

明 細 書

発明の名称： 航法メッセージ認証型測位装置

関連出願の相互参照

[0001] 本出願は、2014年2月6日に提出された日本国特許出願2014-21632号に基づくものであり、ここにその記載内容を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受信する航法メッセージの認証を行う航法メッセージ認証型測位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測位装置の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、悪意の行為者が位置情報の改竄やなりすましを行う虞がある。

[0005] これに対して、特許文献1には、受信機（つまり、測位装置）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、測位装置は、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、測位装置は、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。

[0006] また、従来、測位装置に短時間の電源オフ状態が存在した場合でも、航法メッセージに含まれる軌道情報としてのエフェメリスデータをバックアップ

メモリに保持しておくことで、再度のエフェメリスデータの収集を省き、測位開始時間を早くするホットスタートと呼ばれる再起動の方法が知られている（例えば特許文献2）。

[0007] 他にも、軌道情報としてのアルマナックデータをバックアップメモリに保持しておくことで、再度のアルマナックデータの収集を省き、測位開始時間を早くするウォームスタートと呼ばれる再起動の方法も知られている。エフェメリスデータはアルマナックデータよりも詳細な軌道情報であって、有効期限がアルマナックデータよりも短い。

[0008] ウォームスタートは、測位装置の電源オフ時間が、バックアップメモリに保持しておくエフェメリスデータの有効期限を超えて続いたが、バックアップメモリに保持しておくアルマナックデータの有効期限は超えていない場合の再起動の方法である。ウォームスタート時には、エフェメリスデータの収集が必要になる分だけホットスタートより測位開始時間は遅くなるが、アルマナックデータの再度の収集が必要でない分だけ測位開始時間を早くできる。

[0009] 本願発明者は、航法メッセージ認証型測位装置に関して、以下を見出した。

[0010] 特許文献1に開示の技術をホットスタート時やウォームスタート時に用いる場合、信頼度の高い測位を行うためには、測位装置の再起動後に、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、認証センタと通信を行って航法メッセージの認証を行う分だけ測位開始時間が遅れる虞がある。

先行技術文献

特許文献

[0011] 特許文献1：日本国公開特許公報2013-130395号

特許文献2：日本国公開特許公報2000-292521号

発明の概要

[0012] 本開示の目的は、信頼度のより高い測位を実現しながらも、ホットスター

ト時やウォームスタート時における測位開始時間の遅れを抑えることを可能にする航法メッセージ認証型測位装置を提供することにある。

[0013] 本開示の一例に係る航法メッセージ認証型測位装置は、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、認証センタから取得する認証用情報取得部と、認証用情報取得部で取得した認証用情報を用いて、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ことの認証を行う認証部と、衛星受信機で複数の人工衛星から受信した航法メッセージをもとに自装置（航法メッセージ認証型測位装置）の位置を測位する測位部とを備える。航法メッセージ認証型測位装置は、衛星受信機が受信した航法メッセージのうちの、人工衛星の軌道情報を少なくとも含む情報である衛星情報と、その航法メッセージについての認証部での認証結果とを、自装置の電源オフの間も保存しておく保存部と、自装置の再起動時に、保存部に保存しておいた軌道情報を利用して、人工衛星の捕捉を行う捕捉部と、保存部に保存しておいた認証結果が認証成立であった航法メッセージが存在した場合、保存部に保存しておいた航法メッセージの衛星情報に含まれる情報を用いて、航法メッセージと、航法メッセージの発信元の人工衛星から再起動後に受信した航法メッセージとに整合性があ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性があると判定した場合には、整合性があると判定した航法メッセージの発信元の人工衛星を、測位部での測位に用いる人工衛星として選択する選択部とを備える。測位部は、捕捉部で捕捉した人工衛星のうちの、選択部で選択した人工衛星から受信した航法メッセージを用いて自装置の位置を測位する。

[0014] これによれば、自装置の再起動時に、保存部に保存しておいた軌道情報を利用して、捕捉部で人工衛星の捕捉を行うので、ホットスタートやウォームスタートを行うことができる。また、同一の人工衛星についての、自装置の電源オフ前に認証部で認証成立していた航法メッセージと、自装置の再起動後に受信した航法メッセージとに整合性がある場合には、再起動後に受信し

た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、整合性判定部で整合性があると判定した航法メッセージは正規のものである可能性が高く、その航法メッセージの発信元の人工衛星から再起動後に受信する航法メッセージを用いれば、信頼度のより高い測位を行うことが可能と言える。従って、選択部で選択した人工衛星から受信した航法メッセージを用いることで、信頼度のより高い測位を行うことが可能となる。

[0015] さらに、測位部は、捕捉部で捕捉した人工衛星のうちの、選択部で選択した人工衛星から受信した航法メッセージを用いて自装置の位置を測位するので、ホットスタート時やウォームスタート時に、信頼度のより高い測位を行うことが可能となる。また、本開示によれば、認証用情報取得部で取得した認証用情報を用いて認証部で認証を行わなくても、選択部で選択した人工衛星から受信した航法メッセージを用いることで、信頼度のより高い測位を行うことが可能となる。よって、選択部で選択した人工衛星については、認証用情報取得部で取得した認証用情報を用いて認証部で認証を行う時間を削減することができ、ホットスタート時やウォームスタート時における測位開始時間の遅れを抑えることが可能になる。

図面の簡単な説明

[0016] 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における航法メッセージ認証システムの概略的な構成の一例を示す図であり、

[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り、

[図3]図3は、第1車載機の概略的な構成の一例を示すブロック図であり、

[図4]図4は、第1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り、

[図5]図5は、第1車載機のメモリに保存される一時保存情報の一例を示す図であり、

[図6]図6は、第1車載機での再起動方法選択処理の流れの一例を示すフロー

チャートであり、

[図7]図7は、実施形態1における第1車載機での初期測位関連処理の流れの一例を示すフローチャートであり、

[図8]図8は、第1車載機のメモリに保存される認証情報リストの一例を示す図であり、

[図9]図9は、第1車載機での測位情報送信処理の流れの一例を示すフローチャートであり、

[図10]図10は、第2車載機の概略的な構成の一例を示すブロック図であり、

[図11]図11は、変形例1における第1車載機での初期測位関連処理の流れの一例を示すフローチャートであり、

[図12]図12は、変形例4における第1車載機での認証確認用情報送信処理の流れの一例を示すフローチャートであり、

[図13]図13は、第1車載機から送信される認証情報リストの一例を示す図である。認証確認用情報の一例を示す図であり、

[図14]図14は、変形例4における第2車載機での確認処理の流れの一例を示すフローチャートであり、

[図15]図15は、第2車載機のメモリに保存される認証情報リストの一例を示す図である。

発明を実施するための形態

[0017] 以下、本開示の実施形態について図面を用いて説明する。

[0018] (実施形態1)

図1に示すように、実施形態1における航法メッセージ認証システム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、第1車載機200、及び第2車載機300を含む。第1車載機200を用いる車両を車両A、第2車載機300を用いる車両を車両Bとする。第1車載機200及び第2車載機300が本開示の航法メッセージ認証型測位装置に相当する。

[0019] <航法メッセージ認証システム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～２fが発信するGPS電波を受信する。GPS衛星２a～２fが本開示の人工衛星に相当する。以降では、GPS衛星２a～２f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。

[0020] 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。

[0021] 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、第１車載機２００や第２車載機３００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。

[0022] 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。

[0023] 第１車載機２００及び第２車載機３００は、航法メッセージ認証型（NMA : Navigation Message Authentication）車載機である。第１車載機２００

及び第2車載機300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。また、第1車載機200及び第2車載機300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第1車載機200及び第2車載機300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。第1車載機200及び第2車載機300の詳細な説明は、後に行う。

