have shown, that in mode of spoofing attacks in both receivers of satellite compass we have the equality of coordinates, which in algorithm coordinate definitions, determine mathematical indeterminate form 0/0. This means getting out of the operating status of the satellite compass that can be used as an alarm "spoofing attack" to take appropriate security measures of GNSS navigation.

Основные обозначения (рис. 1) и определения

ГНСС – Глобальная Навигационная Спутниковая Система[1].

(x_0, y_0, z_0) – неизвестные координаты судна в пространстве.

Позиционирование – определение (оценка) неизвестных координат судна (x_0, y_0, z_0).

(x', y', z') – неизвестные координаты первой антенны компаса.

(x'', y'', z'') – неизвестные координаты второй антенны компаса.

[1] Так как Россия, Европейский союз, Индия, Китай и Япония разрабатывают собственные системы спутникового позиционирования, то в международных документах все системы получили аббревиатуру – GNSS (Global Navigation Satellites System – Глобальная Навигационная Спутниковая Система). Американская система NAVSTAR стала GPS NAVSTAR или чаще просто GPS.

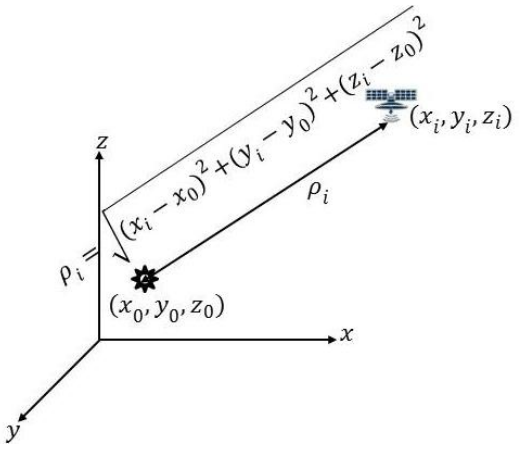

Рис. 1. Основные обозначения

(x_i, y_i, z_i) – известные координаты i-го навигационного спутника ($i = \overline{1, N}$).

$N_{\min} = 4$ – наименьшее количество навигационных спутников, достаточное для оценки координат судна.

ρ_i – неизвестные расстояния от i-го навигационного спутника до судна.

$\hat{\rho}_i$ – оценка расстояния от i-го навигационного спутника до судна (псевдодальности).

t'_i – известное точное время излучения ГНСС-сигнала от i-го навигационного спутника (по точным атомным часам космического аппарата).

t''_i – неизвестное точное время приема ГНСС-сигнала от i-го навигационного спутника ГНСС-приёмником.

$\hat{t}''_i$ – оценка времени приема ГНСС-сигнала от i-го навигационного спутника ГНСС-приёмником (по неточным кварцевым часам ГНСС-приёмника).

$\hat{t}''_i = t''_i + \varepsilon$, где ε – неизвестная систематическая ошибка измерения времени ГНСС-приёмником, постоянная на время приема ГНСС-сигналов от N навигационных спутников[2].

c – скорость света.

Эфемерида – спрогнозированные параметры орбиты и их производные.

Альманах – набор сведений, о текущем состоянии навигационной системы в целом, включая загрублённые эфемериды применяемые для поиска видимых спутников и выбора оптимального созвездия и содержащих сведения.

Навигационные сообщения – передаваемые спутником пакетные данные, содержащие эфемериду с метками времени и альманахом.

[2] Ошибка определения времени в 1 мкс приводит к ошибке определения расстояния в 300 м.

Опираясь на введённые обозначения и определения, можно записать:

$\rho_i = (t''_i - t'_i)\, c = \sqrt{(x_i - x_0)^2 + (y_i - y_0)^2 + (z_i - z_0)^2}$
$i = \overline{1, N}$;

$\hat{\rho}_i = (\hat{t}''_i - t'_i) \cdot c,\ i = \overline{1, N}$

$\varepsilon = \hat{t}''_i - t''_i,\ i = \overline{1, N}$ – неизвестная систематическая ошибка измерения времени ГНСС-навигатором, постоянная на время приема ГНСС-сигналов от N навигационных спутников;

$\rho_i = \hat{\rho}_i + \varepsilon = (\hat{t}''_i - t'_i) \cdot c + \varepsilon,\ i = \overline{1, N}$;

