

明 細 書

発明の名称：

航法メッセージ認証システム、受信端末、及び認証処理装置

関連出願の相互参照

[0001] 本出願は、2014年2月6日に出願された日本国特許出願2014-21631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、受信端末が受信した航法メッセージの認証を行うことができる航法メッセージ認証システム、その航法メッセージ認証システムが備える受信端末、及び認証処理装置に関する。

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が送信する航法メッセージを受信し、その航法メッセージに基づいて現在位置を算出する受信端末が広く知られている。

[0004] しかしながら、近年では、人工衛星が送信する信号と同様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、悪意のある者が当該シミュレータを使って、受信端末に誤った位置を算出させる虞がある。

[0005] これに対して、特許文献1には、受信端末が受信している航法メッセージが、衛星測位システムで用いられる人工衛星が送信した航法メッセージであるかの認証処理を行う航法メッセージ認証システムが提案されている。より具体的には、航法メッセージ認証システムは、準天頂衛星システムで用いられる準天頂衛星から、航法メッセージの認証に用いるデータを送信させる。

[0006] そして、受信端末は、準天頂衛星から取得したデータと、自端末が受信した航法メッセージとを用いた数値計算を実施することによって、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判定を行う。

[0007] 上述した認証処理において認証された航法メッセージに基づいて算出され

た位置情報は、シミュレータ等によって改竄されている可能性は相対に小さい。すなわち、この航法メッセージ認証システムを導入することによって、受信端末が算出する位置情報に対する信頼性を向上させることができる。

[0008] 受信端末が算出する位置情報に対する信頼性が向上することによって、受信端末の位置情報を利用した様々なサービスが提供できるようになると考えられる。位置情報を利用したサービスとは、例えば受信端末の位置に応じて有料道路の通行料を自動的に課金するサービスなどである。

[0009] しかしながら、本願発明者らの検討によれば、特許文献 1 の受信端末が実施する航法メッセージ認証処理には、数値計算が必要となるため、1 つの航法メッセージに対する認証処理を実施する際にも、CPU には相応の処理負荷がかかると想定される。また、受信端末は、自端末が受信している航法メッセージのいずれに対しても航法メッセージ認証処理を行う必要があり、それら全ての航法メッセージに対して、この認証処理を行うには、より多くの処理負荷がかかってしまう。したがって、各航法メッセージに対する認証が完了するまでに、サービス提供者又はサービスの提供を受ける者にとって許容できない待ち時間が生じてしまう恐れがある。

[0010] 受信端末に相対的に演算処理能力の高い CPU を搭載すれば、待ち時間を低減させることはできる。しかしながら、演算処理能力が高い CPU ほど高価であるため、受信端末のコストが増大してしまう。

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

発明の概要

[0012] 本開示は、この事情に基づいて成されたものであり、その目的とするところは、受信端末が受信した航法メッセージを認証するための受信端末のコスト増加を抑制可能な航法メッセージ認証システム、受信端末、及び認証処理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システムは、第 1 航法メッセージ

を送信する少なくとも1つの第1衛星と、第1航法メッセージの認証処理に用いられる検査用データを含む第2航法メッセージを送信する第2衛星と、第1航法メッセージ及び第2航法メッセージを受信する受信端末と、を備える。航法メッセージ認証システムは、第2航法メッセージに含まれる検査用データを用いて受信端末が受信した第1航法メッセージが、第1衛星が送信した第1航法メッセージであるかの認証処理を実施する。航法メッセージ認証システムは、さらに、受信端末の外部に設けられ、受信端末と通信する認証処理装置を備える。受信端末は、第1衛星が送信した第1航法メッセージ及び第2衛星が送信した第2航法メッセージを受信する端末側衛星受信機と、端末側衛星受信機が受信した第2航法メッセージから検査用データを抽出する検査用データ抽出部と、端末側衛星受信機が受信した第1航法メッセージから、当該第1航法メッセージの認証処理に必要な部分である認証関連データを抽出する認証関連データ抽出部と、検査用データ抽出部が抽出した検査用データと認証関連データ抽出部が抽出した認証関連データとを含み、衛星受信機が受信した第1航法メッセージに対する認証処理を実施するように要求する認証要求信号を生成する認証要求信号生成部と、認証要求信号生成部が生成した認証要求信号を送信する認証要求信号送信処理部と、を備える。認証処理装置は、認証要求信号送信処理部が送信した認証要求信号を受信する認証要求信号受信処理部と、認証要求信号に含まれる検査用データ及び認証関連データに基づいて、受信端末が受信した第1航法メッセージに対する認証処理を実施する認証演算部と、を備える。

