(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 June 2018 (28.06.2018)

WIPO | PCT

(10) International Publication Number
WO 2018/116141 A1

(51) International Patent Classification:
G01S 19/21 (2010.01) *G01S 19/20* (2010.01)

(21) International Application Number:
PCT/IB2017/058091

(22) International Filing Date:
19 December 2017 (19.12.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/436,323 19 December 2016 (19.12.2016) US

(71) Applicant: **MAGELLAN SYSTEMS JAPAN, INC.** [JP/JP]; Amagasaki Research Incubation Center, Room 210, 7-1-3, Doui, Amagasaki, Hyogo, Hyogo 660-0083 (JP).

(72) Inventor: **LYUSIN, Sergey**; 9 Kravchenko Street, #1, Moscow, 119415 (RU).

(74) Agent: **MAGELLAN SYSTEMS JAPAN, INC.**; Amagasaki Research Incubation Center, Room 210, 7-1-3, Doui, Amagasaki, Hyogo, Hyogo 660-0083 (JP).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(54) Title: DETECTION AND ELIMINATION OF GNSS SPOOFING SIGNALS WITH PVT SOLUTION ESTIMATION

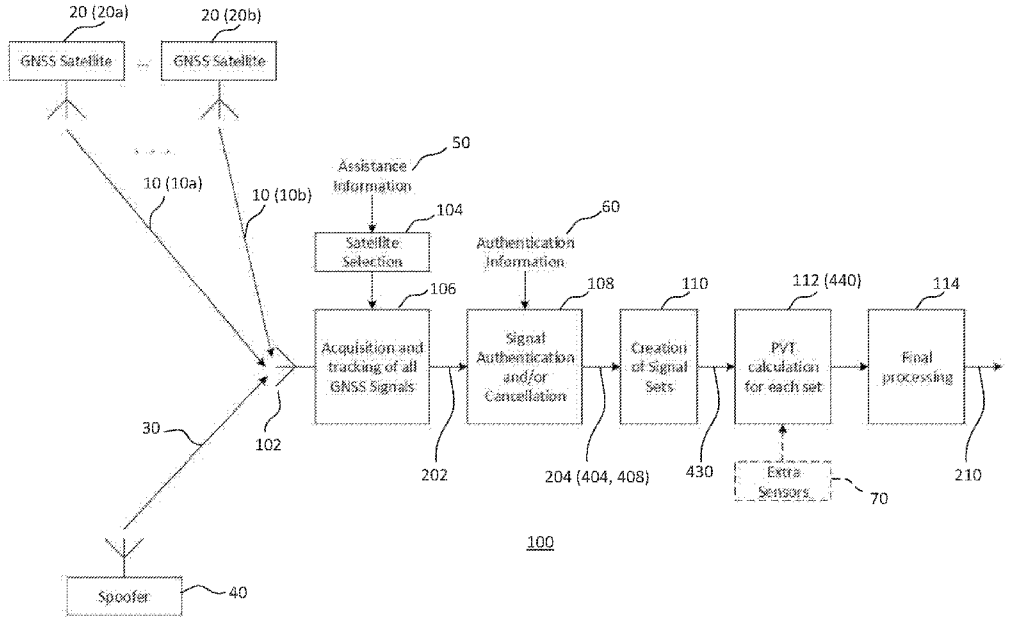

FIG. 1

(57) Abstract: A GNSS spoofing signal detection and elimination includes acquiring and tracking a plurality of GNSS signals, authenticating the acquired signals based on available authentication information to determine if the acquired signals are authentic, unverified, or counterfeit, creating a first list of the authentic signals and a second list of unverified signals, by removing the counterfeit signal(s), creating a plurality of sets of the signals by selecting at least four GNSS signals such that each set includes all of the authentic signals and at least one unverified signal, calculating PVT solutions and post-fit residuals for each set, estimating authenticity of unverified signals by analyzing the PVT solutions and post-fit residuals, estimating authenticity and accuracy of PVT solutions based on the estimation, and outputting a list of all of the acquired GNSS signals with the respective authenticity, and a list of all possible PVT solutions with the respective authenticity and accuracy.

WO 2018/116141 A1

[Continued on next page]

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

DETECTION AND ELIMINATION OF GNSS SPOOFING SIGNALS WITH PVT SOLUTION ESTIMATION

CLAIM OF PRIORITY

[0001] This application claims priority to United States Provisional Patent Application No. 62/436,323, filed on December 19, 2016, which is hereby incorporated by reference.

BACKGROUND OF THE INVENTION

1. Field of the Invention

[0002] The present invention relates to GNSS receivers and GNSS signal processing. More specifically, the present invention relates to detection and elimination of GNSS spoofing signals and estimation of PVT (position, velocity, and time) solutions at a GNSS receiver.

2. Description of the Related Art

[0003] Global Navigation Satellite Systems (GNSS) available today include United States Global Positioning System (GPS), Russian Global Orbiting Navigation Satellite System (GLONASS), European Union's Galileo, China's regional BeiDou Satellite Navigation System (BDS, formerly known as Compass), and Japanese Quasi-Zenith Satellite System (QZSS).