При $N = 4$ можно записать систему из четырех уравнений с четырьмя неизвестными (x_0, y_0,z_0, ε):

$$\sqrt{(x_1 - x_0)^2 + (y_1 - y_0)^2 + (z_1 - z_0)^2} = (\hat{t}''_1 - t'_1)c + \varepsilon$$
$$\sqrt{(x_2 - x_0)^2 + (y_2 - y_0)^2 + (z_2 - z_0)^2} = (\hat{t}''_2 - t'_2)c + \varepsilon$$
$$\sqrt{(x_3 - x_0)^2 + (y_3 - y_0)^2 + (z_3 - z_0)^2} = (\hat{t}''_3 - t'_3)c + \varepsilon$$
$$\sqrt{(x_4 - x_0)^2 + (y_4 - y_0)^2 + (z_4 - z_0)^2} = (\hat{t}''_4 - t'_4)c + \varepsilon$$

решением которой являются искомые координаты судна (x_0, y_0, z_0). Задача решается методом последовательных приближений. В реальных системах для увеличения точности позиционирования количество уравнений достигает нескольких десятков, при неизменном количестве неизвестных (x_0, y_0, z_0, ε).

Введение

ГНСС предназначены для определения местоположения, скорости движения, а также точного времени морских, воздушных, сухопутных и других видов потребителей. NAVSTAR и ГЛОНАСС – системы двойного назначения, изначально разработанные по заказу и под контролем военных для нужд Министерств обороны и поэтому первое, и основное назначение у систем стратегическое, второе назначение указанных систем гражданское[3]. Исходя из этого, все действующие ныне спутники передают два вида сигналов: стандартной точности для гражданских пользователей и высокой точности для военных пользователей (этот сигнал закодирован и доступен только при предоставлении соответствующего уровня доступа от Министерства обороны).

[3] GPS клуб – сообщество любителей и профессионалов в области GPS, ГЛОНАСС и ГНСС технологий; http://gps-club.ru/

ГНСС может быть задействована для наведения высокоточного оружия, десантирования грузов, ориентирования на местности, проведения разведывательно-диверсионных операций и как результат – серьезное преимущество в скорости и точности позиционирования перед противником, не имеющим собственных технологий спутникового позиционирования.

В ближайшие несколько лет США планирует вывести на орбиту новые модификации NAVSTAR GPS спутников (GPS-IIF, GPS-III) с новыми военными закрытыми сигналами M и L1C и гражданским открытым сигналом L5. Любая компания может заниматься разработкой двухчастотных L1/L5 GPS, при этом точность позиционирования L1/L5 GPS будет превышать точность позиционирования L1/L2 GPS.

Основной принцип ГНСС – это использование искусственных спутников Земли в качестве точек отсчета для вычисления координат на Земле на основе тригонометрических соотношений. Точное местоположение навигационных спутников известно из данных эфемерид и альманаха, передаваемых в навигационных сообщениях. Зная точные расстояния до трех спутников, можно определить текущее местоположение, как точку пересечения трех сфер. Существует множество причин, благодаря которым точные расстояния до спутников измерить невозможно, основным из которых является неточность хода часов ГНСС-приемника. Дополнительное четвертое измерение дает возможность исключить ошибку часов приемника. Зная приближенные оценки расстояний до четырех спутников, можно определить местоположение ГНСС-приемника, как точку наилучшего приближения к его точной позиции, т.е. необходимо иметь не менее четырех уравнений типа: „*расстояние равно произведению скорости света на разность момента времени приема ГНСС-сигнала ГНСС-навигатором и момента времени передачи ГНСС-сигнала от навигационных спутников*”.

Военная версия ГНСС-сигналов поддерживают аутентификацию, то есть ГНСС-приемники с помощью методов криптографии могут определить достовернсть принятого сигнала. Гражданская версия ГНСС имеет опасные уязвимости, которые однажды могут привести к серьезным последствиям. В то время как устройства для создания помех для ГНСС-сигнала и ГНСС-глушилки (джаммеры) становятся всё дешевле и доступнее, всё острее встаёт необходимость в защите важнейших элементов военной, гражданской и индустриальной инфраструктуры от действий злоумышленников. Технология спуфинга или подмены реальных ГНСС-сигналов искаженными или искусственно созданными с помощью имитаторов ГНСС-сигналов стала сегодня реальной угрозой для беспилотных систем навигации. Имитаторы ГНСС-сигналов выпускаются серийно и предназначаются для тестирования навигационных систем.