[0014] 本開示の別の一例によれば、第1衛星が送信する第1航法メッセージ、及び、第2衛星が送信する、第1航法メッセージの認証処理に用いられる検査用データを含む第2航法メッセージを受信する端末側衛星受信機と、端末側衛星受信機が受信した第2航法メッセージから検査用データを抽出する検査用データ抽出部と、端末側衛星受信機が受信した第1航法メッセージから、当該第1航法メッセージの認証処理に必要な部分である認証関連データを抽出する認証関連データ抽出部と、検査用データ抽出部が抽出した検査用デー

タと認証関連データ抽出部が抽出した認証関連データとを含み、衛星受信機が受信した第1航法メッセージに対する認証処理を実施するように要求する認証要求信号を生成する認証要求信号生成部と、認証要求信号生成部が生成した認証要求信号を送信する認証要求信号送信処理部と、を備える受信端末が提供される。

[0015] さらに、本開示の別の一例によれば、第1衛星が送信する第1航法メッセージのうち、当該第1航法メッセージの認証処理に必要な部分である認証関連データと、第1航法メッセージの認証処理に用いられる検査用データと、を含む認証要求信号を受信する認証要求信号受信処理部と、認証要求信号に含まれる検査用データ及び認証関連データに基づいて、受信端末が受信した第1航法メッセージに対する認証処理を実施する認証演算部と、を備える認証処理装置が提供される

[0016] 本開示の航法メッセージ認証システム、受信端末、認証処理装置によれば、受信端末が認証処理を実施する必要は無く、認証処理装置が受信端末に代わって認証処理を実施する。すなわち、受信端末は、認証処理に伴う数値計算を高速に実施するための演算処理能力が高いCPUは必要としないため、受信端末のコスト増加を抑制することができる。

図面の簡単な説明

[0017] 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ブロック図であり、

[図2]コントロールセグメントの概略的な構成の一例を示すブロック図であり、

[図3]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]車載機の制御部が実施する認証要求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]NMA情報管理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6]NMA情報管理センタの制御部が実施する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7]NMA情報管理センタの制御部が実施する認証演算処理の流れの一例を示すフローチャートであり、

[図8]実施形態2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ブロック図であり、

[図9]実施形態2におけるサービス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10]サービスセンタの制御部が実施するSC側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11]変形例2におけるサービス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12]変形例3における車載機の制御部が備える機能を説明するための模式図である。

発明を実施するための形態

[0018] <実施形態1>

以下、本開示の実施形態1について図を用いて説明する。図1は、本実施形態における航法メッセージ認証システム1の概略的な構成の一例を示す図である。図1に示すように航法メッセージ認証システム1は、GPS衛星2、準天頂衛星（以下、QZS衛星）3、コントロールセグメント（CS）100、車載機200、及びNMA情報管理センタ300を備えている。コントロールセグメント100は、モニタステーション（MS）110、認証センタ（AC）120、マスタコントロールステーション（MCS）130を備えている。

[0019] GPS衛星2が本開示に記載の第1衛星、QZS衛星3が本開示に記載の第2衛星にそれぞれ相当する。また、NMA情報管理センタ300が本開示に記載の認証処理装置に、車載機200が本開示に記載の受信端末に、コントロールセグメント100が本開示に記載の認証センタ装置に、それぞれ相

当する。

[0020] <航法メッセージ認証システム1の概略構成>

ここでは、航法メッセージ認証システム1が備える各要素の概略について述べる。まず、モニタステーション110は、衛星測位システムの1つであるGPS (Global Positioning System) が備えるGPS衛星2が送信する電波（いわゆるGPS電波）を受信する。図1においてはGPS衛星2を1つしか図示していないが、もちろん、航法メッセージ認証システム1は、複数のGPS衛星2を備えている。