[0024] <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。

[0025] 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と同じでよい。

[0026] 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メッセージを生成する。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TOC、AFO、AF1とが順番に並んでいる。TOW、TOC、AFO、AF1が信号の発信時刻を特定するデータである。さらに、その後に、アンチスプーフフラグであるASFlag、衛星番号であるPRN (Pseudo Random Noise) IDが追加されている。

[0027] TOWとPRN IDを含んでいるRANDは、どのGPS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、TOWが6秒ごとに変化し、ま

た、PRN IDを含んでいるので、モニタステーション110が受信したGPS衛星2ごと、かつ、6秒ごとにRANDを生成することになる。

[0028] SEED値生成部1222は、PCクロックを入力として乱数を発生させることで、SEED値を生成する。

[0029] Hマトリクス計算部1223は、SEED値生成部1222が生成したSEED値を使い、このSEED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LDPC (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。

[0030] パリティ計算部1224は、RANDメッセージ生成部1221が生成したRAND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。

[0031] 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RANDメッセージを、QZS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。

[0032] 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RANDメッセージ、Hマトリクス、Hマトリクスの計算に用いたSEED値を対応付けて、データ記憶部124に記憶する。

[0033] この信号加工部1225は、RANDメッセージ生成部1221がRANDメッセージを生成するごとに、RANDメッセージとパリティデータをQZS衛星3に送信させる航法メッセージに挿入する。よって、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も、RANDメッセージ生成部1221がRANDメッセージを生成するごとに、処理を実行する。

[0034] Hマトリクス選択部1226は、第1車載機200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 マトリクスを第 1 車載機 2 0 0 へ返信する。

[0035] <第 1 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、第 1 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、この第 1 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。

[0036] 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、狭域通信機能と広域通信機能を備えている。狭域通信機能は、例えば、通信距離が数百メートルである。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。狭域通信機能により、第 2 車載機 3 0 0 の通信部 3 1 0 といわゆる車車間通信を行い、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。

[0037] 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。そして、受信した電波に含まれる航法メッセージを制御部 2 2 0 に出力する。衛星受信機 2 3 0 から制御部 2 2 0 へ逐次行われる出力の 1 周期内に、複数の G P S 衛星 2 の航法メッセージを衛星受信機 3 3 0 で受信していた場合には、1 周期内に、その複数の G P S 衛星 2 の航法メッセージが制御部 2 2 0 に出力されることになる。

[0038] 制御部 2 2 0 は、C P U、メモリ 2 2 0 a を含むメモリ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。メモリには R O M や R A M 等があり、メモリ 2 2 0 a は、バックアップ R A M 等の不揮発性の一時保存メモリであるものとする。また、C P U が、R A M の一時記憶機能を利用しつつ R O M に記憶されているプログラムを実行することで、認証関連処理（図 4 参照）や一時保存処理や再起動方法選択処理（図 6 参照）

や初期測位関連処理（図 7）や認証情報保存処理や測位情報送信処理（図 9 参照）等の各種処理を実行する。

[0039] 概略として、認証関連処理は、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である。一時保存処理は、航法メッセージに含まれる情報と、その航法メッセージについての認証関連処理での認証結果とをメモリ 220a に一時的に保存する処理である。

[0040] 再起動選択処理は、第 1 車載機 200 の電源が一旦オフになった後、第 1 車載機 200 の電源が再度オンになったときに行われる処理である。初期測位関連処理は、ホットスタートやウォームスタート時に行われる初期測位に関連する処理である。認証情報保存処理は、測位に用いた GPS 衛星 2 についての後述の NMA 認証情報及びみなし認証情報といった認証情報をメモリ 220a に保存する処理である。測位情報送信処理は、測位した位置とその測位に用いた GPS 衛星 2 についての認証情報を送信する処理である。

[0041] <認証関連処理>

ここで、第 1 車載機 200 の制御部 220 での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、GPS 衛星 2 から衛星受信機 230 で受信した航法メッセージの出力を制御部 220 が受けたときに開始する構成とすればよい。ここでは、1 周期分の出力時に、複数の GPS 衛星 2 の航法メッセージが出力され、この複数の GPS 衛星 2 の航法メッセージについて認証を行うように処理を繰り返すものとして説明を行う。

[0042] 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。

[0043] まず、S1 では、衛星受信機 230 から出力された、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を取得する。

- [0044] S 2では、Q Z S衛星3から受信した航法メッセージを、受信部2 1 1から取得する。S 3では、S 1で取得した航法メッセージから、P R N I D、T O Wを抽出する。
- [0045] S 4では、S 3で抽出したP R N I DとT O Wを公開鍵とともに、送信部2 1 2から認証センタ1 2 0へ送信する。前述したように、認証センタ1 2 0は、このP R N I DとT O W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第1車載機2 0 0へ送信する。第1車載機2 0 0から認証センタ1 2 0に送信したP R N I DとT O Wとにより定まるHマトリクスが、本開示の認証用情報に相当する。
- [0046] S 5では、認証センタ1 2 0から送信されたHマトリクスを受信部2 1 1から取得する。よって、このS 5が本開示の認証用情報取得部に相当する。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。
- [0047] S 7では、G P S衛星2から受信したG P S電波に含まれる航法メッセージのうち、S 4で送信したP R N I Dと同じP R N I Dを含んでいる航法メッセージから、R A N Dメッセージを作成する。
- [0048] S 8では、S 7で作成したR A N D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。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。
- [0049] S 6で復号したHマトリクスは、認証センタ1 2 0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1 2 0のパリティ計算部1 2 2 4は、このHマトリクスとR A N D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。
- [0050] 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R A N Dメッセージが、認証センタ1 2 0が作成したR A N Dメッセージと同じであると考えられることができる。
- [0051] 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（Ｓ９でＹＥＳ）には、Ｓ１０に進み、認証成立とする。一方、２つのパリティデータが一致しない場合（Ｓ９でＮＯ）には、Ｓ１１に進み、認証不成立とする。よって、このＳ９～Ｓ１１が本開示の認証部に相当する。Ｓ１０、Ｓ１１の後には、Ｓ１２に進む。

[0052] Ｓ１２では、対象とする全ＧＰＳ衛星２、すなわち、衛星受信機２３０から出力された１周期分の全ＧＰＳ衛星２の航法メッセージについて、認証成立か不成立かの判断が完了した場合（Ｓ１２でＹＥＳ）には、図４の処理を終了する。一方、１つでも認証成立か不成立かの判断が完了していない場合（Ｓ１２でＮＯ）には、Ｓ１２に戻って処理を繰り返す。この認証関連処理での認証を以下ではＮＭＡ認証と呼ぶ。

[0053] なお、衛星受信機２３０から出力された１周期分の全ＧＰＳ衛星２の航法メッセージについて、認証を行う必要はなく、例えば４つなどの測位に必要な数のＧＰＳ衛星２に絞ったり、後述する初期測位関連処理に必要な数のＧＰＳ衛星２に絞って行う構成としたりしてもよい。

[0054] ＜一時保存処理＞

また、第１車載機２００の制御部２２０は、衛星受信機２３０から出力された直近の航法メッセージに含まれる情報と、その航法メッセージについての前述の認証関連処理での認証結果（以下、ＮＭＡ認証情報）とをメモリ２２０ａに一時的に保存する一時保存処理を行う。衛星受信機２３０からの１周期分の出力時に、複数のＧＰＳ衛星２の航法メッセージが出力される場合には、この複数の航法メッセージが全て直近の航法メッセージに該当することになる。