Одна из версий захвата американского беспилотника Lockheed RQ 170 в северо-восточном Иране в декабре 2011, это результат такой спуфинг-атаки[4]. Статья под названием „On the Requirements for Successful GPS Spoofing Attacks”, которую написали специалисты ETH Zurich (Швейцария, Eidgenössische Technische Hochschule Zürich) и UCI (США, University of California, Irvine), предлагает различные меры противодействия спуфингу [1].

Репитер сигналов ГНСС

Предположим, что репитер сигналов ГНСС, находящийся в точке (x_s, y_s, z_s), принимает, усиливает и транслирует с помощью передающей антенны сигналы ГНСС. Допустим также, что судно находится на расстоянии $\Delta\rho$ от репитера. Так как время распространения сигнала от репитера до судна $\Delta t = \Delta\rho/c$ представляет собой дополнительное смещение временной шкалы судна относительно системного времени, т.е. дополнительную систематическую погрешность измерения времени прохождения сигналов от спутников до судна, то в соответствии с системой уравнений (2.5) при $N = 4$ можно записать систему из четырех уравнений с четырьмя неизвестными $(x_0, y_0, z_0, \varepsilon')$, где $\varepsilon' = \varepsilon + \Delta\rho/c$

$$\begin{aligned}
\sqrt{(x_1 - x_s)^2 + (y_1 - y_s)^2 + (z_1 - z_s)^2} &= (\hat{t}_1'' - t_1')c + \varepsilon \\
\sqrt{(x_2 - x_s)^2 + (y_2 - y_s)^2 + (z_2 - z_s)^2} &= (\hat{t}_2'' - t_2')c + \varepsilon \\
\sqrt{(x_3 - x_s)^2 + (y_3 - y_s)^2 + (z_3 - z_s)^2} &= (\hat{t}_3'' - t_3')c + \varepsilon \\
\sqrt{(x_4 - x_s)^2 + (y_4 - y_s)^2 + (z_4 - z_s)^2} &= (\hat{t}_4'' - t_4')c + \varepsilon
\end{aligned} \tag{1}$$

решением которой являются координаты репитера (x_s, y_s, z_s). Это означает, что все суда, находящиеся в зоне действия репитера, имеют одинаковые результаты измерения своих

[4] Iran spy drone GPS hijack boasts: Rubbish, say experts. Internet Journal “The Register” http://www.theregister.co.uk/2011/12/21/spy_drone_hijack_gps_spoofing_implausible/

координат, то есть вместо реальных координат получают фальшивые координаты (x_s, y_s, z_s). Это означает также, что репитер сигналов ГНСС можно использовать в качестве спуфера с ограниченными возможностями.

Спутниковые компасы в современной навигации

Информация от системы ГНСС в значительной степени освободила судоводителя от рутинной работы по текущему определению места судна. Она позволяет так же контролировать параметры движения судна такие, как его скорость, ветровой дрейф, снос течением и множество других. Сфера применения приёмоиндикаторов системы ГНСС постоянно расширяется, позволяя решать различные навигационные, организационные и технические задачи.

Существенным шагом вперёд в вопросе использования системы ГНСС стала разработка спутниковых компасов. Спутниковые компасы в отличие от гироскопических не имеют скоростных и инерционных девиаций, а в отличие от магнитных компасов не зависят от земного и судового магнетизмов. Спутниковый компас готов к работе сразу же после включения, его точность меньше зависит от широты судна. Всё это очень существенные достоинства спутниковых компасов в сравнении с классическими типами компасов – гироскопическими и магнитными.

Главным недостатком спутниковых компасов является его неавтономность (зависимость от сигналов принимаемых со спутников системы ГНСС). Спутниковый компас ещё не является конвенционным прибором, обязательным для установки на морских судах, но он находит всё более и более широкое применение. Спутниковые компасы имеют в своей основе два приёмника типа ГНСС, ДГНСС или РТК. Линия, соединяющая антенны этих приёмников является опорной для определения курса судна через координаты, полученные с каждого из этих приёмников.

Систематическая погрешность координат каждого из этих приёмников не оказывает влияния на точность определения опорного направления и, как следствие, на точность курсоуказания. Использование фактически разностного метода позволяет исключить погрешностей скорости распространения радиоволны, погрешности измерения элементов орбиты и других систематических погрешностей. Увеличение расстояния между антеннами позволяет увеличивает точность компаса. На практике базовое расстояние между антеннами находится в диапазоне от 0,8 м до 4 м. По такой схеме построены, например, компасы фирмы Kongsberg типа Seate Seapath 200, 200 RTK (рис. 1).