[0021] 周知のように、GPS衛星2が送信するGPS電波が搬送している信号は、C/Aコードを用いて位相変調が施されている。C/Aコードに用いられる擬似乱数雑音 (PRN: Pseudo Random Noise) の値は、GPS衛星2毎に異なる値となっており、これに伴ってC/Aコードもまた、GPS衛星2毎に異なっている。GPS電波の送信元となるGPS衛星2は、C/Aコードに用いられるPRNの値（すなわちPRN ID）によって特定することができる。以降では、GPS衛星2を識別する衛星番号として、このPRN IDを用いて説明する。

[0022] また、GPS電波には、航法メッセージMも含んでいる。各GPS衛星2が送信する航法メッセージMは、一週間内での経過時間を表すTOW (Time Of Week) や、衛星時計のクロック補正パラメータ、そのGPS衛星2の詳細軌道情報（すなわちエフェメリスデータ）、電離層補正パラメータ、全てのGPS衛星2の概略軌道情報（すなわちアルマナックデータ）などを含んでいる。このGPS衛星2が送信する航法メッセージMが本開示に記載の第1航法メッセージに相当する。

[0023] 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Mを抽出する。そして、モニタステーション110は、その抽出した航法メッセージMを認証センタ120へ逐次送る。このモニタステーション110が本開示に記載の第1航法メッセージ受信部に相当する。

[0024] 認証センタ120は、モニタステーション110から取得した航法メッセ

ージMに基づいて、レファランス認証ナビゲーションデータ（R A N D :
R e f e r e n c e A u t h e n t i c a t i o n N a v i g a t i o n
D a t a）メッセージを生成する。R A N Dメッセージについての詳細
は後述するが、R A N Dメッセージは、少なくともP R N I DとT O Wを含
んでおり、どのG P S衛星2がいつ送信した航法メッセージMに対応するも
のであるかを特定できるようになっている。認証センタ120は、作成した
R A N Dメッセージと暗号キーであるHマトリクスとから、当該航法メッ
セージM及びR A N Dメッセージに対応するパリティデータを作成する。この
パリティデータが、本開示に記載の検査用データに相当する。

[0025] 認証センタ120は、モニタステーション110や、マスタコントロール
ステーション130、車載機200などと相互通信可能な構成となっている
。例えば認証センタ120は、作成した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。

[0026] 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、Q Z S衛星3に送信する。Q Z S衛星3は、パリティ
データを含んだ航法メッセージNを地上に向けて放送する。パリティデー
タには、どのR A N Dメッセージに対応するデータであるのかを示すデー
タが付与されている。Q Z S衛星3が送信する航法メッセージNが本開示に記
載の第2航法メッセージに相当し、マスタコントロールステーション130
が本開示に記載の検査用データ送信部に相当する。

[0027] 車載機200は、G P S衛星2やQ Z S衛星3が送信する電波を受信する
とともに、NMA情報管理センタ300と通信可能な構成となっている。車
載機200は、G P S衛星2やQ Z S衛星3が送信する電波から、自端末の
位置を検出（すなわち、測位）する。

[0028] また、車載機200は、自端末が受信しているG P S電波から航法メッ
セージMを取得し、さらに航法メッセージMから航法メッセージ認証（NMA
: N a v i g a t i o n M e s s a g e A u t h e n t i c a t i o n
）処理に用いる情報（NMA用G P S側情報とする）を抽出する。ここでは

、NMA用GPS側情報として、RANDメッセージを生成する。なお、ここではNMA用GPS側情報としてRANDメッセージを用いるがこれに限らない。NMA用GPS側情報は、航法メッセージMであってもよい。NMA用GPS側情報は、航法メッセージMの送信元となるGPS衛星2、及び送信時刻を特定するための情報を備えていればよい。このNMA用GPS側情報が本開示に記載の認証関連データに相当する。

[0029] さらに、車載機200は、QZS衛星3が送信する航法メッセージNから、NMA処理に用いる情報としてパリティデータを取得する。

[0030] なお、車載機200は、QZS衛星3から、GPS衛星2の数に応じた複数種類のパリティデータを取得する。それら複数のパリティデータのうち、NMA用GPS側情報として作成したRANDメッセージに対応するパリティデータは、そのRANDメッセージのPRNIDとTOWから特定される。そして、車載機200は、自端末で作成したRANDメッセージと、QZS衛星3より受信したパリティデータとを含むNMA要求データRqを生成して、NMA情報管理センタ300に送信する。