[0055] 一時保存処理でメモリ２２０ａに保存する情報（以下、一時保存情報）としては、航法メッセージに含まれるＰＲＮ ＩＤ、エフェメリスデータやアルマナックデータといった軌道情報、発信時刻や、航法メッセージを受信した時刻、ＮＭＡ認証情報がある。エフェメリスデータはホットスタートに必要な軌道情報であって、アルマナックデータはウォームスタートに必要な軌道情報である。

- [0056] ここで、図5を用いて、一時保存情報の一例について説明を行う。図5の例では、例えば第1車載機200からGPS衛星2a～2dの4つのGPS衛星2が観測可能であって、GPS衛星2a、2bの航法メッセージまでがNMA認証が成立済であるものとする。ここでは、GPS衛星2aのPRN IDは「1」、GPS衛星2bのPRN IDは「3」、GPS衛星2cのPRN IDは「5」、GPS衛星2dのPRN IDは「10」とする。
- [0057] メモリ220aに保存する一時保存情報は、図5に示すように、航法メッセージの発信元のGPS衛星2ごとに、PRN IDと、そのPRN IDが示すGPS衛星2についてNMA認証が成立しているか否かを示すNMA認証情報と、軌道情報と、発信時刻と、受信時刻とが対応付けられている構成とすればよい。軌道情報と発信時刻と受信時刻とが本開示の衛星情報に相当する。
- [0058] NMA認証情報は、例えば、図5に示すように、認証成立であるか（図中の「T」）、認証不成立若しくは未認証であるか（図中の「F」）の2つの状態を表す2値のフラグとすればよい。他にも、認証成立と認証不成立と未認証との3つの状態を表す情報としてもよい。よって、図5の例では、GPS衛星2a、2bについては「T」となり、GPS衛星2c、2dについては「F」となる。
- [0059] メモリ220aに保存する一時保存情報については、衛星受信機230から新たな1周期分の出力を制御部220が受けた場合に、その新たな出力をもとに逐次更新していくものとする。よって、現在位置において第1車載機200が観測可能なGPS衛星2についての一時保存情報が残ってゆくことになる。また、NMA関連情報については、衛星受信機230から新たな1周期分の出力を制御部220が受けた場合以外にも、逐次更新してゆく構成とすればよい。詳しくは以下の通りである。
- [0060] 前述の認証関連処理では、対象とする全GPS衛星2についてNMA認証を逐次行うことになる。しかしながら、1つのGPS衛星2についてNMA認証を行うにも時間がかかるため、対象とする全GPS衛星2についてNM

A認証を行うまでには、一部のGPS衛星2についてしかNMA認証が行われていない状況が生じる。よって、NMA認証情報は、新たにGPS衛星2についてのNMA認証が行われるごとに更新する構成とすればよい。例えば、図5において、GPS衛星2の航法メッセージについてNMA認証が成立した場合には、GPS衛星2cについてのNMA関連情報は「F」から「T」に更新される。

[0061] また、メモリ220aは前述したようにバックアップメモリであり、例えば車両Aのイグニッション電源がオフになって、第1車載機200の電源がオフになった場合にも、一時保存情報の記憶を維持する。よって、メモリ220aが本開示の保存部に相当する。第1車載機200の電源がオフになったときに、前述の認証関連処理で対象とする全GPS衛星2のうちの一部についてしかNMA認証が完了していなかった場合には、この一部のGPS衛星2については、NMA認証情報が「F」となる状況が生じることになる。

[0062] <再起動方法選択処理>

続いて、第1車載機200の制御部220での再起動方法選択処理について、図6に示すフローチャートを用いて説明を行う。図6のフローチャートは、例えば、第1車載機200の電源が一旦オフになった後、第1車載機200の電源が再度オンになったときに開始する構成とすればよい。

[0063] まず、S21では、第1車載機200の電源がオフになっていた期間を特定する。第1車載機200の電源がオフになっていた期間（以下、電源オフ期間）は、RTC（Real Time Clock）のカウントから特定すればよい。

[0064] S22では、電源オフ期間が第1の所定期間内であった場合（S22でYES）には、S23に移る。一方、第1の所定期間内でなかった場合（S22でNO）には、S25に移る。ここで言うところの第1の所定期間は、エフェメリスデータの有効期限を超えない値であればよく、例えば15分としてもよいし、2時間などとしてもよい。

[0065] S23では、ホットスタートを行うことを選択し、S24に移る。S24では、メモリ220aに一時保存情報が存在するGPS衛星2について、一

時保存情報に含まれる軌道情報のうちのエフェメリスデータを用いてGPS電波を捕捉し、図6の処理を終了する。よって、S24が本開示の捕捉部に相当する。

[0066] S22で電源オフ期間が第1の所定期間内でなかった場合のS25では、電源オフ期間が第2の所定期間内であった場合（S25でYES）には、S26に移る。一方、第2の所定期間内でなかった場合（S25でNO）には、S28に移る。ここで言うところの第2の所定期間は、第1の所定期間よりも長い期間であって、アルマナックデータの有効期限を超えない値であればよく、例えば2時間としてもよいし、1日としてもよいし、1週間などとしてもよい。

[0067] S26では、ウォームスタートを行うことを選択し、S27に移る。S27では、メモリ220aに一時保存情報が存在するGPS衛星2について、一時保存情報に含まれる軌道情報のうちのアルマナックデータを用いてGPS電波を捕捉し、図6の処理を終了する。よって、S27も本開示の捕捉部に相当する。

[0068] S25で電源オフ期間が第2の所定期間内でなかった場合のS28では、コールドスタートを行うことを選択し、S29に移る。S29では、軌道情報を用いずに、全てのGPS衛星2を対象としてGPS電波の捕捉を試み、図6の処理を終了する。

[0069] <初期測位関連処理>

続いて、第1車載機200の制御部220での初期測位関連処理について、図7に示すフローチャートを用いて説明を行う。図7のフローチャートは、例えば、再起動方法選択処理でホットスタート及びウォームスタートのいずれかを選択したときに開始する構成とすればよい。

[0070] まず、S31では、メモリ220aに保存されている一時保存情報をもとに、第1車載機200の電源オフ前に航法メッセージのNMA認証が成立済であったGPS衛星2（以下、NMA認証済GPS衛星2）を抽出する。

[0071] S32では、NMA認証済GPS衛星2が存在した場合（S31でYES

）には、S 3 3に移る。一方、存在しなかった場合（S 3 1でNO）には、S 4 0に移る。

[0072] S 3 3では、メモリ220aに保存されている一時保存情報から、S 3 1で抽出したNMA認証済GPS衛星2についての、航法メッセージの発信時刻、及びその航法メッセージを第1車載機200で受信した受信時刻を取得する。

[0073] S 3 4では、S 3 1で抽出したNMA認証済GPS衛星2と同じGPS衛星2から第1車載機200の再度の電源オン（つまり、再起動）後に衛星受信機230で受信した航法メッセージを取得する。以下では、再起動後に衛星受信機230で受信した航法メッセージをNMA認証前の航法メッセージと呼ぶ。

[0074] S 3 5では、S 3 4で取得したNMA認証前の航法メッセージを受信した受信時刻を特定するとともに、この航法メッセージから、この航法メッセージの発信時刻を特定する。NMA認証前の航法メッセージを受信した受信時刻は、図示しないRTCで計時した値から特定する構成とすればよい。

[0075] S 3 6では、S 3 1で抽出したNMA認証済GPS衛星2について、NMA認証が成立済の航法メッセージとNMA認証前の航法メッセージとに経過時間に応じた整合性があるか否かを判定する。よって、S 3 6が本開示の整合性判定部に相当する。

[0076] 具体例としては、S 3 3で一時保存情報から取得した発信時刻（すなわち、メモリ220aに保存しておいたNMA認証成立済の航法メッセージの発信時刻）と、S 3 5で特定したNMA認証前の航法メッセージの発信時刻との発信時刻差と、両者の航法メッセージをそれぞれ受信した受信時刻差との差が閾値未満である場合に、整合性があると判定する。

