

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2015 年 9 月 3 日(03.09.2015)



(10) 国際公開番号

WO 2015/129204 A1

- (51) 国際特許分類:
G01S 19/05 (2010.01) G01S 19/21 (2010.01)
- (21) 国際出願番号: PCT/JP2015/000744
- (22) 国際出願日: 2015 年 2 月 18 日(18.02.2015)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2014-037047 2014 年 2 月 27 日(27.02.2014) JP
- (71) 出願人: 株式会社デンソー(DENSO CORPORATION) [JP/JP]; 〒4488661 愛知県刈谷市昭和町 1 丁目 1 番地 Aichi (JP).
- (72) 発明者: 山城 貴久(YAMASHIRO, Takahisa); 〒4488661 愛知県刈谷市昭和町 1 丁目 1 番地株式会社デンソー内 Aichi (JP). 隈部 正剛(KUMABE, Seigou); 〒4488661 愛知県刈谷市昭和町 1 丁目 1 番地株式会社デンソー内 Aichi (JP).
- (74) 代理人: 金 順姫(KIN, Junhi); 〒4600003 愛知県名古屋市中区錦 2 丁目 1 3 番 1 9 号 瀧定ビル 6 階 Aichi (JP).
- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): 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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, KE, KG, KN, KP, KR, 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.
- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーロパ (AM, AZ, BY, KG, KZ, RU, TJ, TM), ユーロッパ (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).
- 添付公開書類:
— 国際調査報告 (条約第 21 条(3))

(54) Title: NAVIGATION MESSAGE RECEPTION DEVICE

(54) 発明の名称: 航法メッセージ受信装置

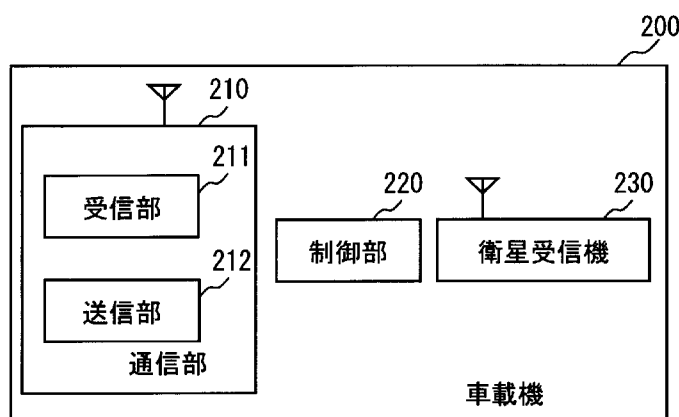


FIG. 3:
200 In-vehicle unit
210 Communication unit
211 Receiver unit
212 Transmitter unit
220 Controller
230 Satellite receiver

(57) Abstract: Provided is a navigation message reception device for deciding whether navigation messages from space satellites used in a satellite positioning system are legitimate. The navigation message reception device according to one aspect decides that a navigation message is legitimate when a transmission time matching a transmission time included in a navigation message which has been successfully authenticated through communication with an authentication center (120) is determined to be included in a navigation message received by a satellite receiver (230) from a GPS satellite (2) different from the one that transmitted the navigation message which was successfully authenticated through communication with the authentication center (120).

(57) 要約: 衛星測位システムで用いられる人工衛星からの航法メッセージが正規のものであるかを判断する航法メッセージ受信装置を提供する。一実施形態の航法メッセージ受信装置は、認証センタ(120)との通信で認証が成立した航法メッセージに含まれる発信時刻と一致する発信時刻が、認証

センタ(120)との通信で認証が成立した航法メッセージの発信元とは異なるGPS衛星(2)から衛星受信機(230)で受信した航法メッセージに含まれると判定した場合には、当該航法メッセージが正規のものであると判断する。

明 細 書

発明の名称： 航法メッセージ受信装置

関連出願の相互参照

[0001] 本出願は、2014年2月27日に出願された日本国特許出願2014-37047号に基づくものであり、これをここに参照により援用する。

技術分野

[0002] 本開示は、衛星測位システムで用いられる人工衛星から航法メッセージを受信する航法メッセージ受信装置に関するものである。

背景技術

[0003] 従来、衛星測位システムで用いられる人工衛星から発信される航法メッセージを受信機によって受信し、位置を測位する技術が知られている。

[0004] しかしながら、近年では、人工衛星からの信号を複製するリピータや、人工衛星からの信号を擬似的に生成可能なシミュレータ等の開発により、悪意の行為者による位置情報の改竄やなりすましが発生してきている。

[0005] これに対して、特許文献1には、受信機が受信した航法メッセージが、衛星測位システムで用いられる人工衛星からの正規の航法メッセージであるかの認証を行う技術が開示されている。特許文献1に開示の技術では、受信機は、認証センタのデータベースにアクセスし、人工衛星から受信した航法メッセージに含まれる衛星番号と衛星時刻から、対象とする人工衛星の認証に用いるデータを取得する。そして、受信機は、認証センタから取得したデータを用いて、受信した航法メッセージが、衛星測位システムで用いられる人工衛星からの正規の航法メッセージであるかの認証を行う。

先行技術文献

特許文献

[0006] 特許文献1：特開2013-130395号公報

発明の概要

[0007] 本願発明者は、特許文献1に開示の技術に関し以下を見出した。

[0008] 特許文献 1 に開示の技術では、受信機が測位のたびに、測位に用いた複数の人工衛星からの航法メッセージの全てについて、認証センタと通信を行って正規の航法メッセージであるかの認証を行う必要がある。よって、各受信機と認証センタとが頻繁に通信を行う必要が生じ、認証センタの通信処理負荷が膨大になってしまう。

[0009] 本開示は、上記に鑑みなされたものであって、その目的は、衛星測位システムで用いられる人工衛星からの航法メッセージが正規のものであるかの認証に用いられる認証センタの通信処理負荷を抑えながらも、人工衛星からの航法メッセージが正規のものであるかを判断することを可能にする航法メッセージ受信装置を提供することにある。

[0010] 本開示の一例に係る航法メッセージ受信装置は、衛星測位システムで用いられる人工衛星からの航法メッセージを受信する衛星受信機と、人工衛星から受信した航法メッセージに応じた認証用情報を、認証センタから受信する認証用情報受信部と、衛星受信機で受信した航法メッセージが正規の航法メッセージであることの認証を、当該航法メッセージに応じて認証用情報受信部で受信した認証用情報を用いて行うセンタ使用認証部とを備える航法メッセージ受信装置であって、航法メッセージには、複数の人工衛星間で整合性が取れる整合情報が含まれており、センタ使用認証部で認証が成立した航法メッセージに含まれる整合情報と整合性が取れる情報が、センタ使用認証部で認証が成立した航法メッセージの発信元とは異なる人工衛星である未認証衛星から衛星受信機で受信した航法メッセージに含まれるか否かを判定する整合性判定部と、整合性判定部で整合情報と整合性が取れる情報が含まれると判定した場合には、衛星受信機で受信した航法メッセージが正規のものであると判断する一方、整合性判定部で整合情報と整合性が取れる情報が含まれていないと判定した場合には、衛星受信機で受信した航法メッセージが正規のものであると判断しない簡易判断部とを備える。

[0011] 上記の航法メッセージ受信装置によれば、センタ使用認証部で認証が成立した航法メッセージに含まれる整合情報と整合性が取れる情報が、センタ使

用認証部で認証が成立した航法メッセージの発信元とは異なる未認証衛星から衛星受信機で受信した航法メッセージに含まれると判定した場合に、未認証衛星から衛星受信機で受信した航法メッセージが正規のものであると判断する。つまり、認証センタとの通信を行わずに、センタ使用認証部で認証が成立した航法メッセージに含まれる整合情報と整合性が取れる情報を含むか否かによって、正規の航法メッセージであるかを判断する。