[0031] NMA情報管理センタ300は、車載機200及び認証センタ120と、周知の通信ネットワークを介して通信可能な構成となっている。NMA情報管理センタ300は、車載機200からNMA要求データRqを取得すると、当該NMA要求データRqから、車載機200が生成したRANDメッセージと、それに対応するパリティデータを抽出する。

[0032] そして、NMA情報管理センタ300は、認証センタ120のデータ記憶部124にアクセスし、RANDメッセージに含まれているPRNID、TOWから、RANDメッセージに対応するHマトリクスを取得する。例えば、NMA情報管理センタ300は、RANDメッセージに含まれているPRNID、TOWを含み、これらのPRNID、TOWに対応するHマトリクスを送信するように要求するHマトリクス要求信号を認証センタ120に送信する。そして、認証センタ120から取得するHマトリクスを用いて後述する認証関連処理を実施する。この認証関連処理を実施することによって、

車載機２００が受信している航法メッセージＭが正規の航法メッセージであるかの認証処理、すなわちＮＭＡ処理を実施することができる。

[0033] ところで、車載機２００は、正規のＧＰＳ衛星２が送信する信号の他、ＧＰＳ衛星２が送信する信号を擬似的に生成するシミュレータが送信する電波を受信する可能性がある。そして、そのような非正規の信号によって車載機２００の位置情報が改竄されている場合には、例えばサービス事業者が位置情報を用いたサービスを提供する上で、適切な課金ができないなどの不具合が生じる。

[0034] これに対し、ＮＭＡ情報管理センタ３００が上述したＮＭＡ処理を実施することで、車載機２００が正規の送信元（すなわちＧＰＳ衛星２）が送信した信号を受信しているかをサービス事業者は識別することができるようになる。以降においては、車載機２００が受信している航法メッセージＭの送信元のうち、認証済みの航法メッセージＭを送信するＧＰＳ衛星２を、認証済みのＧＰＳ衛星２とも称する。

[0035] ＜認証センタ１２０の詳細構成＞

ここで、認証センタ１２０のより詳細な構成について説明する。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。

[0036] 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、種々の機能を実現する。より具体的に制御部１２２は、機能ブロックとして、ＲＡＮＤメッセージ生成部１２２１、ＳＥＥＤ値生成部１２２２、Ｈマトリクス生成部１２２３、パリティ生成部１２２４、信号加工部１２２５を備える。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。

[0037] 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Ｍから、ＲＡＮＤメッセージを作成する。このＲＡＮ

Dメッセージが本開示に記載の認証用データに相当し、R A N Dメッセージ生成部1 2 2 1が本開示に記載の認証用データ生成部に相当する。

[0038] R A N Dメッセージは、航法メッセージMのビット列の中から抽出した、一週間内での経過時間を表すT O W (T i m e O f W e e k)、クロック補正パラメータであるT O C、A F 0、A F 1を備えている。なお、T O Wは6秒ごとに更新され、一週間分の時間が経過するとリセットされる。このT O Wが本開示に記載の衛星時刻に相当し、T O C、A F 0、及びA F 1が、本開示に記載の衛星時刻補正用パラメータに相当する。クロック補正パラメータは、衛星時刻を特定するために用いられる情報であるとともに、衛星固有の情報でもある。すなわち、P R N I Dやクロック補正パラメータが本開示に記載の送信元固有の情報に相当し、T O Wが送信時刻情報に相当する。

[0039] さらに、R A N Dメッセージは、A F 1の後に、アンチスプーフフラグであるA S F l a g、P R N I Dが追加されている。T O W、P R N I D、T O C、A F 0、A F 1、A S F l a gなどは、適宜設計されるフォーマットに従って、R A N Dメッセージを構成するビット列中に配置される。

[0040] 上述したようにR A N DメッセージはP R N I DとT O Wを含んでいるため、どのG P S衛星2がいつ送信したかを示すデータであると言える。また、T O Wは6秒毎に更新されるため、R A N Dメッセージ生成部1 2 2 1は、モニタステーション1 1 0が航法メッセージMを受信する全てのG P S衛星2のそれぞれに対して、6秒毎にR A N Dメッセージを生成することになる。