[0077] ここで言うところの閾値とは、S 3 1で抽出したNMA認証済GPS衛星2が、上述の発信時刻差にあたる時間に移動することにより生じる伝搬時間のずれに相当する値とすればよい。なお、第1車載機200の位置が固定であるものとして閾値を設定する構成とすればよい。

- [0078] S 3 5 で特定した N M A 認証前の航法メッセージが前述のリピータやシミュレータによるものである場合には、正規の航法メッセージに対して、発信時刻と受信時刻との関係に齟齬が生じ、上述した発信時刻差と受信時刻差との差が閾値以上となる。よって、S 3 6 で整合性があると判定した航法メッセージは、N M A 認証を行っていないなくても、正規のものであると言える可能性が高い。
- [0079] なお、S 3 6 では、前述の発信時刻差と、前述の受信時刻差との差が前述した閾値と一致（言い換えると、誤差程度の範囲内で略一致）する場合に、整合性があると判定する構成としてもよい。
- [0080] そして、S 3 7 では、S 3 6 で整合性があると判定した場合（S 3 7 で Y E S）には、S 3 8 に移る。一方、S 3 6 で整合性がないと判定した場合（S 3 7 で N O）には、S 3 9 に移る。
- [0081] S 3 8 では、整合性があると判定した航法メッセージの発信元の G P S 衛星 2 を、測位用の G P S 衛星 2 として選択する。よって、S 3 8 が本開示の選択部に相当する。前述したように、S 3 6 で整合性があると判定した航法メッセージは、N M A 認証を行っていないなくても、正規のものであると言える可能性が高い。よって、S 3 6 で整合性があると判定した航法メッセージの発信元の G P S 衛星 2 について、航法メッセージの N M A 認証が成立したものと同様に信頼度のより高い測位が可能であるものとし、測位用の G P S 衛星 2 として選択する。以降では、S 3 8 で選択された G P S 衛星 2 については、みなし認証成立済みの G P S 衛星 2 と呼ぶ。
- [0082] S 3 9 では、みなし認証成立済みの G P S 衛星 2 の数が、測位に必要な数（以下、測位必要数）に達したか否かを判定する。測位必要数の一例としては、例えば 3 や 4 などとすればよい。そして、測位必要数に達したと判定した場合（S 3 9 で Y E S）には、S 4 2 に移る。一方、測位必要数に達していないと判定した場合（S 3 9 で N O）には、S 4 0 に移る。
- [0083] S 4 0 では、S 3 1 で抽出した N M A 認証済 G P S 衛星 2 の全てについて S 3 3 ～ S 3 8 の処理を完了した場合（S 4 0 で Y E S）には、S 4 1 に移

る。一方、S 3 1 で抽出した NMA 認証済 G P S 衛星 2 の一部でも S 3 3 ~ S 3 8 の処理が完了していない場合 (S 4 0 で N O) には、S 3 3 に戻って、S 3 3 ~ S 3 8 の処理が完了していない NMA 認証済 G P S 衛星 2 について、S 3 3 ~ S 3 8 の処理を行う。

[0084] S 4 1 では、NMA 認証済 G P S 衛星 2 以外の、捕捉している G P S 衛星 2 について、測位必要数に足りない分だけの数の NMA 認証成立済の G P S 衛星 2 が得られるまで、NMA 認証を行い、S 4 2 に移る。

[0085] S 4 2 では、再起動後の初期測位を行って、図 7 の処理を終了する。測位自体は、測位用に選択した測位必要数の G P S 衛星 2 から受信した航法メッセージを用いて周知の方法によって行う。S 4 2 が本開示の測位部に相当する。

[0086] みなし認証成立済みの G P S 衛星 2 のみで測位必要数をまかなえる場合には、再起動後の NMA 認証なしで初期測位を開始できる。よって、再起動後の NMA 認証を行わないで済む分だけ、初期測位の遅れを抑えることができる。また、みなし認証成立済みの G P S 衛星 2 で測位必要数の一部しかまかなえない場合でも、その一部について再起動後の NMA 認証を行わないで済む分だけ、初期測位の遅れを抑えることができる。

[0087] なお、再起動後の初期測位を行う場合、ホットスタート時には、エフェメリスデータの収集なしで測位を開始できるが、ウォームスタート時には、エフェメリスデータの収集を行ってから測位を開始する必要がある。よって、エフェメリスデータの収集を行ってから測位を開始する分、ウォームスタート時の方がホットスタート時よりも初期測位の開始時間が遅れる。

[0088] <認証情報保存処理>

また、第 1 車載機 2 0 0 の制御部 2 2 0 は、測位を行った場合に、その測位に用いた G P S 衛星 2 について、NMA 認証成立済みか否かを示す前述の NMA 認証情報と、みなし認証成立済みか否かを示す情報 (以下、みなし認証情報) を含む認証情報リストをメモリ 2 2 0 a に保存する認証情報保存処理を行う。

- [0089] ここで、図8を用いて、認証情報リストの一例について説明を行う。図8の例では、例えば第1車載機200が、GPS衛星2a~2dを測位用のGPS衛星2として用いて測位を行ったものとする。ここでは、GPS衛星2aのPRN IDは「1」、GPS衛星2bのPRN IDは「3」、GPS衛星2cのPRN IDは「5」、GPS衛星2dのPRN IDは「10」とする。
- [0090] 認証情報リストには、図8に示すように、航法メッセージの発信元のGPS衛星2ごとに、PRN IDと、そのPRN IDが示すGPS衛星2についてNMA認証が成立しているか否かを示すNMA認証情報と、みなし認証が成立しているか否かを示すみなし認証情報とが対応付けられている構成とすればよい。
- [0091] みなし認証情報は、例えば、図8に示すように、認証成立であるか（図中の「T」）、認証不成立若しくは未認証であるか（図中の「F」）の2つの状態を表す2値のフラグとすればよい。他にも、認証成立と認証不成立と未認証との3つの状態を表す情報としてもよい。例えば、初期測位において、みなし認証成立済みのGPS衛星2のみでは測位必要数をまかなえず、NMA認証成立済みのGPS衛星2も測位に用いた場合には、このGPS衛星2については、NMA認証情報は「T」、みなし認証情報は「F」となる。
- [0092] メモリ220aに保存する認証情報リストについては、NMA認証を行っていないが、みなし認証成立済みのGPS衛星2について、初期測位後にNMA認証を行って情報を更新してもよい。例えば、みなし認証成立済みのGPS衛星2について、NMA認証も成立した場合には、NMA認証情報もみなし認証情報も「T」となる。
- [0093] また、メモリ220aに保存する認証情報リストについては、初期測位を行った場合に保存するだけでなく、新たに測位を行うごとに逐次更新してゆく構成としてもよい。新たに測位する場合にも、みなし認証成立済みのGPS衛星2については、NMA認証を行わずに測位用のGPS衛星2として継続して用いる構成としてもよい。

[0094] <測位情報送信処理>

続いて、第1車載機200の制御部220での測位情報送信処理について、図9に示すフローチャートを用いて説明を行う。図9で示す測位情報送信処理は、例えば一定の周期で開始する構成とすればよい。

[0095] 図9のフローチャートで示す測位情報送信処理では、第1車載機200で測位した位置と、その測位に用いたGPS衛星2についての前述の認証情報リストの情報とを含む測位情報を送信する。

[0096] まず、S51では、第1車載機200での直近の測位で算出した位置を取得する。S52では、メモリ220aに保存されている認証情報リストの情報を取得する。S53では、S51で取得した位置と、認証情報リストに含まれる各GPS衛星2のPRN ID、NMA認証情報、みなし認証情報といった情報とを含む測位情報を、送信部212の狭域通信機能によって送信させ、処理を終了する。よって、S53が本開示の測位位置送信処理部に相当する。