[0004] A GNSS spoofing signal is a type of structured interference that is close enough to a GNSS specification so as to appear authentic to an unsuspecting GNSS receiver. An intentional spoofer deliberately attempts to manipulate the PVT (position, velocity, and time) readout of a target GNSS receiver. For example, a GNSS spoofing attack may try to deceive a GNSS receiver by broadcasting incorrect GNSS signals, structured to resemble a set of normal GNSS signals, or by rebroadcasting genuine GNSS signals captured elsewhere or at a different time. These spoofed signals may be modified in such a way as to cause the GNSS receiver to estimate its position to be somewhere other than where it actually is, or to be located where it is but at a different time, as determined by the attacker. One common form of a GNSS spoofing attack, commonly termed a carry-off attack, begins by broadcasting signals synchronized with the genuine GNSS signals observed by the target GNSS receiver. The power of the counterfeit GNSS signals is then gradually increased and drawn away from the genuine GNSS signals.

[0005] Spoofing has become a more general concern as low-cost off-the shelf software-defined radio hardware, low-cost GNSS signal simulators, and record-and-play

devices, and the like become available for a competent programmer to generate realistic civil GNSS signals. As economic and practical dependences on civil GNSS for transportation, location services, communication, finance, power distribution, and other applications increase, the consequences of GNSS spoofing become more serious. Accordingly, finding effective anti-spoofing measure in GNSS receivers is one of the urgent issues.

BRIEF DESCRIPTION OF THE INVENTION

[0006] The embodiments of the present invention provide a method for detecting and eliminating a GNSS spoofing signal with PVT solutions. The method includes (a) acquiring and tracking a plurality of GNSS signals from selected GNSS satellites, (b) authenticating each of the acquired GNSS signals based on available authentication information for the acquired GNSS signals, thereby identifying each of the acquired GNSS signals as authentic, unverified, or counterfeit, (c) generating and storing a first list of the GNSS signals identified as authentic and a second list of GNSS signals identified as unverified, (d) continuing tracking and further processing the authentic signals and the unverified signals, while removing the GNSS signals identified as counterfeit from tracking and further processing,(e) creating a plurality of sets of the GNSS signals by selecting at least four GNSS signals from among the first and second lists of the GNSS signals, each set including all of the authentic GNSS signals on the first list and at least one unverified GNSS signal from the second list, (f) calculating position, velocity, and time (PVT) solutions and post-fit residuals for each of the plurality of sets based on the GNSS signals therein, (g) estimating authenticity of each of the unverified signals by analyzing the PVT solutions and post-fit residuals obtained from the respective sets including the corresponding unverified signals, (h) estimating authenticity and accuracy of each of the PVT solutions based on the estimated authenticity of the unverified signals, and (i) generating and outputting a list of all of the acquired GNSS signals with the respective authenticity thereof, and a list of all possible PVT solutions with the respective authenticity and accuracy thereof.

[0007] The acquiring and tracking the plurality of GNSS signals may includes (a1) determining an area of search for each GNSS signal based on assistance information on the corresponding GNSS satellite, (a2) searching the area for a target GNSS signal from the corresponding GNSS satellite, (a3) continuing searching the area after acquiring the target GNSS signal until the entire area is searched, whereby

acquiring any additional GNSS signal also corresponding to the target GNSS signal, and (a4) tracking the target GNSS signal and the any additional GNSS signal for each of the selected GNSS satellites.

[0008] The area of search may include a time delay search range and a frequency search range.

[0009] In accordance with one embodiment of the present invention, the selected GNSS satellites may include satellites from different GNSS's. The GNSS signals may include GNSS signals in different frequency bands.

[0010] The authentication information may include a security code included in the acquired GNSS signal, and information for verifying authenticity of the GNSS signal obtained separately from the GNSS signal.

[0011] The calculation of the PVT solutions may include obtaining positional information from at least one sensor. The at least one sensor may include at least one of an optical sensor and an inertial sensor, and the positional information may include a trajectory of a GNSS receiver.

[0012] The GNSS receive may output the PVT solutions having the highest authenticity and accuracy as a GNSS receiver output.

[0013] In accordance with one embodiment of the present invention, the method of detecting and eliminating a GNSS spoofing signal with PVT solutions may be implemented in a non-transitory computer-readable storage medium with an executable program stored thereon, wherein the program instructs a microprocessor to perform the above-described method.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] The present invention is illustrated by way of example, and not by way of limitation, in the FIG.s of the accompanying drawings and in which like reference numerals refer to similar elements and in which:

[0015] FIG. 1 is a block diagram schematically illustrating a method for detecting and eliminating GNSS spoofing signals and obtaining PVT solutions in accordance with one embodiment of the present invention.

[0016] FIG. 2 is a table showing examples of currently available GNSS signals from different GNSS systems (GPS, GLONASS, Galileo, BeiDou, and QZSS) and their frequency ranges.

[0017] FIG. 3 is a flow chart showing details of the acquisition and tracking process in accordance with one embodiment of the present invention.

[0018] FIG. 4 is a diagram schematically illustrating details of the signal authentication and/or cancelation process and the creation of the list and a plurality of sets of the acquired GNSS signals in accordance with one embodiment of the present invention.

[0019] FIG. 5 is a diagram schematically and conceptually illustrates an example of plotting M estimated positions of the GNSS receiver.