[0012] 整合情報は、複数の人工衛星間で整合性が取れるものであるため、正規のものとセンタ使用認証部で認証が成立した航法メッセージに含まれる整合情報と整合性が取れる情報を含む航法メッセージも、正規のものである可能性が高い。よって、上記の航法メッセージ受信装置によれば、1つの航法メッセージについてセンタ使用認証部で認証が成立すれば、その他の航法メッセージについては、認証センタとの通信を行わなくても、正規のものである可能性の高い航法メッセージを、正規のものであると判断することが可能になる。従って、自装置が認証センタから認証用情報を受信しなくてもよくなる分だけ、認証センタの通信処理負荷を軽減できる。

[0013] その結果、衛星測位システムで用いられる人工衛星からの航法メッセージが正規のものであるかの認証に用いられる認証センタの通信処理負荷を抑えながらも、人工衛星からの航法メッセージが正規のものであるかを判断することが可能になる。

図面の簡単な説明

[0014] 本開示についての上記および他の目的、特徴や利点は、添付の図面を参照した下記の詳細な説明から、より明確になる。添付図面において

[図1]図1は、実施形態1における簡易認証システムの概略的な構成の一例を示す図である。

[図2]図2は、認証センタの概略的な構成の一例を示すブロック図である。

[図3]図3は、車載機の概略的な構成の一例を示すブロック図である。

[図4]図4は、実施形態1における車載機での認証関連処理の流れの一例を示すフローチャートである。

[図5]図5は、実施形態における車載機での簡易判断処理の流れの一例を示すフローチャートである。

[図6]図6は、S32の処理の一例について説明を行うための模式図である。

[図7]図7は、変形例1における車載機200での簡易判断処理の流れの一例を示すフローチャートである。

発明を実施するための形態

[0015] 以下、実施形態について図面を用いて説明する。

[0016] (実施形態1)

図1に示すように、実施形態1における簡易認証システム1は、モニタステーション110、認証センタ120、マスタコントロールステーション130及び車載機200を含む。車載機200を用いる車両を車両Aとする。車載機200が航法メッセージ受信装置に相当する。

[0017] <簡易認証システム1の概略構成>

モニタステーション110は、衛星測位システムの一つであるGPSが備えるGPS衛星2a～2cが発信するGPS電波を受信する。GPS衛星2a～2cが人工衛星に相当する。以降では、GPS衛星2a～2cの個々を区別しない場合にはGPS衛星2と表現する。周知のように、GPS電波には航法メッセージが含まれている。モニタステーション110は、受信したGPS電波を復調して航法メッセージを抽出し、認証センタ120へ送る。複数のGPS衛星2からGPS電波を受信した場合には、それぞれのGPS電波から航法メッセージを抽出して、認証センタ120へ送る。

[0018] 認証センタ120は、航法メッセージと暗号キーであるHマトリクスとからパリティデータを作成する。そして、このパリティデータを含む信号をマスタコントロールステーション130に送る。また、車載機200との間で通信も行う。この認証センタ120の詳細な説明は図2を用いて後に行う。

[0019] マスタコントロールステーション130は、認証センタ120から受信したパリティデータを準天頂衛星（以下、QZS衛星）3に送信する。QZS衛星3は、パリティデータを含んだ航法メッセージを地上に向けて放送する

。

[0020] 車載機 200 は、航法メッセージ認証型（NMA : Navigation Message Authentication）車載機である。車載機 200 は、認証センタ 120 と通信を行い、GPS 衛星 2 から受信した航法メッセージが正規の航法メッセージであることの認証を行う。認証の詳細な説明については、図 4 を用いて後に行う。

[0021] また、車載機 200 は、複数の GPS 衛星 2 から受信した航法メッセージを用いて自機器の現在位置を測位する。現在位置の測位には、最低でも 3 つの GPS 衛星 2 から受信した航法メッセージを用いる。

[0022] さらに、車載機 200 は、自機器で認証が成立した航法メッセージを用いて、その航法メッセージとほぼ同じタイミングで受信していた他の GPS 衛星 2 の航法メッセージが正規のものであるかを、認証センタ 120 へのアクセスなしに判断する簡易判断処理を行う。車載機 200 の詳細な説明は、図 3 を用いて後に行う。

[0023] <認証センタ 120 の詳細構成>

図 2 に示すように、認証センタ 120 は、制御部 122、データ記憶部 124、通信部 126 を備える。

[0024] 制御部 122 は、CPU、ROM、RAM 等を備えたコンピュータであり、データ記憶部 124、通信部 126 を制御する。また、CPU が、RAM の一時記憶機能を利用しつつ ROM に記憶されているプログラムを実行することで、RAND メッセージ生成部 1221、SEED 値生成部 1222、H マトリクス計算部 1223、パリティ計算部 1224、信号加工部 1225 として機能する。なお、これら、各部 1221 ~ 1225 の機能は、特許文献 1 に開示されている機能を含んでいてもよい。

[0025] RAND メッセージ生成部 1221 は、モニタステーション 110 から取得する航法メッセージから、RAND メッセージを作成する。RAND メッセージは、航法メッセージのビット列の中から、TOW (time of week) のビット列のデータとエフェメリスデータのうちのクロック補正パラメータで

あるT O C、A F 0、A F 1とが順番に並んでいる。T O W、T O C、A F 0、A F 1が信号の発信時刻を特定するデータであって、発信時刻に相当する。さらに、その後に、アンチスプーフフラグであるA S F l a g、衛星番号であるP R N (Pseudo Random Noise) I Dが追加されている。

[0026] T O WとP R N I Dを含んでいるR A N Dは、どのG P S衛星がいつ発信したかを示すデータであると言える。また、T O Wが6秒ごとに変化し、また、P R N I Dを含んでいるので、モニタステーション110が受信したG P S衛星2ごと、かつ、6秒ごとにR A N Dを生成することになる。

[0027] S E E D値生成部1222は、P Cクロックを入力として乱数を発生させることで、S E E D値を生成する。

[0028] Hマトリクス計算部1223は、S E E D値生成部1222が生成したS E E D値を使い、このS E E D値に一对一に対応するHマトリクスを計算する。Hマトリクスとしては、周知のハッシュ関数を用いればよく、例えばL D P C (Low Density Parity Check) 符号化を行うためのパリティ検査行列を用いればよい。さらに、パリティ検査行列から決定される生成行列を用いてもよい。

[0029] パリティ計算部1224は、R A N Dメッセージ生成部1221が生成したR A N Dメッセージと、Hマトリクス計算部1223が計算したHマトリクスに基づいて、パリティデータを計算する。

[0030] 信号加工部1225は、パリティ計算部1224が計算したパリティデータ、及びその計算に使用したR A N Dメッセージを、Q Z S衛星3から発信させる航法メッセージに挿入する。そして、挿入済みの航法メッセージをマスタコントロールステーション130に送る。

[0031] さらに、信号加工部1225は、信号の挿入に合わせて、パリティ計算部1224が計算したパリティデータ、パリティデータの計算に用いたR A N Dメッセージ、Hマトリクス、Hマトリクスの計算に用いたS E E D値を対応付けて、データ記憶部124に記憶する。

[0032] この信号加工部1225は、R A N Dメッセージ生成部1221がR A N

Dメッセージを生成するごとに、R A N DメッセージとパリティデータをQ Z S衛星3に送信させる航法メッセージに挿入する。よって、R A N Dメッセージ生成部1 2 2 1、S E E D値生成部1 2 2 2、Hマトリクス計算部1 2 2 3、パリティ計算部1 2 2 4も、R A N Dメッセージ生成部1 2 2 1がR A N Dメッセージを生成するごとに、処理を実行する。

[0033] Hマトリクス選択部1 2 2 6は、車載機2 0 0から送信されてきたP R N I D、T O W、公開キーを通信部1 2 6で受信した場合に、データ記憶部1 2 4に記憶されているHマトリクスから、受信したP R N I D、T O Wに対応するHマトリクスを選択する。そして、選択したHマトリクスを公開鍵で暗号化し、暗号化したHマトリクスを車載機2 0 0へ返信する。