[0097] 送信部212から送信された測位情報は、本実施形態では第2車載機300で受信されるものとして以降の説明を行う。

[0098] <第2車載機300の詳細構成>

続いて、図10を用いて、第1車載機200から送信された測位情報を受信する側の第2車載機300についての説明を行う。第2車載機300は、図10に示すように、通信部310、制御部320、衛星受信機330を備える。通信部310は、第1車載機200が備える通信部210と無線通信を行う。

[0099] 通信部310は、受信部311と送信部312とを備える。通信部310は、前述した通信部210と同様に、狭域通信機能及び広域通信機能を備えている。衛星受信機330は、衛星受信機230と同様に、GPS衛星2、QZS衛星3が発信する電波を一定周期で受信する。

[0100] 制御部320は、CPU、ROM、RAM等を備えたコンピュータであり、通信部310、衛星受信機330を制御する。メモリにはROMやRAM

等があり、メモリ 220a は、バックアップ RAM 等の不揮発性の一時保存メモリであるものとする。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、第 1 車載機 200 と同様に、前述の認証関連処理や一時保存処理や再起動方法選択処理や初期測位関連処理や認証情報保存処理や測位情報送信処理等の各種処理を実行する。

[0101] また、制御部 320 は、第 1 車載機 200 から受信部 311 で受信した測位情報を取得し、取得した測位情報に含まれる第 1 車載機 200 の位置（つまり、車両 A の位置）を利用した処理（以下、位置情報利用処理）を行う。位置情報利用処理の一例としては、第 1 車載機 200 を用いる車両 A との車間距離を適正な距離に保って追従走行する追従走行処理や第 2 車載機 300 を用いる車両 B の周辺にどの程度の車両が存在するかの混雑度を知らせる処理などがある。

[0102] また、制御部 320 は、測位情報に含まれていた認証情報をもとに、測位情報に含まれていた位置の信頼性の高さを判断し、判断した信頼性の高さに応じて、前述の位置情報利用処理の実行の有無を判断したりする構成とすればよい。

[0103] 例えば、高い信頼性が必要な追従走行処理では、位置の測位に用いた GPS 衛星 2 の全てが NMA 認証成立済みであった場合には実行すると判断するが、NMA 認証成立済みでないものがあつた場合には追従走行処理を実行しないと判断する構成とすればよい。一方、それほど高い信頼性が必要でない混雑度を知らせるような処理では、NMA 認証成立済みでないものがあつた場合でも、みなし認証成立済みであれば実行すると判断する構成などとすればよい。

[0104] <実施形態 1 のまとめ>

実施形態 1 によれば、ホットスタート時やウォームスタート時において、同一の GPS 衛星 2 についての、第 1 車載機 200 の電源オフ前に認証成立済みであつた航法メッセージと、再起動後に受信した航法メッセージとに、

経過時間に応じた整合性がある場合に、測位用のGPS衛星2として選択する。前述したように、経過時間に応じた整合性があると判定した航法メッセージは正規のものである可能性が高いので、その航法メッセージの発信元のGPS衛星2から再起動後に受信する航法メッセージを用いれば、信頼度のより高い測位を行うことが可能と言える。従って、実施形態1によれば、ホットスタート時やウォームスタート時において、信頼度のより高い初期測位を行うことが可能となる。

[0105] さらに、前述したように、実施形態1によれば、みなし認証成立済みのGPS衛星2を測位に用いることで、再起動後のNMA認証を行う時間を削減することができるので、ホットスタート時やウォームスタート時における測位開始時間の遅れを抑えることが可能になる。

[0106] また、実施形態1によれば、第1車載機200で測位した位置を第2車載機300に車車間通信によって送信する場合に、測位に用いたGPS衛星2についてのNMA認証情報及びみなし認証情報といった認証情報も付与して送信する。よって、第2車載機300では、この認証情報を用いて、第1車載機200での測位の信頼性がどの程度高いのかを判断することが可能になる。その結果、判断した信頼性の高さをもとに、位置情報利用処理の必要とする信頼性の高さに応じて、位置情報利用処理を実行するか否かを判断することが可能になる。

[0107] <変形例1>

第1車載機200での初期測位関連処理において、メモリ220aに保存しておいたNMA認証成立済みの航法メッセージの発信時刻と、NMA認証前の航法メッセージの発信時刻との発信時刻差と、両者の航法メッセージをそれぞれ受信した受信時刻差との差が閾値未満である場合に、整合性があると判定する構成について説明したが、必ずしもこれに限らない。例えば、NMA認証成立済みの航法メッセージと、NMA認証前の航法メッセージとの間で、航法メッセージの発信時刻と受信時刻とから定まる擬似距離が閾値未満である場合に整合性があると判定する構成（以下、変形例1）としてもよ

い。

[0108] ここで、変形例 1 における航法メッセージ認証システム 1 について、図面を用いて説明を行う。なお、説明の便宜上、前述の実施形態の説明に用いた図に示した部材と同一の機能を有する部材については、同一の符号を付し、その説明を省略する。

[0109] 変形例 1 における航法メッセージ認証システム 1 は、初期測位関連処理の一部が異なる点を除けば、実施形態 1 における航法メッセージ認証システム 1 と同様である。

[0110] <変形例 1 における初期測位関連処理>

ここで、変形例 1 における第 1 車載機 200 の制御部 220 での初期測位関連処理について、図 11 に示すフローチャートを用いて説明を行う。図 11 のフローチャートは、図 7 のフローチャートから S 36 の処理のみを入れ替えたものであって、S 36 の処理と入れ替えた S 36 a ~ S 36 c の処理の部分を抜き出して示している。

[0111] まず、S 35 に続く S 36 a では、S 33 で一時保存情報から取得した発信時刻と受信時刻（すなわち、メモリ 220 a に保存しておいた NMA 認証成立済みの航法メッセージの発信時刻とその航法メッセージを受信した受信時刻）とから、擬似距離を算出する。擬似距離とは、GPS 衛星 2 からの発信時刻と第 1 車載機 200 での受信時刻とから決まる伝搬時間に光速を積算して算出される、GPS 衛星 2 と第 1 車載機 200 との距離である。

[0112] S 36 b では、S 35 で特定した、NMA 認証前の航法メッセージの発信時刻とその航法メッセージを受信した受信時刻とから、擬似距離を算出する。

[0113] S 36 c では、S 31 で抽出した NMA 認証済みの GPS 衛星 2 について、S 36 a で算出した擬似距離と S 36 b で算出した擬似距離とから、NMA 認証が成立済みの航法メッセージと NMA 認証前の航法メッセージとに整合性があるか否かを判定し、S 37 に移る。よって、S 36 c が本開示の整合性判定部に相当する。

[0114] 具体例としては、S 3 6 a で算出した擬似距離と S 3 6 b で算出した擬似距離との差が閾値未満である場合に、整合性があると判定する。ここで言うところの閾値とは、S 3 1 で抽出した NMA 認証済 GPS 衛星 2 が、前述の発信時刻差にあたる時間に移動することにより生じる伝搬時間のずれに相当する擬似距離のずれとすればよい。なお、第 1 車載機 2 0 0 の位置が固定であるものとして閾値を設定する構成とすればよい。