[0041] S E E D値生成部1 2 2 2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。

[0042] Hマトリクス生成部1 2 2 3は、S E E D値生成部1 2 2 2が生成したS E E D値を使い、入力データから一意に定まるパリティビットを生成するためのHマトリクスを生成する。Hマトリクスは行列であってその行数及び列数は、入力データのビット数とパリティビットのビット数に応じた値となっ

ている。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。このHマトリクスが本開示に記載の暗号キーに相当し、Hマトリクス生成部1223が本開示に記載の暗号キー生成部に相当する。

[0043] パリティ生成部1224は、RANDメッセージ生成部1221が作成したRANDメッセージと、Hマトリクス生成部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。すなわち、このHマトリクスをRANDメッセージに乗じることで、パリティデータを算出する。このパリティ生成部1224が本開示に記載の検査用データ生成部に相当する。

[0044] 信号加工部1225は、パリティ生成部1224が生成したパリティデータ、及びその計算に使用したRANDメッセージを対応付けて、QZS衛星3から送信させる航法メッセージNに挿入する。そして、挿入済みの航法メッセージNをマスタコントロールステーション130に送る。

[0045] なお、本実施形態では一例として、QZS衛星3が送信する航法メッセージNは、モニタステーション110が捕捉している各GPS衛星2に対応するパリティデータ及びRANDメッセージを備える構成とする。すなわち、信号加工部1225は、複数のGPS衛星2に対応するパリティデータ及びRANDメッセージを対応付けて航法メッセージNに挿入する。

[0046] さらに、信号加工部1225は、信号の挿入に合わせて、パリティ生成部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。このデータ記憶部124が本開示に記載の記憶部に相当する。

[0047] 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毎に、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N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マトリクス生成部1

２２３、パリティ生成部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。

[0048] 通信部１２６は、ＮＭＡ情報管理センタ３００が送信するＨマトリクス要求信号を受信した場合に、データ記憶部１２４に記憶されているＨマトリクスから、受信したＨマトリクス要求信号に対応する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ＮＭＡ情報管理センタ３００へ返信する。

[0049] 認証センタ１２０とＮＭＡ情報管理センタ３００との間におけるＨマトリクスの送受信は、暗号化されたセキュアな通信で実施される。例えば、認証センタ１２０は、ＮＭＡ情報管理センタ３００が発行した公開鍵を用いて、Ｈマトリクスを暗号化してＮＭＡ情報管理センタ３００に送信すればよい。もちろん、共通鍵暗号方式などを用いることによって、通信の秘匿性を確保してもよい。

[0050] <車載機２００の詳細構成>

ここで、車載機２００の構成について図３を用いて説明する。図３に示すように、この車載機２００は、通信部２１０、制御部２２０、衛星受信機２３０を備える。

[0051] 通信部２１０は、受信信号の復調などを行う受信部２１１と、制御部２２０から入力されたデータを変調して送信する送信部２１２と、を備える。この送信部２１２が本開示に記載の端末側送信部に相当する。

[0052] また、通信部２１０は、狭域通信機能と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。広域通信機能は、例えば第３世代移動体通信システムで用いられる通信モジュールによって実現されるものとする。広域通信機能により、ＮＭＡ情報管理センタ３００と通信を行う。また、狭域通信機能は、例えば、通信距離が数百メートルである。車載機２００が図示しない路側機を介して認証センタ１２０やサービスセンタ４００と通信する構

成とする場合、車載機２００は、当該狭域通信機能を用いて路側機と通信する。

[0053] 衛星受信機２３０は、ＧＰＳ衛星２、ＱＺＳ衛星３が送信する電波を一定周期で受信する。受信した電波は復調して、制御部２２０に出力する。すなわち、衛星受信機２３０は、ＧＰＳ衛星２が送信した航法メッセージＭや、ＱＺＳ衛星３が送信した航法メッセージＮを逐次受信して制御部２２０に出力する。この衛星受信機２３０が本開示に記載の端末側衛星受信機に相当する。

[0054] 制御部２２０は、ＣＰＵ、ＲＯＭ、ＲＡＭ等を備えたコンピュータであり、通信部２１０、衛星受信機２３０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、後述する認証要求関連処理などを実行する。