[0034] <車載機2 0 0の詳細構成>

Q Z S衛星3が放送した航法メッセージは、車載機2 0 0の通信部2 1 0が備える受信部2 1 1に受信される。図3に示すように、この車載機2 0 0は、通信部2 1 0、制御部2 2 0、衛星受信機2 3 0を備える。

[0035] 通信部2 1 0は、受信部2 1 1と送信部2 1 2とを備える。通信部2 1 0は、広域通信機能を備えている。広域通信機能は、例えば、通信距離が数キロメートルであり、公衆通信回線網の基地局と通信を行うことにより、公衆通信回線網の通信圏内にある他の通信機器と通信することができる。広域通信機能により、認証センタ1 2 0の通信部1 2 6との間で通信を行う。

[0036] 衛星受信機2 3 0は、G P S衛星2、Q Z S衛星3が発信する電波を一定周期で受信する。衛星受信機2 3 0は、一定の周期ごとに、1周期内にG P S衛星2から受信した航法メッセージを車載機2 0 0の制御部2 2 0に出力する。よって、1周期内に複数のG P S衛星2から航法メッセージを受信していた場合には、これらのG P S衛星2についての航法メッセージを制御部3 2 0に出力することになる。1周期内に受信した複数の航法メッセージは、ほぼ同じタイミングで受信した航法メッセージと言える。

[0037] 制御部2 2 0は、C P U、R O M、R A M等を備えたコンピュータであり、通信部2 1 0、衛星受信機2 3 0を制御する。また、C P Uが、R A Mの

一時記憶機能を利用しつつROMに記憶されているプログラムを実行することで、図4に示す認証関連処理や図5に示す簡易判断処理を実行する。

[0038] <認証関連処理>

続いて、車載機200の制御部220が実行する、衛星受信機230で受信した信号がGPS衛星2から受信した正規の航法メッセージであることの認証に関連する処理（以下、認証関連処理）について、図4に示すフローチャートを用いて説明を行う。図4のフローチャートは、例えば衛星受信機230が前述の1周期内に受信した3つ以上のGPS衛星2からGPS電波を受信するごとに実行する構成とすればよい。

[0039] ここで、衛星受信機230は、GPS衛星2からの信号を複製するリピータや、GPS衛星2からの信号を擬似的に生成可能なシミュレータからの信号を、GPS電波に含まれる航法メッセージと誤って受信している場合もあるものとする。

[0040] まず、ステップS1では、3つ以上の複数のGPS衛星2から受信したGPS電波に含まれる航法メッセージに基づいて自装置の現在位置を測位する。

[0041] ステップS2では、QZS衛星3から受信した航法メッセージを、受信部211から取得する。ステップS3では、S1で取得した航法メッセージから、PRN ID、TOWを抽出する。

[0042] ステップS4では、S3で抽出したPRN IDとTOWを公開鍵とともに、送信部212から認証センタ120へ送信する。前述したように、認証センタ120は、このPRN IDとTOWとにより定まるHマトリクスを、公開鍵により暗号化して車載機200へ送信する。車載機200から認証センタ120に送信したPRN IDとTOWとにより定まるHマトリクスが、認証用情報に相当する。

[0043] ステップS5では、認証センタ120から送信されたHマトリクスを受信部211から取得する。つまり、GPS衛星2から受信した航法メッセージに応じたHマトリクスを認証センタ120から受信する。このS5が認証用

情報受信部に相当する。ステップS 6では、S 5で取得した、暗号化されたHマトリクスを秘密鍵で復号する。

[0044] ステップS 7では、GPS衛星2から受信したGPS電波に含まれる航法メッセージのうち、S 4で送信したPRN IDと同じPRN IDを含んでいる航法メッセージから、RANDメッセージを作成する。

[0045] ステップS 8では、S 7で作成したRANDメッセージと、S 6で復号したHマトリクスとに基づいて、比較パリティデータを作成する。ステップS 9では、S 8で作成した比較パリティデータと、S 3で抽出したパリティデータとが一致するか否かを判断する。

[0046] S 6で復号したHマトリクスは、認証センタ120がパリティデータの作成に使用したHマトリクスと同じである。そして、認証センタ120のパリティ計算部1224は、このHマトリクスとRANDメッセージとに基づいてパリティデータを計算している。

[0047] よって、S 8で作成した比較パリティデータが、S 3で抽出したパリティデータと一致する場合、S 7で作成したRANDメッセージが、認証センタ120が作成したRANDメッセージと同じであると考えることができる。

[0048] そこで、S 8で作成した比較パリティデータと、S 3で抽出したパリティデータとが一致する場合（S 9でYES）には、ステップS 10に進み、認証成立とする。認証成立した場合、図4の処理を終了する。一方、2つのパリティデータが一致しない場合（S 9でNO）には、ステップS 11に進み、認証不成立とする。認証不成立であった場合には、S 2に戻り、S 1での測位に用いた全ての航法メッセージのうちの、1つでも認証成立となるまで処理を繰り返す。このように、認証関連処理では、GPS衛星2から受信した航法メッセージに応じて認証センタ120から受信したHマトリクス（つまり、認証用情報）を用いて認証を行う。このS 9～S 11がセンタ使用認証部に相当する。

[0049] <簡易判断処理>

ここで、実施形態1における車載機200の制御部320が実行する簡易

判断処理について、図5に示すフローチャートを用いて説明を行う。図5のフローチャートは、測位に用いた複数の航法メッセージのうち、少なくとも1つの航法メッセージについて認証関連処理で認証が成立したときに開始する構成とすればよい。図5のフローチャートは、測位に用いた複数の航法メッセージのうち、認証関連処理で認証を未だに行っていない航法メッセージについてそれぞれ処理を行う構成とすればよい。

[0050] まず、ステップS21では、測位に用いた航法メッセージのうち、認証関連処理で認証が成立した航法メッセージ（つまり、認証済航法メッセージ）以外の航法メッセージ（以下、未認証航法メッセージ）を取得する。

[0051] ステップS22では、S21で取得した未認証航法メッセージに含まれる発信時刻と、認証済航法メッセージに含まれる発信時刻とが一致しているか否かを判定する。ここで言うところの一致とは、完全に一致する場合だけでなく、誤差程度の範囲内で略一致する場合も含むものとする。認証済航法メッセージに含まれる発信時刻が整合情報に相当し、S22が整合性判定部に相当する。

[0052] ここで、S22の処理の一例について、図6を用いて説明を行う。図6の例では、測位に用いられたGPS衛星のうち、GPS衛星2aから発信された航法メッセージについては、車載機200で認証センタ120を用いた認証が成立しており、GPS衛星2bから発信された航法メッセージについては認証が未だ行われていないものとする。

[0053] また、GPS衛星2aから発信された航法メッセージ（つまり、認証済航法メッセージ）の発信時刻を T_{i1} とし、GPS衛星2bから発信された航法メッセージ（つまり、未認証航法メッセージ）の発信時刻を T_{i2} とする。S22の処理では、認証済航法メッセージの発信時刻（ T_{i1} ）と未認証航法メッセージの発信時刻（ T_{i2} ）とが一致しているか否かを判定する。

[0054] 衛星受信機230において1周期内に受信する複数の航法メッセージは、GPS衛星2からの信号を複製するリピータやGPS衛星2からの信号を擬似的に生成可能なシミュレータが用いられていなければ、発信時刻が一致す

る関係にある。

[0055] ステップS 2 3では、発信時刻が一致していると判定した場合（S 2 3でY E S）には、認証済航法メッセージに含まれていた発信時刻と整合性が取れる発信時刻が未認証航法メッセージに含まれると判定し、S 2 4に進む。S 2 4では、S 2 1で取得した未認証航法メッセージを、正規の航法メッセージであると判断し、処理を終了する。一方、発信時刻が一致していないと判定した場合（S 2 3でN O）には、S 2 1で取得した未認証航法メッセージを、正規の航法メッセージであると判断せず、処理を終了する。このS 2 3～S 2 4が簡易判断部に相当する。