DETAILED DESCRIPTION OF EMBODIMENTS OF THE INVENTION

[0020] The present invention provides detection and elimination of GNSS spoofing signals in GNSS receivers with estimated PVT solutions. The invention protects such GNSS receivers against spoofing attacks.

[0021] FIG. 1 is a block diagram schematically illustrating a method for detecting and eliminating GNSS spoofing signals and obtaining PVT solutions in accordance with one embodiment of the present invention. The method may be implemented in a GNSS receiver 100 for a navigation device and the like. Functional blocks in FIG. 1 also correspond to schematic structure of the GNSS receiver 100. The GNSS receiver 100 implementing the present invention may be configured as a computer including a CPU, a memory (RAM, ROM), and the like therein so as to have the illustrated functional blocks. These functional blocks may be realized by means of software/computer programs realizing the respective functions, but a part or the whole of them may be realized by hardware.

[0022] The GNSS receiver 100 receives GNSS signals 10 (10a, 10b …) from a plurality of GNSS satellites 20 (20a, 20b …) at an antenna 102 thereof. The GNSS receiver 100 also receives a counterfeit signal (GNSS spoofing signal) 30 from a spoofer device 40.

[0023] FIG. 2 shows examples of currently available GNSS signals from different GNSS systems (GPS, GLONASS, Galileo, BeiDou, and QZSS) and their frequency ranges. Each GNSS has three or more frequency bands. The GNSS receiver 100 may obtain assistance information 50 regarding the currently available GNSS satellites, such as the GNSS satellites within a view form the GNSS receiver's approximate position and time. Such assistance information may be stored in a memory of the GNSS receiver 100 or obtained through a connection link such as the

Internet or radio communication. The assistance information 50 may be transmitted from a base station (server) to the GNSS receiver 100 (client receiver unit). The assistance information 50 may include frequency and timing information of the GNSS signal, the sequence of navigation data bits from each GNSS satellite, ephemeris information for determining the positions of the GNSS satellites, and the like.

[0024] Based on available assistance information 50, a plurality of GNSS satellites are selected for acquisition and tracking (104). For example, all visible GNSS satellites from the GNSS receiver 100 may be selected.

[0025] All of the available GNSS signals 10 from the selected GNSS satellites 20 that the GNSS receiver 100 can receive may be received for acquisition and tracking (106). The selected GNSS satellites 20 may include a plurality of satellites from different GNSSs, for example, GPS, GLONASS, Galileo, QZSS, etc. The selected GNSS satellites 20 may be a plurality of satellites from the same GNSS, for example GPS. The plurality of GNSS signals 10 may include GNSS signals in different frequency bands, or may be in the same frequency band, depending on the receiving bandwidth of GNSS receiver 100. The GNSS signals 10, which are used for tracking, may be pre-processed by filters with a different bandwidth in order to reduce processing complexity.

[0026] FIG. 3 shows details of the acquisition and tracking process 106. As shown in FIG. 3, an area of search for each GNSS signal 10 is determined (302) based on the information on the corresponding GNSS satellite and its GNSS signals, for example, obtained from the assistance information 50. The search area may be defined in the frequency-delay dimension. The frequency range to be searched for the acquisition may be determined from preciseness of the frequency information of the GNSS signal 10, frequency uncertainty in a local oscillator of the GNSS receiver 100, and any other frequency-related errors and uncertainties. The time-delay range to be searched for the acquisition may also be determined from preciseness of the timing information of the GNSS signal 10, time-delay uncertainty on the side of GNSS receiver 100, and any other time-related errors and uncertainties. The frequency search range and the time-delay search range may define the respective search area for each GNSS signal 10 (a target GNSS signal) from the corresponding GNSS satellite (a target GNSS satellite).

[0027] Each search area is searched for acquiring the corresponding target GNSS signal (304). The search is continued even after the target GNSS signal is acquired until the entire area is searched, such that any additional GNSS signal corresponding to the target GNSS signal is also acquired. This is because the spoofer device 40 may transmit a disguised GNSS signal(s) to the GNSS receiver 100, as mentioned above. The acquired GNSS signals, including the target GNSS signal and any additional GNSS signal(s) for each of the selected GNSS satellites are tracked (306). In addition, only the GNSS signals having energy that is not less than a predetermined threshold may be selected for further tracking.

[0028] Returning to FIG. 1, each of the acquired GNSS signals 202 are authenticated based on available authentication information 60 for the acquired GNSS signals (108), so as to identify each of the acquired GNSS signals as authentic (verified), unverified (questionable), or counterfeit/spoofing. For example, one or more of the acquired GNSS signals 202 may be a security-enhanced GNSS signal that includes a security code therein. Such a security code may be fully encrypted or contains periodic authentication codes such that some or all of its symbols are unpredictable to a would-be spoofer. By obtaining the security code from another link as the authentication information 60, the acquired GNSS signals 202 can be verified by correlating with the security code sequence. Such a security code may be preliminary obtained as a digital key, or transmitted in real time by a communication link and the like. Any other authentication information may also be used for the authentication process 108.