[0115] ホットスタート時やウォームスタート時には、第 1 車載機 2 0 0 の電源オフ時から第 1 車載機 2 0 0 の位置は移動していない筈である。よって、S 3 5 で特定した NMA 認証前の航法メッセージが正規のものであれば、NMA 認証前の航法メッセージの発信時刻と受信時刻とから定まる擬似距離と、NMA 認証成立済みの航法メッセージの発信時刻と受信時刻とから定まる擬似距離とは閾値未満におさまる筈である。よって、S 3 6 c で整合性があると判定した航法メッセージは、NMA 認証を行っていなくても、正規のものであると言える可能性が高い。

[0116] なお、S 3 6 c では、S 3 6 a で算出した擬似距離と、S 3 6 b で算出した擬似距離との差が前述した閾値と一致（言い換えると、誤差程度の範囲内で略一致）する場合に、整合性があると判定する構成としてもよい。

[0117] <変形例 1 のまとめ>

前述したように、NMA 認証成立済みの航法メッセージと、NMA 認証前の航法メッセージとの間で、航法メッセージの発信時刻と受信時刻とから定まる擬似距離が一致する場合には、航法メッセージは正規のものである可能性が高い。変形例 1 では、このような条件を満たす場合に、NMA 認証前の航法メッセージを発信した GPS 衛星 2 を測位用の GPS 衛星 2 として選択する。よって、変形例 1 によっても、信頼度のより高い測位を実現しながらも、ホットスタート時やウォームスタート時における測位開始時間の遅れを抑えることが可能になる。

[0118] <変形例 2>

変形例 1 の構成は、第 2 車載機 3 0 0 での初期測位関連処理に適用する構

成としてもよい。

[0119] <変形例 3>

実施形態 1 では、第 1 車載機 200 から送信した測位情報を、第 2 車載機 300 が受信する場合について説明を行ったが、必ずしもこれに限らない。例えば、第 1 車載機 200 から狭域通信機能により送信した測位情報を、路側機が受信する構成（以下、変形例 3）としてもよい。

[0120] 変形例 3 の構成では、路側機は、第 1 車載機 200 から送信される位置を利用して所定のサービスを提供する処理を実行するシステムの端末であるものとする。例えば、上記サービスを提供する処理としては、第 1 車載機 200 を用いる車両 A が有料駐車区域に駐車したと判定した場合や、車両 A が有料道路を走行したと判定した場合に、その車両の使用者に自動的に課金を行う課金処理などがある。他にも、位置情報を利用するゲームなどがある。

[0121] 変形例 3 では、路側機が、測位情報に含まれていた認証情報をもとに、測位情報に含まれていた位置の信頼性の高さを判断し、判断した信頼性の高さに応じて、前述の所定のサービスを提供する処理の実行の有無を判断したりする構成とすればよい。

[0122] 例えば、高い信頼性が必要な課金処理では、位置の測位に用いた GPS 衛星 2 の全てが NMA 認証成立済みであった場合には実行すると判断するが、NMA 認証成立済みでないものがあつた場合には追従走行処理を実行しないと判断する構成とすればよい。一方、それほど高い信頼性が必要でないゲームなどでは、NMA 認証成立済みでないものがあつた場合でも、みなし認証成立済みであれば実行すると判断する構成などとすればよい。

[0123] <変形例 3 のまとめ>

変形例 3 によれば、第 1 車載機 200 で測位した位置を路側機に送信する場合に、測位に用いた GPS 衛星 2 についての NMA 認証情報及びみなし認証情報といった認証情報も付与して送信する。よって、路側機では、この認証情報を用いて、第 1 車載機 200 での測位の信頼性がどの程度高いのかを判断することが可能になる。その結果、判断した信頼性の高さをもとに、位

置情報利用処理の必要とする信頼性の高さに応じて、第1車載機200から送信される位置を利用して所定のサービスを提供する処理を実行するか否かを判断することが可能になる。

[0124] <変形例4>

また、第1車載機200でのNMA認証の結果を利用して、第2車載機300でみなし認証を行った結果が正しかったことを確認する構成（以下、変形例4）としてもよい。

[0125] ここで、変形例4における航法メッセージ認証システム1について、図面を用いて説明を行う。なお、説明の便宜上、前述の実施形態の説明に用いた図に示した部材と同一の機能を有する部材については、同一の符号を付し、その説明を省略する。

[0126] 変形例4における航法メッセージ認証システム1は、NMA認証情報とNMA認証を行ったことを証明するための認証済み証とを含む認証確認用情報を送信する認証確認用情報送信処理を行う点と、他機器から送信されたその認証確認用情報を用いて、みなし認証を行った結果を確認する確認処理を行う点を除けば、実施形態1における航法メッセージ認証システム1と同様である。

[0127] <認証確認用情報送信処理>

まず、第1車載機200の制御部220での認証確認用情報送信処理について、図12に示すフローチャートを用いて説明を行う。図12で示す認証確認用情報送信処理は、例えば一定の周期で開始する構成とすればよい。

[0128] まず、S61では、メモリ220aに保存されている認証情報リストの情報を取得する。S62では、S61で取得した認証情報リストに含まれるGPS衛星2のうちのNMA認証成立済みのものについて、NMA認証を行ったことを証明するための認証済み証を取得する。認証済み証としては、NMA認証において、認証センタ120から認証用情報として得られる情報、若しくはその情報から生成できる情報を用いる構成とすればよい。例えば、暗号キーとしてのHマトリクスを認証済み証としてもよいし、Hマトリクスと

パリティデータとを入力キーとしてハッシュ関数から作成されるハッシュ値を認証済み証としてもよい。本実施形態では、Hマトリクスを認証済み証として用いる場合を例に挙げて説明を行う。

[0129] 認証済み証として用いるHマトリクスは、NMA認証を行ったときに認証センタ120から取得し、認証情報リストのうちの該当するPRN IDに紐付けしてメモリ220aに保存しておく構成とすればよい。

[0130] S63では、S61で取得した認証情報リストに含まれる各GPS衛星2のPRN ID、NMA認証情報、みなし認証情報と、S62で取得した認証済み証とを含む認証確認用情報を、送信部212の狭域通信機能によって送信させ、処理を終了する。よって、PRN IDが本開示の識別情報に相当し、S63が本開示の認証情報送信処理部に相当する。

[0131] ここで、図13を用いて、認証確認用情報の一例について説明を行う。図13の例では、例えば認証情報リストに図8に示したのと同様の情報が含まれていた場合について説明を行う。ここでは、NMA認証成立済み（図中のNMA認証情報が「T」）であるのは、GPS衛星2a（図中のPRN ID「1」）、GPS衛星2d（図中のPRN ID「10」）であるので、GPS衛星2aとGPS衛星2dについて、認証済み証としてのHマトリクス（図中のKey 1、Key 4）を認証確認用情報に含ませて送信する。

[0132] 送信部212から送信された認証確認用情報は、本実施形態では第2車載機300で受信されるものとして以降の説明を行う。

[0133] <認証処理>

続いて、第2車載機300の制御部320での確認処理について、図14に示すフローチャートを用いて説明を行う。図14で示す確認処理は、例えば、第1車載機200から送信されてきた認証確認用情報を受信部311で受信したときに開始する構成とすればよい。

[0134] まず、S71では、第1車載機200から受信部311で受信した認証確認用情報を取得する。よって、このS71が本開示の認証情報受信処理部に相当する。S72では、メモリ320aに保存されている認証情報リストを

取得する。メモリ 320a は、本開示の保存部に相当する。

[0135] ここで、図 15 を用いて、メモリ 320a に保存されている認証情報リストの一例について説明を行う。図 15 の例では、例えば第 2 車載機 300 が、GPS 衛星 2a ~ 2c、2e を測位用の GPS 衛星 2 として用いて測位を行っていたものとする。ここでは、GPS 衛星 2a の PRN ID は「1」、GPS 衛星 2b の PRN ID は「3」、GPS 衛星 2c の PRN ID は「5」、GPS 衛星 2e の PRN ID は「13」とする。認証情報リストの項目は、図 8 に示したものと同様である。