Рис. 2. Конфигурация спутникового компаса

На рис. 3 представлена связь координат антенн первого и второго приёмоиндикаторов с истинным курсом (ИК) судна [2].

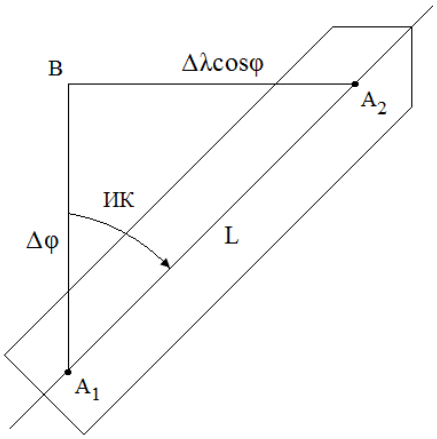

Рис. 3. Связь координат двух спутниковых антенн A_1 и A_2, расположенных в диаметральной плоскости судна. Источник [2]

Значение истинного курса можно рассчитать по одной из формул:

$$ИК = \operatorname{arctg}\frac{\Delta\lambda\cos\varphi}{\Delta\varphi}$$
$$ИК = \operatorname{arcctg}\frac{\Delta\varphi}{\Delta\lambda\cos\varphi} \quad (2)$$

где:

$\Delta\lambda = \lambda_2 - \lambda_1$

$\Delta\varphi = \varphi_2 - \varphi_1$

Можно воспользоваться для определения истинного курса и другими выражениями:

$$ИК = \arccos\frac{\Delta\varphi}{L}$$
$$ИК = \arcsin\frac{\Delta\lambda\cos\varphi}{L} \quad (3)$$

где $L = \sqrt{(\Delta\varphi)^2 + (\Delta\lambda \cos\varphi)^2}$ – базовое расстояние между антеннами, выраженное в угловом измерении. Формулы 3 удобнее формул 2 тем, что аргумент обратных тригонометрических функций в них не принимает ни в каких случаях бесконечных значений, как это имеет место в (2).

В связи с возросшими угрозами пиратства и терроризма на море обсуждаются возможные проблемы спуфинга в системах ГНСС [1, 3, 4, 5]. Это означает, что курсоуказанию с помощью спутниковых компасов тоже сопутствует гипотетическая угроза спуфинга и она требует соответствующего решения.

Двухантенный спутниковый компас как детектор спуфинга

На двухантенном спутниковом компасе установлены два ГНСС-приёмника, каждый из которых определяет собственные координаты (φ_1, λ_1) и (φ_2, λ_2). Измерение истинного курса судна в режиме нормальной навигации осуществляется в соответствии с выражениями (2) или (3). Если схема спутникового компаса для определения курса реализует формулы (2), то на главных курсах (N, E, S, W) приходится иметь дело с бесконечными величинами, что крайне неудобно. Эта проблема решается введением двух компараторов, что несколько усложняет схему.

При спуфинговой атаке с помощью репитера в соответствии с системой уравнений (1) имеет место равенство:

$$(x', y', z') = (x'', y'', z'') = (x_s, y_s, z_s) \qquad (4)$$

из которого вытекает равенство координат обоих приёмоиндикаторов спутникового компаса:

$$(\varphi_1, \lambda_1) = (\varphi_2, \lambda_2) \qquad (5)$$

Подставляя выражение (5) в (2), получим:

$$\begin{aligned} ИК &= \operatorname{arctg}\frac{(\lambda_2 - \lambda_1)\cdot\cos\varphi_1}{\varphi_2 - \varphi_1} = \operatorname{arctg}\frac{0}{0} \\ ИК &= \operatorname{arcctg}\frac{\varphi_2 - \varphi_1}{(\lambda_2 - \lambda_1)\cdot\cos\varphi_1} = \operatorname{arcctg}\frac{0}{0} \end{aligned} \qquad (6)$$

Неопределённости выражений (6) относятся к нераскрываемым неопределённостям. Физически они означают выход устройства из работоспособного состояния. Внешними признаками этого будут беспорядочные показания отсчёта курса. Обнаружение таких хаотических перемен в показаниях курса является свидетельством спуфинговой атаки, при которой необходимо перейти на управление по автономному курсоуказателю (гирокомпас, магнитный компас). Если схема спутникового компаса для определения курса реализует формулы (3), то формула для вычисления истинного курса при спуфинговой атаке прибретает вид:

$$\begin{aligned} ИК &= \arccos\frac{\Delta\varphi}{L} = \\ &= \arccos\frac{\Delta\varphi}{\sqrt{\Delta\varphi^2 + (\Delta\lambda\cos\varphi_1)^2}} \\ ИК &= \arcsin\frac{\Delta\lambda\cos\varphi}{L} = \\ &= \arcsin\frac{\Delta\lambda\cos\varphi}{\sqrt{\Delta\varphi^2 + (\Delta\lambda\cos\varphi_1)^2}} \end{aligned} \qquad (7)$$