[0029] FIG. 4 illustrates more details of the signal authentication and/or cancelation (108), the creation of signal sets (110), and the PVT calculation of each set (112) in FIG. 1. As shown in FIG. 4, the acquired GNSS signals 202 undergo the authentication/verification process 402. The verified GNSS signals are identified and labeled (flagged) as "authentic" signal (404), and the GNSS signals which failed such verification/authentication are labeled (flagged) as "counterfeit" or "spoofing" (406). For example, if an authentic signal for the target GNSS signal has been found in the search area, any other GNSS signal(s) acquired in the same search area would be a counterfeit signal of the target GNSS signal. If an acquired GNSS signal fails the corresponding verification or authentication process, such a GNSS signal is also determined to be as counterfeit. The acquired GNSS signals for which no

authentication information is available or no authentication process is performed are labeled (flagged) as "unverified" (408). The GNSS signals, which are determined as counterfeit or spoofing signals, are discarded or eliminated from further processing, for example, by stopping tracking of the counterfeit signals.

[0030] As a result of the authentication and/or cancelation process, two lists are generated from the flagged GNSS signals 404 and 408: a first list 410 of the authentic GNSS signals A*i* and a second list 420 of unverified GNSS signals U*j*. The generated lists 410 and 420 may be stored in a memory (not shown) of the GNSS receiver 100 and further processing is performed on the listed authentic and unverified GNSS signals.

[0031] Referring back to FIG. 1, a plurality of sets of the GNSS signals are created (110) by selecting at least four (4) GNSS signals from among the first and second lists of the GNSS signals 204 (404, 406), such that each set includes all of the GNSS signals on the first list 410 (i.e., all of the authentic signals A*i*) and at least one GNSS signal from the second list 420 (i.e., at least one unverified signal U*j*).

[0032] For example, if there are four or more authentic GNSS signals A*i*, it is possible to create a first set including only the authentic signals so as to calculate authentic navigation solutions for position, velocity, and time (PVT). In such a case, the first set of authentic signals A*i* may produce the most reliable PVT solutions, and thus other sets of signals may not be necessary to obtain the PVT solutions. However, for the purpose of detecting any possible spoofing signal(s), other sets of GNSS signals may be created and the PVT solutions may be calculated in a similar manner as that described below.

[0033] If the number of the authentic signals A*i* is three or less and the remaining signals are all unverified (questionable) signals U*j*, a plurality (*M*) of sets 430 are created (112 in FIG. 1), and the PVT solutions and post-fit residuals 440 are calculated for each set (114 in FIG. 1).

[0034] For example, if three authentic GNSS signals A1, A2, and A3 and *m* unverified GNSS signals U1, U2… U*m* have been acquired and tracked, *m* sets of the acquired GNSS signals (i.e., $M = m$) may be created such that each set includes the three authentic signals A1, A2, A3, and one unverified signal U*j* ($j = 1, 2, \ldots m$). The PVT solutions and post-fit residuals are calculated for each of the *m* sets of the GNSS signals. For example, *m* estimated positions of the GNSS receiver 100 may be

obtained from the calculated PVT solutions and the post-fit residuals. By analyzing the m estimated positions, for example, by plotting the estimated positions on the coordinate plane or the easting-northing plane, it may found that one or more positions are deviated more than a statistically expected value, indicating that the corresponding set(s) may include a spoofing GNSS signal.

[0035] In the case where there are two authentic GNSS signals A1 and A2, and m unverified GNSS signals U1, U2… Um have been acquired and tracked, it is possible to create $mC2 = m(m-1)/2$ sets of the acquired GNSS signals where each set includes the two authentic signals A1 and A2, and two unverified signals Uj and Uk ($j = 1, 2, \ldots m,\ k = 1, 2, \ldots m,\ j < k$). In order for the full analysis, the PVT solutions and post-fit residuals are calculated for each of the $m(m-1)/2$ sets of the GNSS signals to produce, for example, $m(m-1)/2$ estimated positions of the GNSS receiver 100 and the post-fit residuals.

[0036] The number of sets M is not necessarily $m(m-1)/2$, but may be reduced, if the number m is large and/or if it can be assumed that the number of spoofing signal is one (1). For example, only m sets of GNSS signals may be created such that each set includes authentic GNSS signals A1 and A2, and unverified GNSS signals Uj and Uk ($j = 1, 2, \ldots m,\ k = 1, 2, \ldots m,\ k = j+1$ where $j < m$, $k = 1$ where $j = m$). If unverified GNSS signal Us is the spoofing signal, two sets including Us (when $j = s$ and $j + 1 = s$) would produce PVT solutions greatly deviated compared with other PVT solutions. Any statistical threshold value(s) can be used for the determination of spoofing signal. Any other statistical method can be used to estimate and evaluate authenticity of unverified GNSS singles from the calculated PVT solutions.

[0037] In the case where there is only one authentic GNSS signal A1, and m unverified GNSS signals U1, U2… Um have been acquired and tracked, it is possible to create $mC3 = m(m-1)(m-2)/6$ sets of the acquired GNSS signals where each set includes the authentic signal A1 and three unverified signals Uj, Uk, and Ul ($j = 1, 2, \ldots m,\ k = 1, 2, \ldots m,\ l = 1, 2, \ldots m\ j < k < l$). In order for the full analysis, the PVT solutions and post-fit residuals are calculated for each of the $m(m-1)(m-2)/6$ sets of the GNSS signals to produce, for example, $M = m(m-1)(m-2)/6$ estimated positions of the GNSS receiver 100 and the post-fit residuals. However, the number of the sets M, i.e., the number of the estimated PVT solutions, may be reduced in a similar manner as above, or using any statistical method or scheme. In addition, the number of the

acquired GNSS signals in the set is not limited to four, and the similar statistical measure when each set includes five or more acquired GNSS signals,

[0038] FIG. 5 schematically and conceptually illustrates such a plot of *M* estimated positions of the GNSS receiver. Based on the extent of the deviation compared with a statistical deviation, the authenticity of each unverified GNSS signal U*j* may be estimated. Other PVT solutions, i.e., velocity and time may also be calculated, and the authenticity of each unverified GNSS signal U*j* may be estimated based on any combination of position, velocity, and/or time.