[0055] メモリ２２１は、書き換え可能な記憶媒体であって、例えば制御部２２０が備えるＥＥＰＲＯＭやＲＡＭなどによって実現される。メモリ２２１は、衛星受信機２３０から逐次取得する航法メッセージＭや航法メッセージＮ、及び逐次算出する現在位置を記憶する。なお、記憶容量が一杯になった場合には、古いものから順次破棄していけばよい。また、現在位置は、例えば周知の測地座標系やＥＣＥＦ座標系などで表される。

[0056] 次に、図４に示すフローチャートを用いて、衛星受信機２３０で受信した航法メッセージＭの認証を実施するように、ＮＭＡ情報管理センタ３００に対して要求する一連の処理（認証要求関連処理とする）について説明する。衛星受信機２３０で受信した航法メッセージＭの認証とは、その受信した航法メッセージＭは、シミュレータで偽造された航法メッセージではなく、ＧＰＳ衛星２が送信した正規の航法メッセージＭであることを認証することを指す。

[0057] この認証要求関連処理は、前述の通り、車載機２００の制御部２２０が実施する。制御部２２０は、図４に示すフローチャートに示す認証要求関連処理を、例えば車載機２００に電力が供給されている場合に逐次（例えば１０

0ミリ秒毎に)実施する。その他、例えば衛星受信機230から航法メッセージMが入力された時に実行する構成としてもよい。

[0058] まずS1では、衛星受信機230がQZS衛星3から受信した航法メッセージNを取得する。S2では、S1で取得した航法メッセージNから、パリティデータと、そのパリティデータに対応するRANDメッセージを抽出する。そして、そのパリティデータが、どのRANDメッセージに対応するのかを特定するための情報として、RANDメッセージからPRNID及びTOWを抽出し、当該パリティデータと対応付けてメモリ221に保存しておく。このS2が本開示に記載の検査用データ抽出部に相当する。

[0059] なお、本実施形態における航法メッセージNは、GPS衛星2毎のRANDメッセージ及びそのRANDメッセージに対応するパリティデータを備えている。したがって、このS2によって、制御部220は、各GPS衛星2が送信する航法メッセージMに対応するパリティデータを取得し、メモリ221に保存することになる。これらの航法メッセージNから抽出したパリティデータを、後述の比較パリティデータと区別するため、受信パリティデータと称する。

[0060] S3では、衛星受信機230がGPS衛星2から受信した航法メッセージMを取得する。S4では、航法メッセージMの認証が必要か否かを判定する。受信した航法メッセージMの認証が必要か否かは、例えば車載機200の位置情報を利用するアプリケーションからの要求に応じて決定すればよい。

[0061] 例えば、位置情報を利用するアプリケーションとしては、車載機200を搭載した車両が有料駐車区域に駐車したと判定した場合にその車両の利用者に自動的に課金を行うアプリケーションや、位置情報を利用したゲーム、経路案内などのアプリケーションなどが想定される。そして、位置情報を用いて課金を実施するようなアプリケーションは、その位置情報が改竄されていないことを保証するために、航法メッセージMの認証が必要となり、一方、経路案内などのアプリケーションに位置情報を提供する場合には、航法メッセージMの認証は任意となると考えられる。

- [0062] すなわち、S 4 では、位置情報を提供するアプリケーションの種類や、アプリケーションからの要求に基づいて認証処理が必要か否かを決定する。航法メッセージMの認証が必要である場合には、S 4 がYESとなってS 5 に移る。一方、航法メッセージMの認証が不要である場合にはS 4 がNOとなって本フローを終了する。
- [0063] S 5 では、S 3 で受信した航法メッセージMから、認証センタ120のRANDメッセージ生成部1221と同様の方法によって、RANDメッセージを作成してS 6 に移る。このS 5 が本開示に記載の認証関連データ抽出部に相当する。
- [0064] なお、制御部220は、RANDメッセージ生成部1221と同様の方法によって航法メッセージMからRANDメッセージを生成する。このため、制御部220とRANDメッセージ生成部1221のそれぞれにおいて、RANDメッセージの生成に用いた航法メッセージMが同一のものであれば、それから生成されるRANDメッセージもまた同一の内容となる。
- [0065] すなわち、S 3 で衛星受信機230が受信した航法メッセージMが正規の航法メッセージMであれば、S 5 で生成されるRANDメッセージはRANDメッセージ生成部1221が生成したRANDメッセージと一致する。
- [0066] S 6 では、S 3 で取得した航法メッセージMから、PRNID及びTOWを抽出し、これらの組み合わせに対応する受信パリティデータをメモリ221から読み出してS 7 に移る。S 7 では、S 5 で生成したRANDメッセージとS 6 で読み出した受信パリティデータとを含むNMA要求データRqを生成して、S 8 に移る。このNMA要求データRqが本開示に記載の認証要求信号の一例に相当する。また、S 7 が本開示に記載の認証要求信号生成部に相当する。
- [0067] S 8 では、当該NMA要求データRqをNMA情報管理センタ300に送信する。このS 8 が本開示に記載の認証要求信号送信処理部に相当する。
- [0068] なお、車載機200とNMA情報管理センタ300との間における通信は、暗号化されたセキュアな通信で実施される。例えば、NMA情報管理セン