[0056] なお、S 2 3でN Oであった場合には、S 2 1で取得した未認証航法メッセージを、正規の航法メッセージでないと判断する構成としてもよい。

[0057] <実施形態1のまとめ>

実施形態1によれば、測位に用いた複数の航法メッセージのうち、1つの航法メッセージについて、認証センタ120を用いて車載機200で認証が成立すると、測位に用いたその他の航法メッセージについては、発信時刻をもとに、正規のものであるかを判断することが可能になる。従って、測位に用いたその他の航法メッセージについて、車載機200が認証センタ120からHマトリクスを受信しなくてもよくなる分だけ、認証センタ120の通信処理負荷を軽減できる。

[0058] リピータやシミュレータが用いられなければ、測位に用いた複数の航法メッセージに含まれる発信時刻は一致する。実施形態1では、この発信時刻が、認証が成立した航法メッセージと一致するか否かによって、正規の航法メッセージかを判断するので、リピータやシミュレータが用いられた場合に、航法メッセージを正規の航法メッセージと判断しないようにすることができる。よって、正規の航法メッセージと判断する精度を高めることができる。

<変形例1>

実施形態1では、測位に用いた複数の航法メッセージのうちの、認証済航法メッセージに含まれる発信時刻と未認証航法メッセージに含まれる発信時

刻とが一致するか否かによって、未認証航法メッセージが正規のものを判断する構成を説明したが、必ずしもこれに限らない。

[0059] 例えば、同一のGPS衛星2について、認証済航法メッセージに含まれるGPS衛星2の軌道情報及びその認証済航法メッセージに含まれる発信時刻とから定まる衛星位置と、未認証航法メッセージに含まれるGPS衛星2の軌道情報及びその未認証航法メッセージに含まれる発信時刻とから定まる衛星位置とが一致するか否かによって、未認証航法メッセージが正規のものを判断する構成（以下、変形例1）としてもよい。変形例1は、車載機200の制御部220での処理が一部異なる点を除けば、実施形態1と同様である。詳しくは、変形例1では、制御部220での簡易判断処理の一部が、実施形態1と異なっている。

[0060] 航法メッセージには、周知のようにエフェメリスデータやアルマナックデータが含まれる。アルマナックデータには、航法メッセージの発信元のGPS衛星2に限らない、軌道上の全てのGPS衛星2についての軌道情報が含まれ、この軌道情報と航法メッセージの発信時刻とから、全てのGPS衛星2の衛星位置が算出できる。また、エフェメリスデータには、航法メッセージの発信元のGPS衛星2についての軌道情報が含まれ、この軌道情報と航法メッセージの発信時刻とから、この航法メッセージの発信元のGPS衛星2のより精度の高い衛星位置が算出できる。

[0061] 変形例1では、このアルマナックデータに含まれる軌道情報と、エフェメリスデータに含まれる軌道情報のうち、アルマナックデータに含まれる軌道情報を用いる。以降では、アルマナックデータに含まれる軌道情報を単に軌道情報と呼ぶ。

[0062] <変形例1における簡易判断処理>

ここで、変形例1における車載機200の制御部220が実行する簡易判断処理について、図7に示すフローチャートを用いて説明を行う。図7のフローチャートも、測位に用いた複数の航法メッセージのうち、少なくとも1つの航法メッセージについて認証関連処理で認証が成立したときに開始する

構成とすればよい。図7のフローチャートも、測位に用いた複数の航法メッセージのうち、認証関連処理で認証を未だに行っていない航法メッセージについてそれぞれ処理を行う構成とすればよい。

[0063] 図7の例では、認証済航法メッセージの発信元のGPS衛星2がGPS衛星2aである場合を例に挙げて説明を行う。

[0064] まず、ステップS31では、前述のS21と同様にして、測位に用いた航法メッセージのうち、認証済航法メッセージ以外の未認証航法メッセージを取得する。

[0065] ステップS32では、測位に用いた認証済航法メッセージに含まれる発信時刻と、認証済航法メッセージに含まれるGPS衛星2aの軌道情報から、GPS衛星2aの位置を算出する。よって、発信時刻及び軌道情報が衛星位置算出用情報に相当する。

[0066] ステップS33では、測位に用いた未認証航法メッセージに含まれる発信時刻と、未認証航法メッセージに含まれるGPS衛星2aの軌道情報から、GPS衛星2aの位置を算出する。認証済航法メッセージの発信元のGPS衛星2a以外のGPS衛星2から受信した未認証航法メッセージに含まれる軌道情報からGPS衛星2aの衛星位置が算出できる理由は以下の通りである。認証済航法メッセージの発信元のGPS衛星2a以外のGPS衛星2が未認証衛星に相当する。

[0067] アルマナックデータに含まれる軌道情報には、未認証航法メッセージの発信元のGPS衛星2以外のGPS衛星2aについての軌道情報も含まれている。また、衛星受信機230において1周期内に受信する複数の航法メッセージは、前述のリピータやシミュレータが用いられていなければ、発信時刻が一致する関係にある。よって、未認証航法メッセージに含まれる発信時刻と軌道情報とからでも、GPS衛星2aの衛星位置が算出できる。

[0068] ステップS34では、S32で算出したGPS衛星2aの衛星位置と、S33で算出したGPS衛星2aの衛星位置とが一致しているか否かを判定する。ここで言うところの一致とは、完全に一致する場合だけでなく、誤差程

度の範囲内で略一致する場合も含むものとする。このS 3 4が整合性判定部に相当する。

[0069] 前述のリピータやシミュレータが用いられていなければ、測位に用いられた未認証航法メッセージと認証済航法メッセージとは発信時刻が一致する筈である。従って、リピータやシミュレータが用いられていなければ、未認証航法メッセージに含まれる発信時刻と軌道情報とから、認証済航法メッセージに含まれる発信時刻と軌道情報とから算出されるGPS衛星2 aの衛星位置と同じ衛星位置が算出できる。従って、リピータやシミュレータが用いられていなければ、S 3 2で算出したGPS衛星2 aの衛星位置と、S 3 3で算出したGPS衛星2 aの衛星位置とが一致することになる。

[0070] ステップS 3 5では、衛星位置が一致していると判定した場合（S 3 5でYES）には、認証済航法メッセージに含まれていた軌道情報及び発信時刻と整合性が取れる軌道情報及び発信時刻が未認証航法メッセージに含まれると判定し、S 3 6に進む。S 3 6では、S 3 1で取得した未認証航法メッセージを、正規の航法メッセージであると判断し、処理を終了する。一方、衛星位置が一致していないと判定した場合（S 3 5でNO）には、S 3 1で取得した未認証航法メッセージを、正規の航法メッセージであると判断せず、処理を終了する。このS 3 5～S 3 6も簡易判断部に相当する。

[0071] なお、S 3 5でNOであった場合には、S 3 1で取得した未認証航法メッセージを、正規の航法メッセージでないと判断する構成としてもよい。

[0072] <変形例1のまとめ>

変形例1によっても、実施形態1と同様に、測位に用いた複数の航法メッセージのうち、1つの航法メッセージについて、認証センタ120を用いて車載機200で認証が成立すると、測位に用いたその他の航法メッセージについては、軌道情報及び発信時刻から算出される衛星位置から、正規のものであるかを判断することが可能になる。従って、測位に用いたその他の航法メッセージについて、車載機200が認証センタ120からHマトリクスを受信しなくてもよくなる分だけ、認証センタ120の通信処理負荷を軽減で

きる。

[0073] リピータやシミュレータが用いられると、測位に用いた複数の航法メッセージに含まれる発信時刻が一致しないようになり、発信時刻と軌道情報とから算出される同一のGPS衛星2の衛星位置についても一致しないようになる。実施形態1では、この衛星位置が、認証が成立した航法メッセージと一致するか否かによって、正規の航法メッセージかを判断するので、リピータやシミュレータが用いられた場合に、航法メッセージを正規の航法メッセージと判断しないようにすることができる。よって、正規の航法メッセージと判断する精度を高めることができる。