[0039] In addition, as shown in FIG. 1, other information or data from at least one sensor 70 may also used in calculating the PVT solutions and post-fit residuals calculation. For example, when the position (coordinates) of the GNSS receiver is calculated, an optical sensor and/or an inertia sensor may be used to obtain the GNSS receiver's trajectory. In accordance with one embodiment of the present invention, the coordinates and post-fit residuals may be calculated sequentially in time using the Kalman filter.

[0040] Finally, the authenticity and accuracy of each of the PVT solutions are estimated based on the estimated authenticity of the GNSS signals (114). For example, the following information is outputted: a list of all received GNSS signals; the verified or estimated authenticity of each of the received GNSS signals (with low authenticity indicating possible spoofing attack); a list of all possible PVT solutions; and estimated authenticity and accuracy of each PVT solution.

[0041] The PVT solution having the highest authenticity and accuracy may be outputted as a GNSS receiver output 210.

[0042] In accordance with one embodiment of the present invention, the method as described above may be implemented in a non-transitory computer-readable storage medium with an executable program stored thereon. The program instructs a microprocessor to perform the method described above.

[0043] While this invention has been described in terms of several preferred embodiments, there are alterations, permutations, modifications, and various substitute equivalents, which fall within the scope of this invention. It should also be noted that there are many alternative ways of implementing the methods and apparatuses of the present invention. It is therefore intended that the following appended claims be interpreted as including all such alterations, permutations, and

various substitute equivalents as fall within the true spirit and scope of the present invention.

CLAIMS

What is claimed is:

1. A method for detecting and eliminating a GNSS spoofing signal with PVT solutions, the method comprising:

acquiring and tracking a plurality of GNSS signals from selected GNSS satellites;

authenticating each of the acquired GNSS signals based on available authentication information for the acquired GNSS signals, thereby identifying each of the acquired GNSS signals as authentic, unverified, or counterfeit;

generating and storing a first list of the GNSS signals identified as authentic and a second list of GNSS signals identified as unverified;

continuing tracking and further processing the authentic signals and the unverified signals, while removing the GNSS signals identified as counterfeit from tracking and further processing;

creating a plurality of sets of the GNSS signals by selecting at least four GNSS signals from among the first and second lists of the GNSS signals, each set including all of the authentic GNSS signals on the first list and at least one unverified GNSS signal from the second list;

calculating position, velocity, and time (PVT) solutions and post-fit residuals for each of the plurality of sets based on the GNSS signals therein;

estimating authenticity of each of the unverified signals by analyzing the PVT solutions and post-fit residuals obtained from the respective sets including the corresponding unverified signals;

estimating authenticity and accuracy of each of the PVT solutions based on the estimated authenticity of the unverified signals; and

generating and outputting a list of all of the acquired GNSS signals with the respective authenticity thereof, and a list of all possible PVT solutions with the respective authenticity and accuracy thereof.

2. The method of claim 1, wherein the acquiring and tracking the plurality of GNSS signals includes:

determining an area of search for each GNSS signal based on assistance information on the corresponding GNSS satellite;

searching the area for a target GNSS signal from the corresponding GNSS satellite;

continuing searching the area after acquiring the target GNSS signal until the entire area is searched, whereby acquiring any additional GNSS signal also corresponding to the target GNSS signal; and

tracking the target GNSS signal and the any additional GNSS signal for each of the selected GNSS satellites.

3. The method of claim 2, wherein the area of search includes a time delay search range and a frequency search range.

4. The method of claim 1, wherein the selected GNSS satellites include satellites from different GNSS's.

5. The method of claim 1, wherein the GNSS signals include GNSS signals in different frequency bands.

6. The method of claim 1, wherein the authentication information includes:

a security code included in the acquired GNSS signal; and

information for verifying authenticity of the GNSS signal obtained separately from the GNSS signal.

7. The method of claim 1, wherein the calculating the PVT solutions includes:

obtaining positional information from at least one sensor.

8. The method of claim 7, wherein the at least one sensor includes at least one of an optical sensor and an inertial sensor.

9. The method of claim 7, wherein the positional information includes a trajectory of a GNSS receiver.

10. The method of claim 1, further comprising:

outputting the PVT solutions having the highest authenticity and accuracy as a GNSS receiver output.

11. A non-transitory computer-readable storage medium with an executable program stored thereon, wherein the program instructs a microprocessor to perform the method of claim 1.