[0136] 図 15 の例では、GPS 衛星 2a と GPS 衛星 2c については、NMA 認証は成立しておらず、みなし認証のみが成立している。GPS 衛星 2b については、NMA 認証は成立済みであって、みなし認証は行っていない。GPS 衛星 2e については、NMA 認証もみなし認証も成立済みである。

[0137] S73 では、S72 で取得した第 2 車載機 300 についての認証情報リストから、NMA 認証とみなし認証とのうちのみなし認証のみしか成立していない GPS 衛星 2 の情報を抽出する。図 15 の例では、GPS 衛星 2a と GPS 衛星 2c の情報が該当する。

[0138] S74 では、S73 で抽出できた場合（S74 で YES）には、S75 に移る。一方、S73 で抽出できなかった場合（S74 で NO）には、図 14 の処理を終了する。

[0139] S75 では、S71 で取得した認証確認用情報から、S73 で抽出した GPS 衛星 2 と PRN ID が同じであって、且つ、NMA 認証成立済みである GPS 衛星 2 の情報を抽出する。図 13 の例では、GPS 衛星 2a の情報が該当する。

[0140] S76 では、S75 で抽出できた場合（S76 で YES）には、S77 に移る。一方、S75 で抽出できなかった場合（S76 で NO）には、図 14 の処理を終了する。

[0141] S73 ~ S75 の処理では、第 2 車載機 300 でみなし認証が成立したのみである GPS 衛星 2 から、第 1 車載機 200 で NMA 認証が成立済みであ

るGPS衛星2を抽出している。

[0142] S77では、S75で抽出したGPS衛星2についてのHマトリクスを特定する。一例としては、認証センタ120から取得する構成としてもよいし、過去に取得しておいたものを用いる構成としてもよい。ここで言うところの過去とは、対象とするGPS衛星2についてみなし認証を行った以前に行っていたNMA認証の時点である。また、認証センタ120からHマトリクスを取得する場合には、対象とするGPS衛星2のPRN IDと、そのGPS衛星2について第2車載機300でみなし認証を行った場合に受信していた航法メッセージに含まれるTOWとを用いる構成とすればよい。

[0143] S78では、S75で抽出したGPS衛星2についての、認証確認用情報に含まれていたHマトリクスと、S77で特定したHマトリクスとが一致するか否かを判定する。そして、S79では、一致するものがあった場合（S79でYES）には、S80に移る。一方、一致するものがなかった場合（S79でNO）には、図14の処理を終了する。

[0144] S80では、S75で抽出したGPS衛星2のうち、認証確認用情報に含まれていたHマトリクスと、S77で特定したHマトリクスとが一致したものについては、第2車載機300でのみなし認証が適切であったと判断し、図14の処理を終了する。よって、S80が本開示の確認部に相当する。

[0145] 例えば、第2車載機300において、NMA認証とみなし認証とのうちのみなし認証のみしか成立していないGPS衛星2について、S80でみなし認証が適切であったと判断したもの以外は、第2車載機300でNMA認証を行う構成とすればよい。

[0146] 本実施形態において、第2車載機300が航法メッセージ認証型測位装置に相当し、第1車載機200は他の航法メッセージ認証型測位装置に相当する。

[0147] <変形例4のまとめ>

変形例4によれば、みなし認証が適切であったと判断されたものの以外のGPS衛星2については、NMA認証を行うことで信頼性を確認することがで

きるので、第2車載機300において信頼度のより高い測位を行うことが可能となる。また、みなし認証が適切であったと判断されたGPS衛星2については、確認処理によって信頼性が確認できているので、この点からも、第2車載機300において信頼度のより高い測位を行うことが可能となる。

[0148] <変形例5、6>

変形例4では、認証確認用情報にみなし認証情報や認証済み証を含む構成を示したが、必ずしもこれに限らない。例えば、認証確認用情報にみなし認証情報や認証済み証を含まない構成（以下、変形例5）としてもよい。認証確認用情報に認証済み証を含まない構成とした場合には、図14のフローチャートのS77～S79の処理を省略し、S76でYESの場合にS80に移る構成とすればよい。

[0149] また、変形例4では、測位情報送信処理で送信する測位情報とは別に、認証確認用情報送信処理で認証確認用情報を送信する構成を示したが、必ずしもこれに限らない。例えば、測位情報と認証確認用情報とを組み合わせた共通の情報を用いることで、測位情報送信処理と認証確認用情報送信処理とを共通化する構成（以下、変形例6）としてもよい。

[0150] <変形例7>

前述の実施形態では、第1車載機200は、車車間通信によって測位情報や認証確認用情報を第2車載機300に送信する構成を示したが、必ずしもこれに限らない。例えば、路側機を中継することで、路車間通信によって測位情報や認証確認用情報を第1車載機200から第2車載機300に送信する構成としてもよい。他にも、公衆通信回線網を利用して、測位情報や認証確認用情報を第1車載機200から第2車載機300に送信する構成としてもよい。

[0151] <変形例8>

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。

[0152] 変形例8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。

[0153] 第1車載機200や実施形態2以降の第2車載機300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。

[0154] <変形例9>

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としてもよい。

[0155] <変形例10>

前述の実施形態では、車両で用いられる第1車載機200及び第2車載機300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、第1車載機200や第2車載機300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。

[0156] 本開示の一例に係る航法メッセージ認証型測位装置は、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、認証センタから取得する認証用情報取得部と、認証用情報取得部で取得した認証用情報を用い

て、衛星受信機で受信した航法メッセージが正規であるとの認証を行う認証部と、衛星受信機で複数の人工衛星から受信した航法メッセージをもとに航法メッセージ認証型測位装置の位置を測位する測位部とを備える。航法メッセージ認証型測位装置は、記衛星受信機が受信した航法メッセージのうち、人工衛星の軌道情報を少なくとも含む衛星情報と、航法メッセージについての認証部での認証結果とを、航法メッセージ認証型測位装置の電源オフの間も保存する保存部と、航法メッセージ認証型測位装置の再起動時に、保存部に保存された軌道情報を利用して、人工衛星の捕捉を行う捕捉部と、保存部に保存された認証結果が認証成立であった航法メッセージが存在した場合、保存部に保存された航法メッセージの衛星情報に含まれる情報を用いて、航法メッセージと、航法メッセージの発信元の人工衛星から航法メッセージ認証型測位装置の再起動後に受信した航法メッセージとに、整合性があ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性があると判定した場合には、整合性があると判定した航法メッセージの発信元の人工衛星を、測位部での測位に用いる人工衛星として選択する選択部とを備える。測位部は、捕捉部で捕捉した人工衛星のうちの、選択部で選択した人工衛星から受信した航法メッセージを用いて航法メッセージ認証型測位装置の位置を測位する。

[0157] 本開示の一例に係るメッセージ認証型測位装置によれば、自装置の再起動時に、保存部に保存しておいた軌道情報を利用して、捕捉部で人工衛星の捕捉を行うので、ホットスタートやウォームスタートを行うことができる。また、同一の人工衛星についての、自装置の電源オフ前に認証部で認証成立していた航法メッセージと、自装置の再起動後に受信した航法メッセージとに整合性がある場合には、再起動後に受信した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、整合性判定部で整合性があると判定した航法メッセージは正規のものである可能性が高く、その航法メッセージの発信元の人工衛星から再起動後に受信する航法メッセージを用いれば、信頼度のより高い測位を行うことが可能と言える。従って、選択部で選択した人工衛星か