[0074] なお、変形例1では、一致を判定する衛星位置として、認証済航法メッセージの発信元のGPS衛星2aの衛星位置を用いる場合を例に挙げて説明を行ったが、測位に用いた航法メッセージの発信元のGPS衛星2であれば、GPS衛星2a以外の衛星位置を用いる構成としてもよい。

[0075] <変形例2>

なお、前述の実施形態では、GPS衛星2から受信した航法メッセージのみを測位に用いた場合の例を挙げて説明を行ったが、QZS衛星3から受信した航法メッセージを測位に用いる構成としてもよい。この場合、QZS衛星3から受信した航法メッセージの認証についても、GPS衛星2の場合と同様にして行う構成とすればよい。

[0076] 変形例2の一例としては、QZS衛星3からモニタステーション110で受信した航法メッセージからRANDメッセージを生成し、このRANDメッセージをもとに認証センタ120でパリティデータを作成する。そして、作成したパリティデータをマスタコントロールステーション130に送り、そのパリティデータをマスタコントロールステーション130からQZS衛星3に送信する。QZS衛星3は、そのパリティデータを含んだ航法メッセージを地上に向けて放送する。

[0077] 車載機200は、QZS衛星3から受信した航法メッセージからRANDメッセージを作成し、このRANDメッセージと認証センタ120から取得

するHマトリクスとから比較パリティデータを作成する。そして、作成した比較パリティデータと、QZS衛星3から受信したパリティデータとを比較することで認証を行う構成とすればよい。

[0078] <変形例3>

前述の実施形態で説明した航法メッセージ認証型の認証方法はあくまで一例であり、認証機関へのアクセスが必要な認証方法であれば、他の認証方法を用いる構成（以下、変形例3）としてもよい。

[0079] <変形例4>

前述の実施形態では、車両で用いられる車載機200を例に挙げて説明を行ったが、必ずしもこれに限らない。例えば、車載機200と同様の航法メッセージ受信装置を、ユーザに携帯される携帯端末等に適用する構成としてもよい。

[0080] 以上、本開示に係る実施形態および構成を例示したが、本開示に係る実施形態および構成は、上述した各実施形態および各構成に限定されるものではない。異なる実施形態および構成にそれぞれ開示された技術的要素を適宜組み合わせ得られる実施形態および構成についても本開示に係る実施形態および構成の範囲に含まれる。

請求の範囲

[請求項1]

衛星測位システムで用いられる人工衛星からの航法メッセージを受信する衛星受信機（230）と、

前記人工衛星から受信した前記航法メッセージに応じた認証用情報を、認証センタから受信する認証用情報受信部（S5）と、

前記衛星受信機で受信した前記航法メッセージが正規の航法メッセージであることの認証を、当該航法メッセージに応じて前記認証用情報受信部で受信した認証用情報を用いて行うセンタ使用認証部（S9～S11）とを備える航法メッセージ受信装置（200）であって、

前記航法メッセージには、複数の前記人工衛星間で整合性が取れる整合情報が含まれており、

前記センタ使用認証部で認証が成立した航法メッセージに含まれる整合情報と整合性が取れる情報が、前記センタ使用認証部で認証が成立した航法メッセージの発信元とは異なる前記人工衛星である未認証衛星から前記衛星受信機で受信した航法メッセージに含まれるか否かを判定する整合性判定部（S22、S34）と、

前記整合性判定部によって、前記整合情報と整合性が取れる情報が前記未認証衛星から前記衛星受信機で受信した航法メッセージに含まれると判定された場合には、前記衛星受信機で受信した前記航法メッセージが正規のものであると判断する一方、前記整合性判定部によって、前記整合情報と整合性が取れる情報が前記未認証衛星から前記衛星受信機で受信した航法メッセージに含まれていないと判定された場合には、前記衛星受信機で受信した前記航法メッセージが正規のものであると判断しない簡易判断部（S23、S24、S35、S36）と、をさらに備える航法メッセージ受信装置。

[請求項2]

請求項1において、

前記整合情報は、前記航法メッセージの発信時刻であって、

前記整合性判定部（S32）は、前記センタ使用認証部で認証が成

立した航法メッセージに含まれる発信時刻と、前記未認証衛星から前記衛星受信機で受信した航法メッセージに含まれる発信時刻とが一致するか否かによって、前記整合性が取れる情報が前記未認証衛星から前記衛星受信機で受信した航法メッセージに含まれているか否かを判定する航法メッセージ受信装置。

[請求項3]

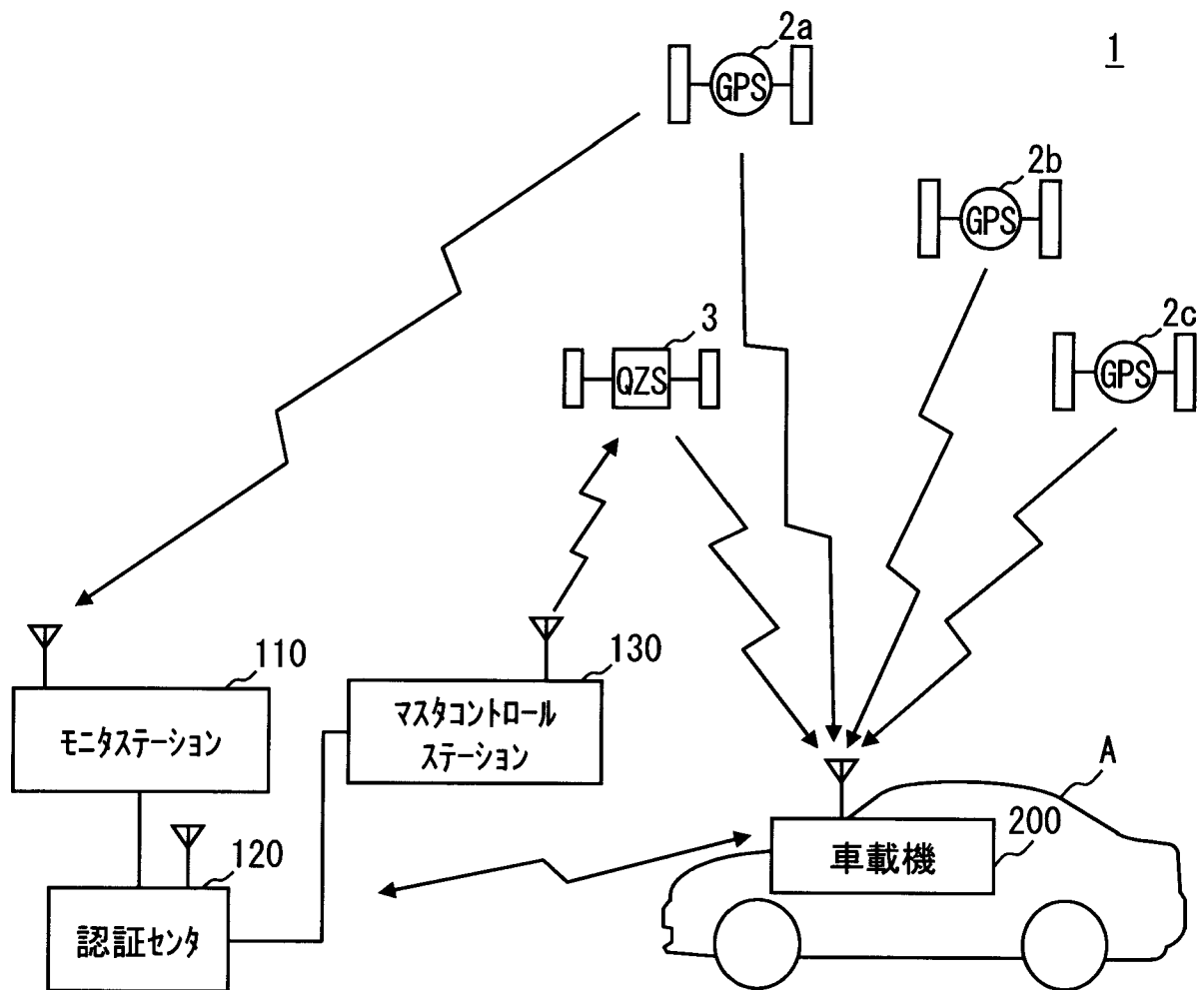
請求項1において、

前記航法メッセージには、当該航法メッセージの発信元の前記人工衛星だけでなく、当該人工衛星以外の前記人工衛星の衛星位置を算出できる衛星位置算出用情報が含まれており、