12. A GNSS receiver configured to perform the method of claim 1.

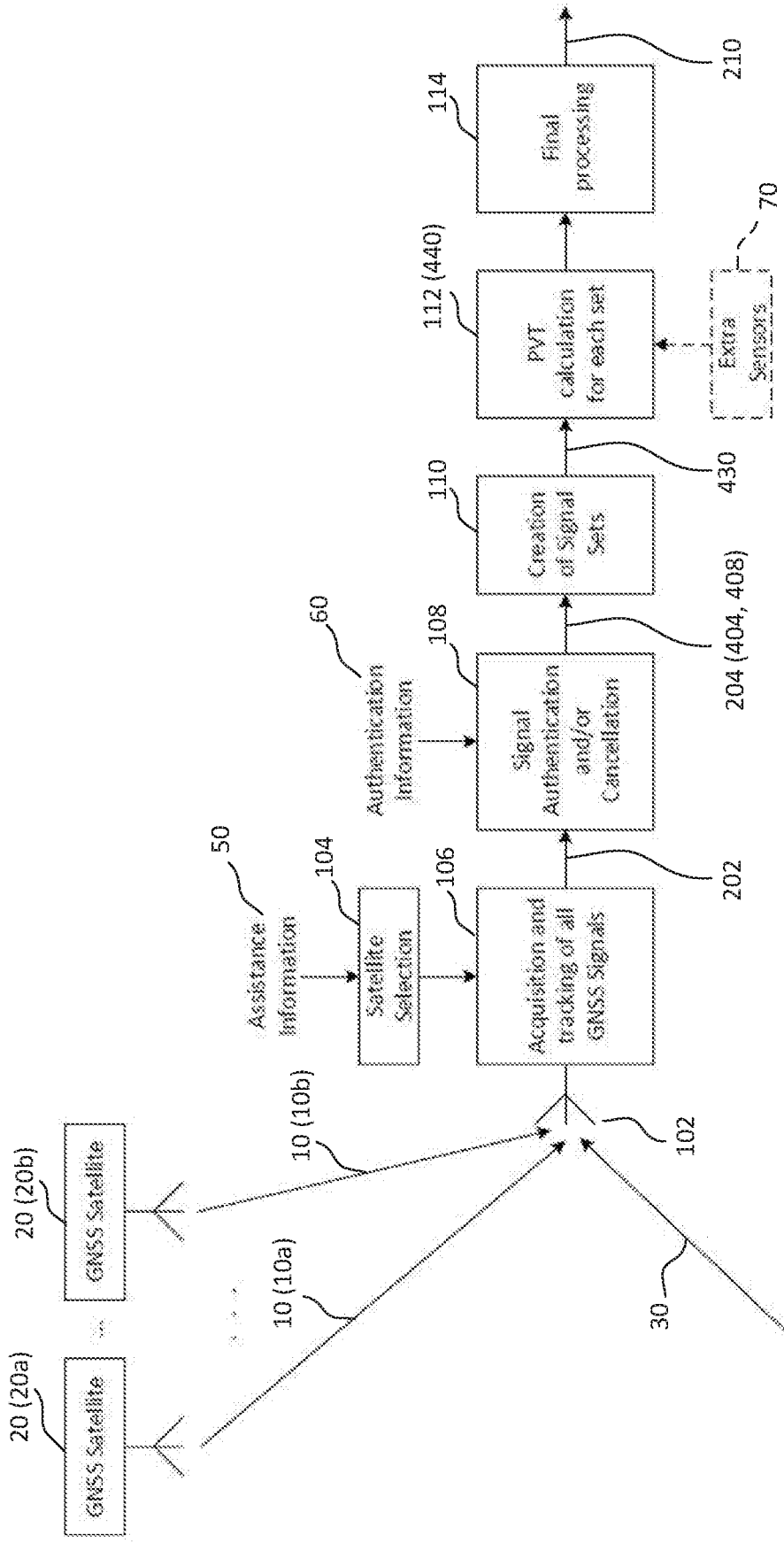
GNSS Satellite
20 (20a)
GNSS Satellite
20 (20b)
10 (10a)
10 (10b)
30
Spoofer
40
102
Acquisition and tracking of all GNSS Signals
106
202
Satellite Selection
104
Assistance Information
50
Signal Authentication and/or Cancellation
108
Authentication Information
60
204 (404, 408)
Creation of Signal Sets
110
430
PVT calculation for each set
112 (440)
Extra Sensors
70
Final processing
114
210
100

FIG. 1

Signal	Notation	Signal Frequency Range, MHz
GLONASS L1	G1	1593 ~ 1610
BeiDou B1-2	B1-2	1580 ~ 1600
GPS L1, Galileo E1, QZSS L1	L1	1563 ~ 1587
BeiDou B1	B1	1551 ~ 1571
Galileo E6, QZSS LEX	E6	1259 ~ 1299
BeiDou B3	B3	1259 ~ 1279
GLONASS L2	G2	1238 ~ 1254
GPS L2, QZSS L2	L2	1218 ~ 1238
BeiDou B2	B2	1197 ~ 1217
GLONASS L3	G3	1191 ~ 1211
Galileo E5	E5	1167 ~ 1217
GPS L5, QZSS L5	L5	1164 ~ 1188