ら受信した航法メッセージを用いることで、信頼度のより高い測位を行うことが可能となる。

[0158] さらに、測位部は、捕捉部で捕捉した人工衛星のうちの、選択部で選択した人工衛星から受信した航法メッセージを用いて自装置の位置を測位するので、ホットスタート時やウォームスタート時に、信頼度のより高い測位を行うことが可能となる。また、本開示によれば、認証用情報取得部で取得した認証用情報を用いて認証部で認証を行わなくても、選択部で選択した人工衛星から受信した航法メッセージを用いることで、信頼度のより高い測位を行うことが可能となる。よって、選択部で選択した人工衛星については、認証用情報取得部で取得した認証用情報を用いて認証部で認証を行う時間を削減することができ、ホットスタート時やウォームスタート時における測位開始時間の遅れを抑えることが可能になる。

[0159] この出願に記載されるフローチャート、あるいは、フローチャートの処理は、複数のステップ（あるいはセクションと言及される）から構成され、各ステップは、たとえば、S 1 と表現される。さらに、各ステップは、複数のサブステップに分割されることができ、一方、複数のステップが合わさって一つのステップにすることも可能である。さらに、このように構成される各ステップは、デバイス、モジュール、ミーンズとして言及されることができ。

[0160] なお、本開示は、上述した各実施形態に限定されるものではなく、本開示に示した範囲で種々の変更が可能であり、異なる実施形態にそれぞれ開示された技術的手段を適宜組み合わせ得られる実施形態についても本開示の技術的範囲に含まれる。

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、３３０）と、

前記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、認証センタから取得する認証用情報取得部（Ｓ５）と、

前記認証用情報取得部（Ｓ５）で取得した前記認証用情報を用いて、前記衛星受信機（２３０、３３０）で受信した前記航法メッセージが正規であるとの認証を行う認証部（Ｓ９～Ｓ１１）と、

前記衛星受信機（２３０、３３０）で複数の前記人工衛星から受信した前記航法メッセージをもとに航法メッセージ認証型測位装置の位置を測位する測位部（Ｓ４２）とを備える航法メッセージ認証型測位装置（２００、３００）であって、

前記衛星受信機（２３０、３３０）が受信した前記航法メッセージのうち、前記人工衛星の軌道情報を少なくとも含む衛星情報と、前記航法メッセージについての前記認証部（Ｓ９～Ｓ１１）での認証結果とを、航法メッセージ認証型測位装置の電源オフの間も保存する保存部（２２０ａ、３３０ａ）と、

前記航法メッセージ認証型測位装置（２００、３００）の再起動時に、前記保存部（２２０ａ、３３０ａ）に保存された前記軌道情報を利用して、前記人工衛星の捕捉を行う捕捉部（Ｓ２４、Ｓ２７）と、

前記保存部（２２０ａ、３３０ａ）に保存された前記認証結果が認証成立であった前記航法メッセージが存在した場合、前記保存部（２２０ａ、３３０ａ）に保存された前記航法メッセージの前記衛星情報に含まれる情報を用いて、前記航法メッセージと、前記航法メッセージの発信元の前記人工衛星から前記航法メッセージ認証型測位装置（２００、３００）の再起動後に受信した航法メッセージとに整合性があるか否かを判定する整合性判定部（Ｓ３６、Ｓ３６ｃ）と、

前記整合性判定部（Ｓ３６、Ｓ３６ｃ）で整合性があると判定した

場合には、整合性があると判定した前記航法メッセージの発信元の前記人工衛星を、前記測位部（S 4 2）での測位に用いる人工衛星として選択する選択部（S 3 8）とを備え、

前記測位部（S 4 2）は、前記捕捉部（S 2 4、S 2 7）で捕捉した前記人工衛星のうちの、前記選択部（S 3 8）で選択した前記人工衛星から受信した前記航法メッセージを用いて航法メッセージ認証型測位装置の位置を測位する航法メッセージ認証型測位装置。

[請求項2]

請求項 1 において、

前記保存部（2 2 0 a、3 3 0 a）は、前記衛星情報として、前記衛星受信機（2 3 0、3 3 0）が受信した前記航法メッセージのうち、前記航法メッセージが前記人工衛星から発信された発信時刻も保存し、

前記整合性判定部（S 3 6）は、

前記保存部（2 2 0 a、3 3 0 a）に保存された前記航法メッセージの発信時刻と、前記航法メッセージの発信元の前記人工衛星から再起動後に受信した前記航法メッセージに含まれる発信時刻との時刻差と、前記保存部（2 2 0 a、3 3 0 a）に保存された前記航法メッセージの受信時刻と、前記航法メッセージの発信元の前記人工衛星から再起動後に受信した前記航法メッセージの受信時刻との時刻差との差が閾値未満である場合に、整合性があると判定する航法メッセージ認証型測位装置。

[請求項3]

請求項 1 において、

前記保存部（2 2 0 a、3 3 0 a）は、前記衛星情報として、前記衛星受信機（2 3 0、3 3 0）が受信した前記航法メッセージのうち、前記航法メッセージが前記人工衛星から発信された発信時刻も保存し、

前記整合性判定部（S 3 6 c）は、

前記保存部（2 2 0 a、3 3 0 a）に保存しておいた前記航法メッ

セージの発信時刻と前記航法メッセージを受信した時刻とから定まる擬似距離と、前記航法メッセージの発信元の前記人工衛星から再起動後に受信した前記航法メッセージに含まれる発信時刻と再起動後に前記航法メッセージを受信した時刻とから定まる擬似距離との差が閾値未満である場合に、整合性があると判定する航法メッセージ認証型測位装置。

[請求項4]

請求項1～3のいずれか1項において、

前記測位部（S42）は前記認証部（S9～S11）で認証が成立した前記航法メッセージの発信元の前記人工衛星から受信した前記航法メッセージも測位に用いることが可能であり、

前記測位部（S42）で測位した位置を、航法メッセージ認証型測位装置の外部に送信する測位位置送信処理部（S53）を備え、

前記測位位置送信処理部（S53）は、

前記測位部（S42）で測位した位置に、この位置の測位に用いた前記人工衛星についての、前記認証部（S9～S11）で認証が成立した前記航法メッセージの発信元の前記人工衛星か否か、及び前記測位部（S42）での測位に用いる人工衛星として前記選択部（S38）で選択された前記人工衛星か否かを示す情報を、付与して送信する航法メッセージ認証型測位装置。

[請求項5]

請求項1～4のいずれか1項において、

前記測位部（S42）は、前記認証部（S9～S11）で認証が成立した前記航法メッセージの発信元の前記人工衛星から受信した前記航法メッセージも測位に用いることが可能であり、

前記人工衛星についての、前記人工衛星を識別できる識別情報、及び前記認証部（S9～S11）で認証が成立した前記航法メッセージの発信元の前記人工衛星か否かを示す認証情報を、航法メッセージ認証型測位装置の外部に送信する認証情報送信処理部（S63）と

前記航法メッセージ認証型測位装置とは異なる、他の航法メッセー

ジ認証型測位装置の認証情報送信処理部（S 6 3）から送信されてくる、前記識別情報及び前記認証情報を受信する認証情報受信処理部（S 7 1）と、

前記認証情報受信処理部（S 7 1）で受信した前記識別情報及び前記認証情報をもとに、前記測位部（S 4 2）での測位に用いる人工衛星として航法メッセージ認証型測位装置の前記選択部（S 3 8）で選択された前記人工衛星が、前記他の航法メッセージ認証型測位装置の前記認証部（S 9 ～ S 1 1）で認証が成立した前記航法メッセージの発信元の前記人工衛星と同一の人工衛星であると特定できる場合に、航法メッセージ認証型測位装置の前記選択部（S 3 8）で選択された前記人工衛星が、前記測位に用いる人工衛星として適切であったと判断する確認部（S 8 0）とを備える航法メッセージ認証型測位装置。