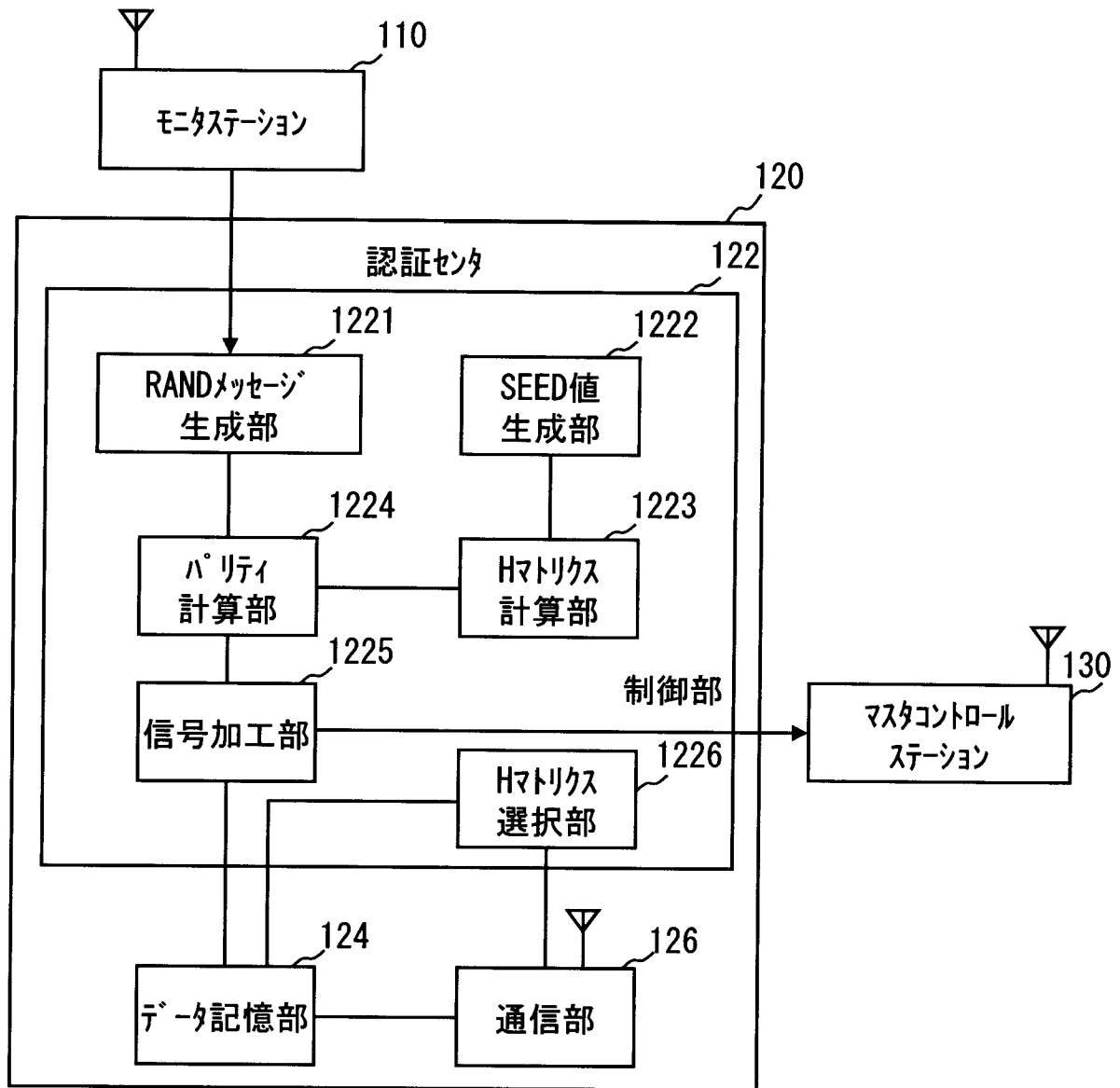
前記整合情報は、前記衛星位置算出用情報であって、

前記整合性判定部（S34）は、前記センタ使用認証部で認証が成立した航法メッセージに含まれる前記衛星位置算出用情報から算出できる前記未認証衛星の衛星位置と、前記未認証衛星から前記衛星受信機で受信した航法メッセージに含まれる前記衛星位置算出用情報から算出できる前記未認証衛星の衛星位置とが一致するか否かによって、前記整合性が取れる情報が前記未認証衛星から前記衛星受信機で受信した航法メッセージに含まれているか否かを判定する航法メッセージ受信装置。

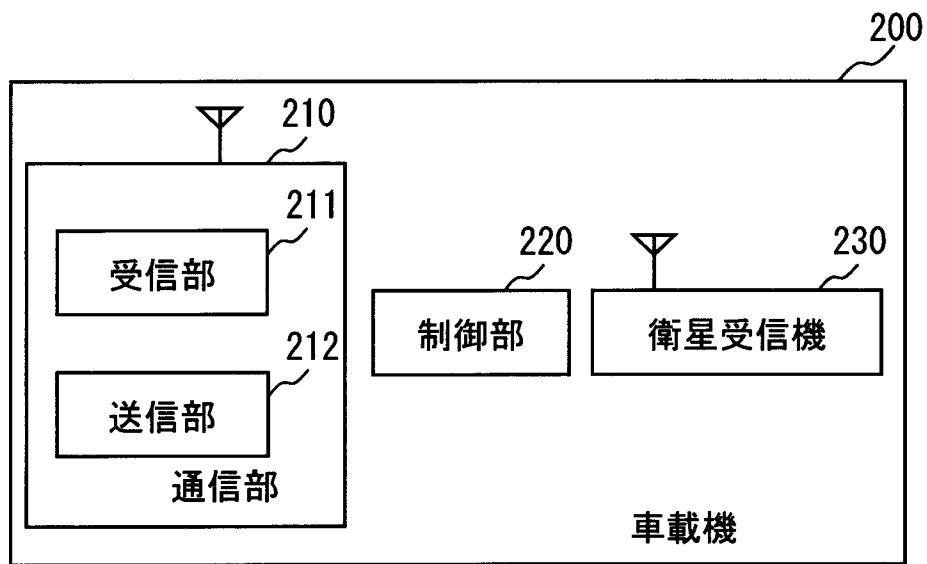
[図1]