FIG. 2

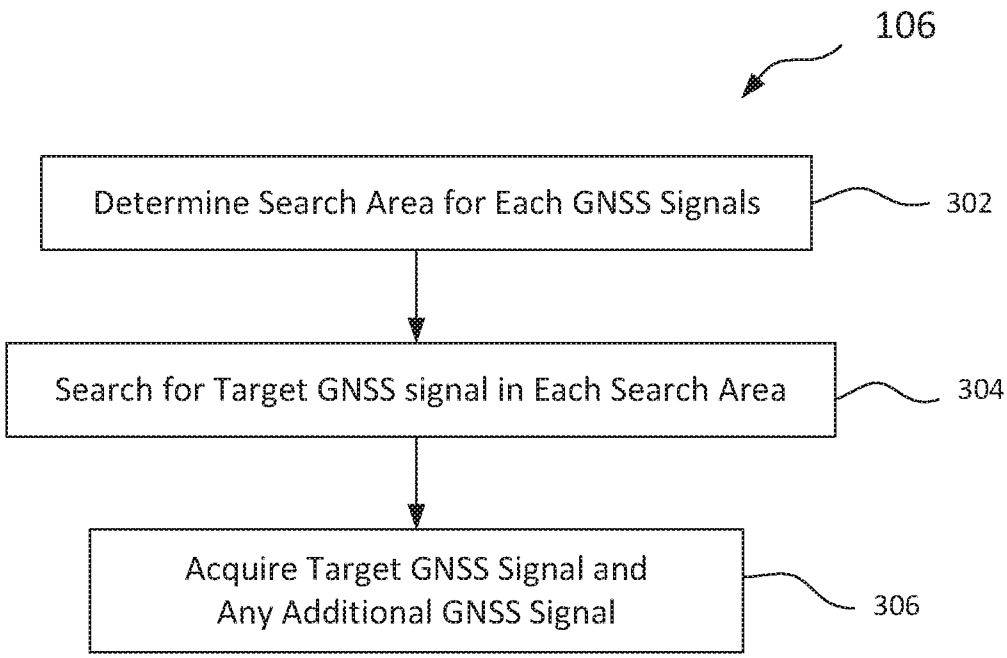
106
Determine Search Area for Each GNSS Signals
302
Search for Target GNSS signal in Each Search Area
304
Acquire Target GNSS Signal and
Any Additional GNSS Signal
306

FIG. 3

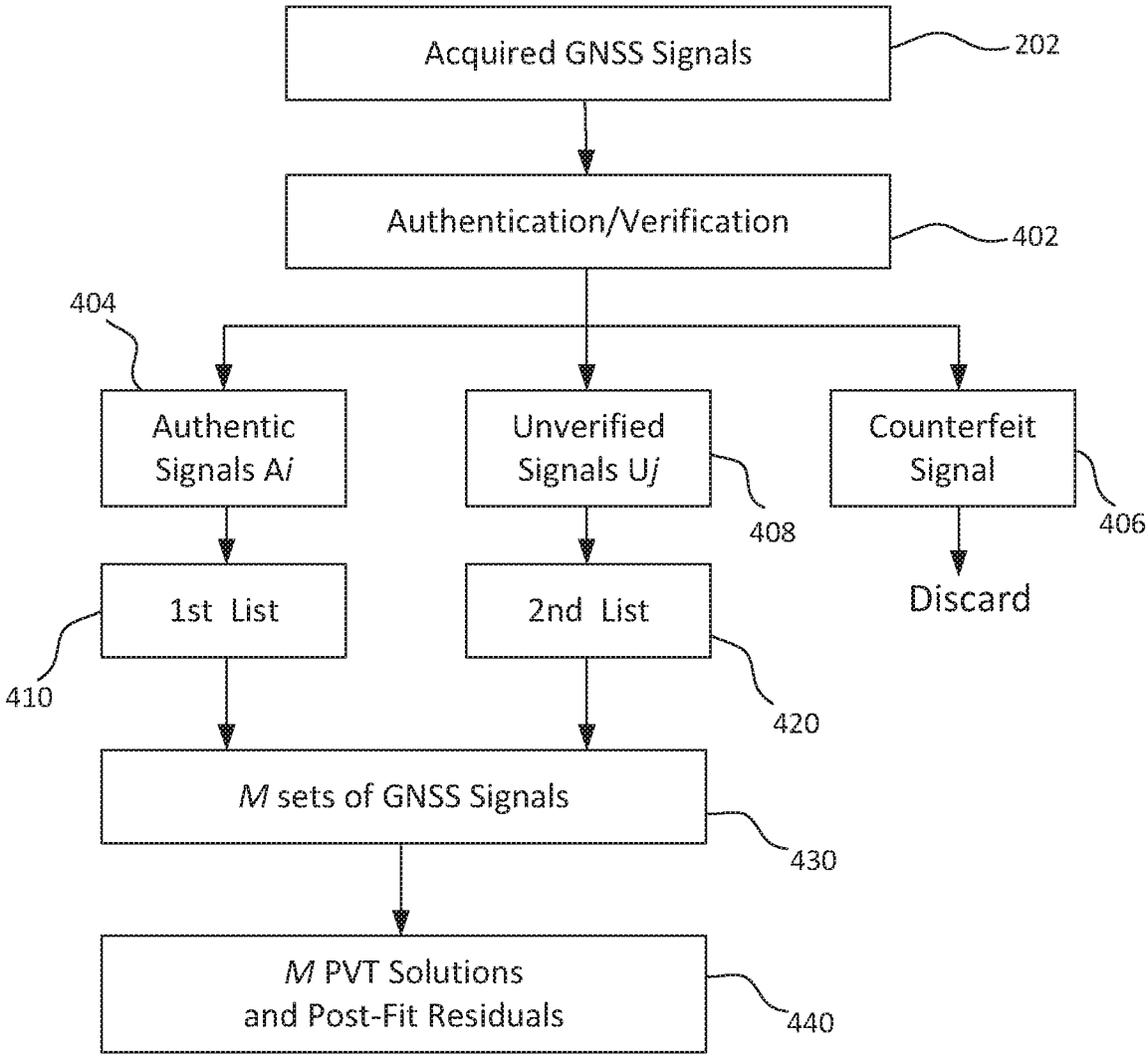
Acquired GNSS Signals
202
Authentication/Verification
402
404
Authentic Signals Ai
Unverified Signals Uj
408
Counterfeit Signal
406
Discard
1st List
410
2nd List
420
M sets of GNSS Signals
430
M PVT Solutions and Post-Fit Residuals
440