タ 3 0 0 が発行した公開鍵を用いて、NMA 要求データ R q を暗号化して NMA 情報管理センタ 3 0 0 に送信すればよい。もちろん、共通鍵暗号方式などを用いることによって、通信の秘匿性を確保してもよい。

[0069] <NMA 情報管理センタ 3 0 0 の詳細構成>

次に、NMA 情報管理センタ 3 0 0 の構成について図 5 を用いて説明する。図 5 に示すように、この NMA 情報管理センタ 3 0 0 は、通信部 3 1 0、制御部 3 2 0、NMA 情報データベース（以降、NMA 情報 DB）3 4 0 を備える。

[0070] 通信部 3 1 0 は、受信信号の復調などを行う受信部 3 1 1 と、制御部 3 2 0 から入力されたデータを変調して送信する送信部 3 1 2 と、を備える。NMA 情報管理センタ 3 0 0 は、この通信部 3 1 0 を介して車載機 2 0 0 や認証センタ 1 2 0 と通信を実施することができる。

[0071] 制御部 3 2 0 は、CPU、ROM、RAM 等を備えたコンピュータであり、通信部 3 1 0 の動作を制御したり、NMA 情報 DB 3 4 0 が格納しているデータの追加、削除、読み出しなどを実施したりする。また、制御部 3 2 0 の 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、後述する認証関連処理などを実行する。

[0072] NMA 情報 DB 3 4 0 は、書き換え可能な大容量記憶装置であって、例えば HDD などによって実現される。NMA 情報 DB 3 4 0 は、制御部 3 2 0 からの指示に基づいて、車載機 2 0 0 が受信した航法メッセージ M の認証に用いる情報（NMA 情報とする）を格納している。より具体的に、NMA 情報 DB 3 4 0 は NMA 情報として、後述する認証演算処理において認証成功と判定された RAND メッセージ及びパリティデータの組み合わせを記憶する。この NMA 情報が本開示に記載の認証済みデータに相当し、NMA 情報 DB 3 4 0 が本開示に記載の認証済みデータ記憶部に相当する。

[0073] NMA 情報 DB 3 4 0 は、各 RAND メッセージ及びパリティデータの組み合わせを、その RAND メッセージに含まれる PRN ID と TOW から特定できるように格納している。すなわち、制御部 3 2 0 は、PRN ID と T

OWを指定すれば、そのPRNID及びTOWの組み合わせに対応するパリティデータ、及びRANDメッセージにアクセスすることができる。以降では、NMA情報DB340が記憶しているRANDメッセージ、及び当該RANDメッセージに対応するパリティデータをそれぞれ、認証済みRANDメッセージ、認証済みパリティデータと称する。

[0074] 次に、図6に示すフローチャートを用いて、制御部320が実施する、衛星受信機230が受信した航法メッセージMの認証を実施する一連の処理（認証関連処理とする）について説明する。図6に示すフローチャートは、例えば車載機200からNMA要求データRqを受信したときに実行される。

[0075] まずS11では、通信部310から、車載機200が送信した、暗号化されているNMA要求データRqを取得する。そして、暗号化されているNMA要求データRqを、その暗号化に用いた公開鍵に対応する秘密鍵を用いて復号し、S12に移る。このS11が本開示に記載の認証要求信号受信処理部に相当する。