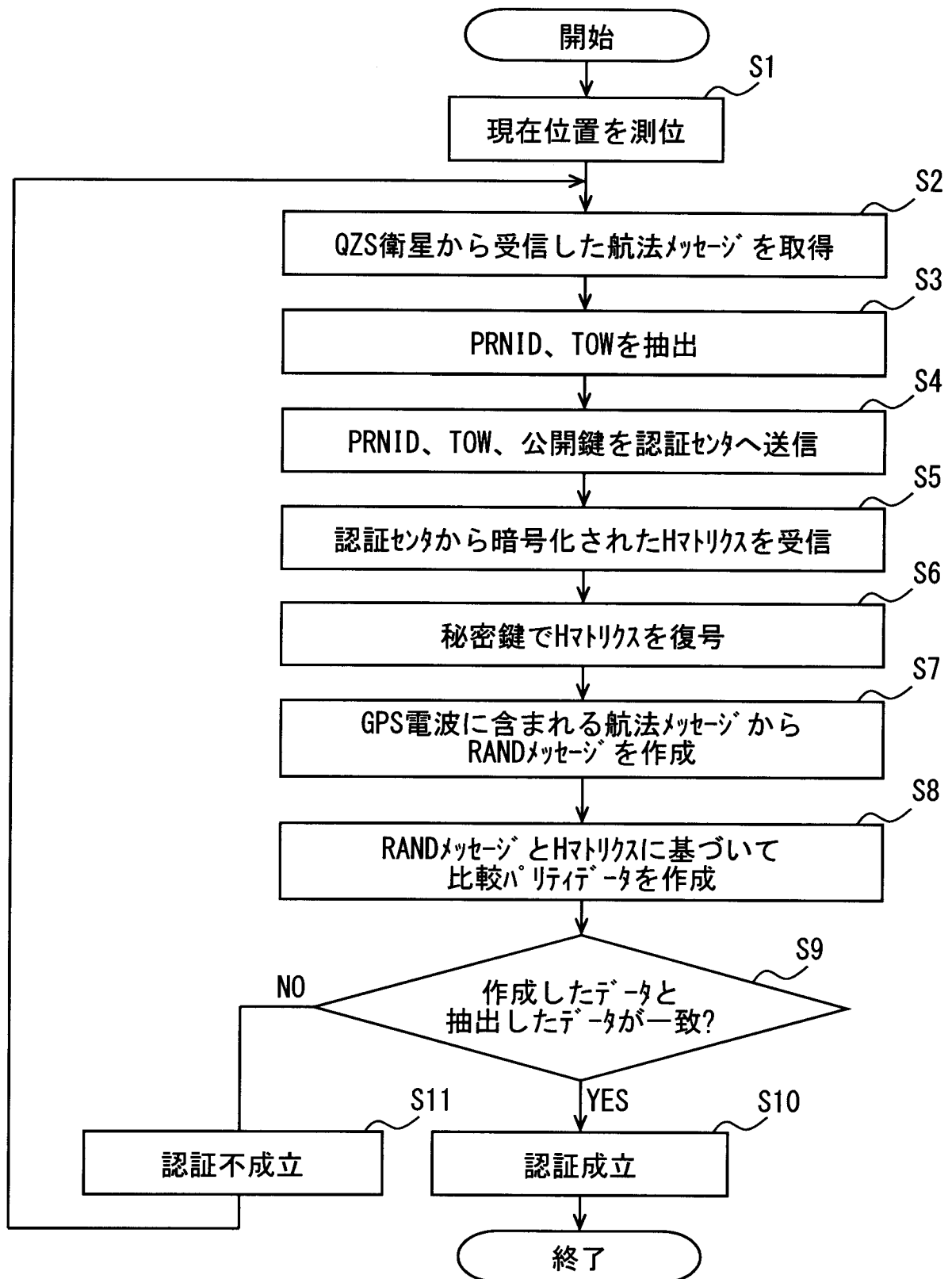
[図2]



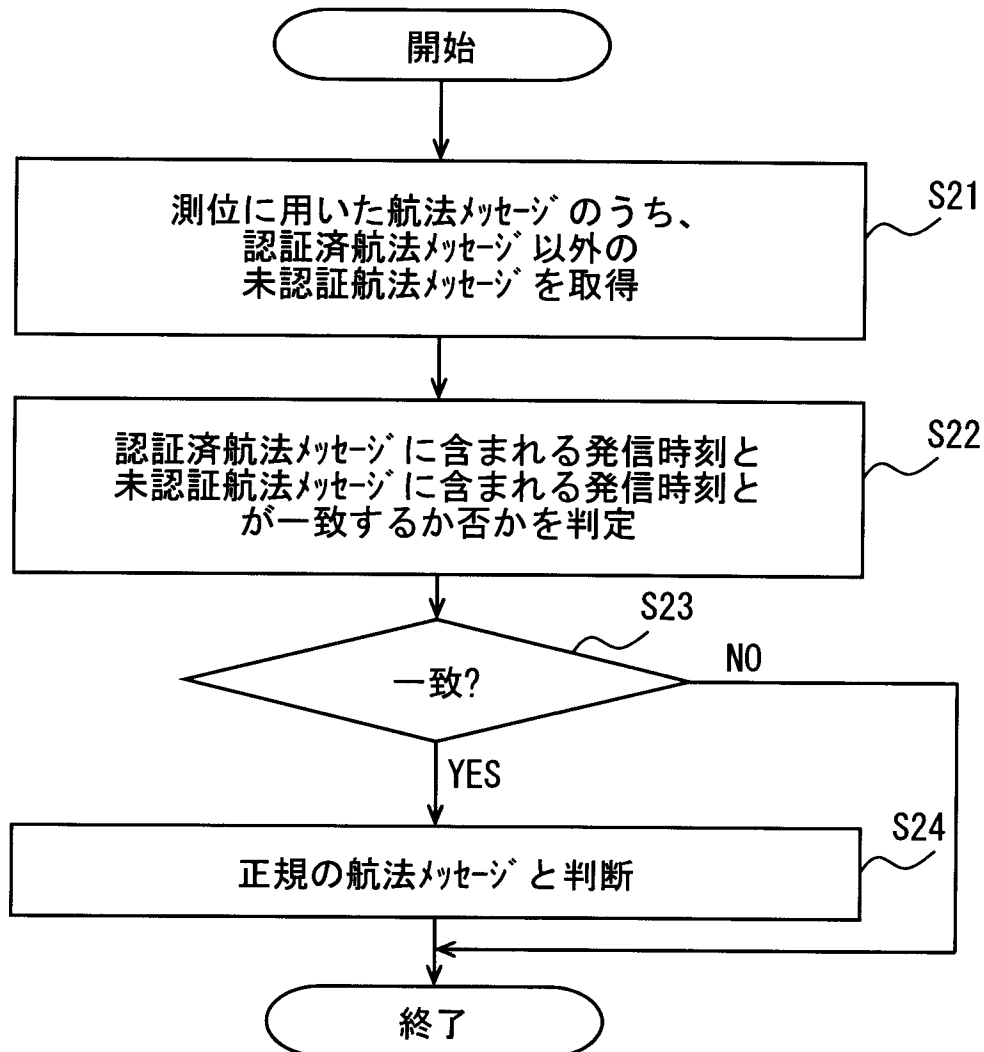
[図3]



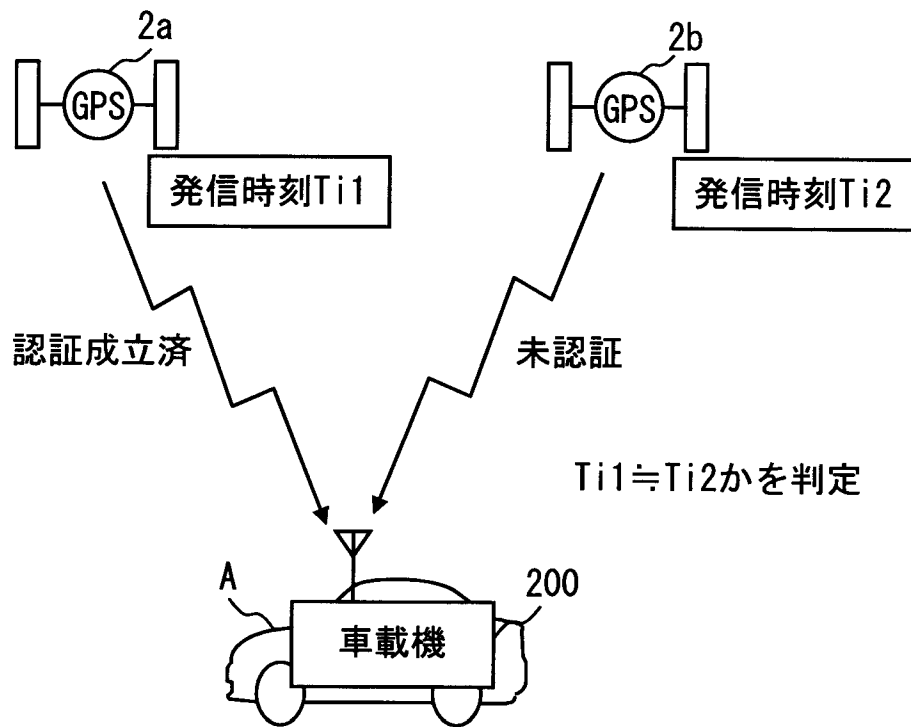
[図4]