Если в формулах (7) базовая величина L заложена, как постоянный параметр (расстояние между антеннами приёмоиндикатора), то при спуфинговой атаке вместо действительного курса всегда будем иметь один из главных курсов. В первом случае (при реализации формулы arccos), будет выскакивать один из главных курсов 90° или 270°, а во втором 0° или 180° (двойственная неопределённость):

$$\begin{aligned} ИК &= \arccos\frac{0}{L} = \arccos 0 \\ ИК &= \arcsin\frac{0}{L} = \arcsin 0 \end{aligned} \qquad (8)$$

Если в формулах (7) величина L рассчитывается как:

$$L = \sqrt{(\Delta\varphi)^2 + (\Delta\lambda\cos\varphi)^2} \qquad (9)$$

то из формул (7) с учётом выражения (5) получится так же неопределённый результат вида:

$$\begin{aligned} ИК &= \arccos\frac{\Delta\varphi}{L} = \\ &= \arccos\frac{\Delta\varphi}{\sqrt{\Delta\varphi^2 + (\Delta\lambda\cos\varphi_1)^2}} = \arccos\frac{0}{0} \\ ИК &= \arcsin\frac{\Delta\lambda\cos\varphi}{L} = \\ &= \arcsin\frac{\Delta\lambda\cos\varphi}{\sqrt{\Delta\varphi^2 + (\Delta\lambda\cos\varphi_1)^2}} = \arcsin\frac{0}{0} \end{aligned} \qquad (10)$$

Все имеющие место неопределённости (6), (8), (10) являются неразрешимыми в принципе, означающими отказ в работе. Это обстоятельство может быть использовано как признак для обнаружения спуфинговой атаки с выводом на соответствующую сигнализацию.

Заключение

Анализ, проведённый в работе показал, что двухантенный спутниковый компас позволяет без каких бы то ни было дополнительных устройств обнаруживать спуфинговую атаку и сигнализировать о ней. Это неизвестное ранее свойство спутникового компаса представляется весьма ценным при решении задач противодействия террористическим операциям. Для технической реализации детектора ГНСС-спуфинга уже сегодня можно использовать существующие двухантенные спутниковые компасы фирм Furuno, Kongsberg и др.

Литература

1. TIPPENHAUER N.O., CHRISTINA PÖPPER CH., KASPER B.: Rasmussen, Srdjan Capkun: On the Requirements for Successful GPS Spoofing Attacks; http://www.syssec.ethz.ch/research/ccs139-tippenhauer.pdf
2. JURDZINSKI M.: Wykorzystanie systemów nawigacji satelitarnej do oceny całkowitego kąta znosu statku w rejonach ograniczonych. 2 Sympozjum „Nawigacja zintegrowana", Szczecin 2000, 151–157.
3. DOBRYAKOVA L., LEMIESZEWSKI Ł., OCHIN E.: Antyterroryzm – Projektowanie i analiza algorytmów antyspoofingu dla globalnych nawigacyjnych systemów satelitarnych. Scientific Journals Maritime University of Szczecin 30(102), 2012, 93–101.
4. OCHIN E., LEMIESZEWSKI Ł., LUSZNIKOV E., DOBRYAKOVA L.: The study of the spoofer's some properties with help of GNSS signal repeater. Scientific Journals Maritime University of Szczecin 36(108) z. 2, 2013, 159–165.
5. MONTGOMERY P.Y., HUMPHREYS T.E., LEDVINA B.M.: Receiver-Autonomous Spoofing Detection: Experimental Results of a Multi-antenna Receiver Defense Against a Portable Civil. GPS Spoofer ION 2009 International Technical Meeting, 2009.

Others

6. SPECHT C.: System GPS. Biblioteka Nawigacji nr 1. Wydawnictwo Bernardinum, Pelplin 2007.
7. JANUSZEWSKI J.: Systemy satelitarne GPS, Galileo i inne. PWN, 2010.
8. LUSHNIKOV E.: Навигационная безопасность морского судна. Edition of LULU Enterprises. Arizona com. USA. Arizona 2012.