FIG. 4

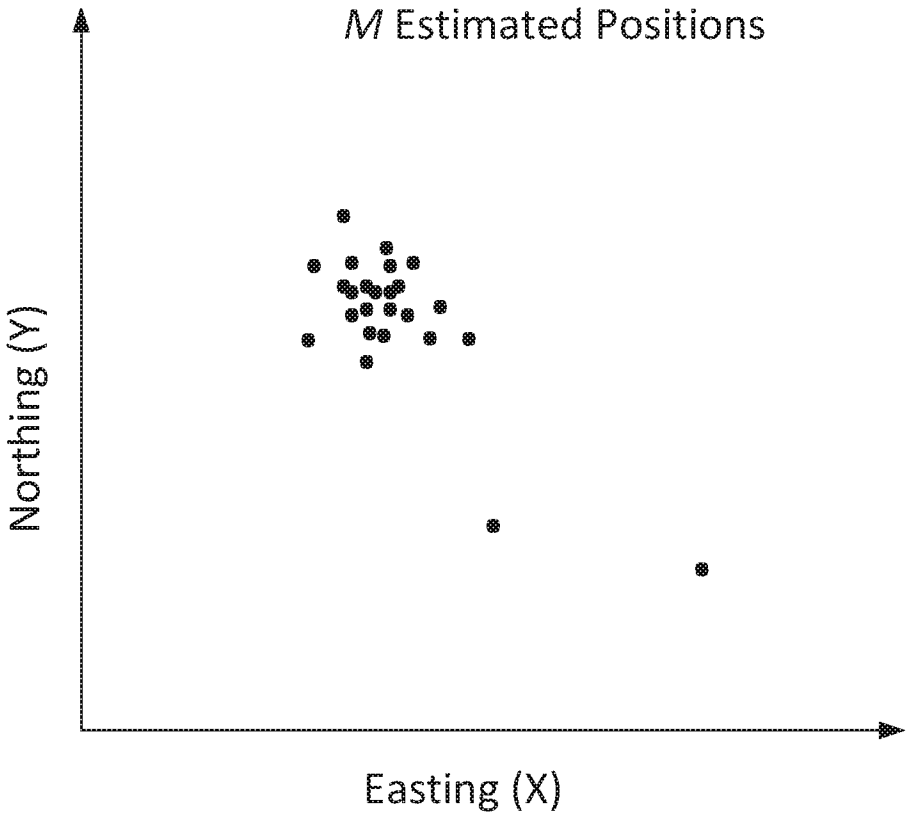

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2017/058091

A. CLASSIFICATION OF SUBJECT MATTER
INV. G01S19/21
ADD. G01S19/20

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G01S

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data, INSPEC, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	GÜNTHER ET AL: "A Survey of Spoofing and Counter-Measures", NAVIGATION: JOURNAL OF THE INSTITUTE OF NAVIGATION, INSTITUTE OF NAVIGATION, FAIRFAX, VA, US, vol. 61, no. 3, 1 September 2014 (2014-09-01), pages 159-177, XP056007288, ISSN: 0028-1522, DOI: 10.1002/NAVI.65 page 167, left-hand column, lines 47-51 page 168, right-hand column, lines 10-14, 26-28 ----- -/--	1-12

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 April 2018	30/04/2018

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Naddeo, Giovanni

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	SCOTT L: "Anti-Spoofing & Authenticated Signal Architectures for Civil Navigation Systems", PROCEEDINGS OF ION GPS/GNSS, XX, XX, vol. 2003, 1 January 2003 (2003-01-01), pages 1543-1552, XP002436415, the whole document -----	1-12
A	WO 2016/067279 A1 (ACCUBEAT LTD [IL]) 6 May 2016 (2016-05-06) the whole document -----	1-12
A	US 7 764 224 B1 (ANDERSON DAVID A [US]) 27 July 2010 (2010-07-27) the whole document -----	1-12

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/IB2017/058091

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2016067279 A1	06-05-2016	CA 2964073 A1	06-05-2016
		EP 3213116 A1	06-09-2017
		IL 235356 A	29-02-2016
		WO 2016067279 A1	06-05-2016
US 7764224 B1	27-07-2010	NONE	