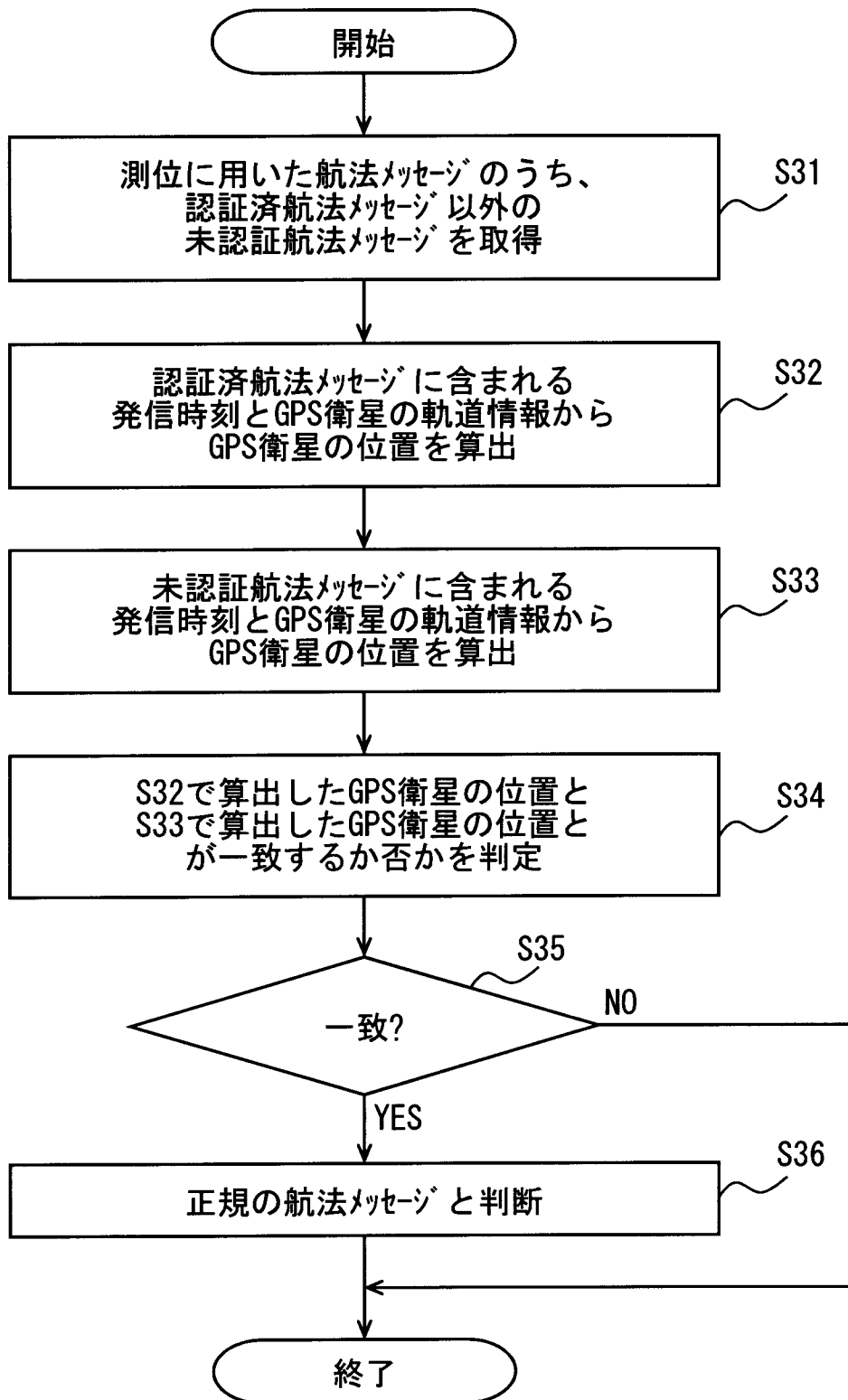
[図5]



[図6]



[図7]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2015/000744

A. CLASSIFICATION OF SUBJECT MATTER

G01S19/05(2010.01)i, G01S19/21(2010.01)i

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)

G01S5/00-5/14, 19/00-19/55, G01C21/00-21/36, 23/00-25/00, G08G1/00-99/00, G09C1/00-5/00, H04K1/00-3/00, H04L9/00-9/04

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

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2015
Kokai Jitsuyo Shinan Koho	1971-2015	Toroku Jitsuyo Shinan Koho	1994-2015

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2013-130395 A (Hitachi Information & Control Solutions, Ltd.), 04 July 2013 (04.07.2013), entire text; all drawings (Family: none)	1-3
A	JP 2013-529289 A (Qualcomm, Inc.), 18 July 2013 (18.07.2013), entire text; all drawings & US 2011/0227787 A1 & US 2013/0328719 A1 & WO 2011/119640 A1 & EP 2550543 A1 & CN 102906589 A & KR 10-2013-0014558 A & KR 10-2014-0017667 A	1-3

☒ Further documents are listed in the continuation of Box C.

☐ 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
12 May 2015 (12.05.15)

Date of mailing of the international search report
26 May 2015 (26.05.15)

Name and mailing address of the ISA/
Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2015/000744

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2002-183188 A (Fuji Xerox Co., Ltd.), 28 June 2002 (28.06.2002), entire text; all drawings (Family: none)	1-3
A	US 2010/0134352 A1 (Martin THOMSON et al.), 03 June 2010 (03.06.2010), entire text; all drawings & WO 2010/065253 A2	1-3

A. 発明の属する分野の分類（国際特許分類（I P C））

Int.Cl. G01S19/05(2010.01)i, G01S19/21(2010.01)i

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（I P C））

Int.Cl. G01S5/00-5/14, 19/00-19/55, G01C21/00-21/36, 23/00-25/00, G08G1/00-99/00, G09C1/00-5/00, H04K1/00-3/00, H04L9/00-9/04

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1 9 2 2 - 1 9 9 6 年
日本国公開実用新案公報	1 9 7 1 - 2 0 1 5 年
日本国実用新案登録公報	1 9 9 6 - 2 0 1 5 年
日本国登録実用新案公報	1 9 9 4 - 2 0 1 5 年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
A	JP 2013-130395 A（株式会社日立情報制御ソリューションズ） 2013.07.04, 全文全図（ファミリーなし）	1-3
A	JP 2013-529289 A（クアルコム, インコーポレイテッド）2013.07.18, 全文全図 & US 2011/0227787 A1 & US 2013/0328719 A1 & WO 2011/119640 A1 & EP 2550543 A1 & CN 102906589 A & KR 10-2013-0014558 A & KR 10-2014-0017667 A	1-3

☒ C 欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日

1 2 . 0 5 . 2 0 1 5

国際調査報告の発送日

2 6 . 0 5 . 2 0 1 5

国際調査機関の名称及びあて先

日本国特許庁（I S A / J P）

郵便番号 1 0 0 - 8 9 1 5

東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員）

目黒 大地

2 S

5 0 6 0

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 2 5 8

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
A	JP 2002-183188 A (富士ゼロックス株式会社) 2002.06.28, 全文全図 (ファミリーなし)	1-3
A	US 2010/0134352 A1 (Martin THOMSON et al) 2010.06.03, 全文全図 & WO 2010/065253 A2	1-3