[0076] S12では、S11で復号したNMA要求データRqから、RANDメッセージとパリティデータとを抽出する。このパリティデータは、車載機200がQZS衛星3から受信したデータ、すなわち受信パリティデータである。NMA要求データRqから抽出したRANDメッセージから、さらに、PRNIDとTOWとを抽出する。

[0077] S13では、NMA情報DB340にアクセスし、S12で取得したPRNIDとTOWに対応する認証済みRANDメッセージ及び認証済みパリティデータを検索する。S12で取得したPRNIDとTOWに対応する認証済みRANDメッセージ及び認証済みパリティデータがNMA情報DB340内に存在する場合には、S13がYESとなってS14に移る。一方、S12で取得した及び認証済みパリティデータがNMA情報DB340内に存在しない場合には、S13がNOとなってS20に移る。このS13が本開示に記載の認証済み判定部に相当する。また、S12で取得したPRNIDとTOWに対応するNMA情報が、本開示に記載の、認証関連データに対応

する認証済みデータに相当する。

[0078] S 1 4 では、S 1 3 で発見した認証済み R A N D メッセージと、S 1 2 で N M A 要求データ R q から抽出した R A N D メッセージとが一致するかを判定する。それぞれの R A N D メッセージが一致する場合には、S 1 4 が Y E S となって S 1 5 に移る。S 1 5 では、認証成功と判定して本フローを終了する。認証成功ということは、車載機 2 0 0 が図 4 の S 3 で受信した航法メッセージ M が、シミュレータなどによって生成された信号ではなく、G P S 衛星 2 が送信した正規の航法メッセージ M であることを意味する。

[0079] なお、ここでは、認証済み R A N D メッセージと、S 1 2 で N M A 要求データ R q から抽出した R A N D メッセージとが一致すれば認証成功とする構成とするが、これに限らない。さらに、認証済みパリティデータと、受信パリティデータとが一致する場合に認証成功と判定する構成としてもよい。

[0080] 一方、S 1 3 で発見した認証済み R A N D メッセージと、S 1 2 で N M A 要求データ R q から抽出した R A N D メッセージとが一致しない場合には、S 1 4 が N O となって S 1 6 に移り、認証失敗と判定して本フローを終了する。これら S 1 4 ~ 1 6 が本開示に記載の認証済みデータ照合認証部に相当する。

[0081] S 2 0 では、N M A 要求データ R q から抽出した R A N D メッセージと受信パリティデータとを用いて、認証演算処理を実施する。この認証演算処理については、別途図 7 に示すフローチャートを用いて説明する。なお、この S 2 0 が本開示に記載の認証演算部に相当する。

[0082] 図 7 のフローチャートは、図 4 の S 2 0 に移った時に実行される。まず、S 2 1 では、N M A 要求データ R q から抽出した受信パリティデータを取得して S 2 2 に移る。S 2 2 では、N M A 要求データ R q から抽出した R A N D メッセージを取得して S 2 3 に移る。

[0083] S 2 3 では、R A N D メッセージに含まれる P R N I D 及び T O W を、秘匿通信に用いる公開鍵とともに、送信部 3 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、NMA情報管理センタ300から配布された公開鍵により暗号化してNMA情報管理センタ300へ送信する。

[0084] S24では、認証センタ120が送信した、暗号化されているHマトリクスを受信部311から取得する。S25では、S24で取得した暗号化されているHマトリクスを、秘密鍵で復号し、S26に移る。このS24～25が本開示に記載の暗号キー取得部に相当する。

[0085] S26では、S22で取得したRANDメッセージと、S25で復号したHマトリクスとから、パリティ生成部1224が実施する処理と同様の処理によって、パリティデータ（これを比較パリティデータと称する）を作成する。この比較パリティデータが本開示に記載の比較検査用データに相当し、S26が本開示に記載の比較検査用データ生成部に相当する。

[0086] S27では、S26で作成した比較パリティデータと、S21で取得した受信パリティデータとが一致するか否かを判断する。そして、両者が一致している場合には、次に述べる理由により、車載機200が受信している航法メッセージMが正規のものであると認証する（S28）。

[0087] すなわち、S25で復号したHマトリクスは、認証センタ120がRANDメッセージからパリティデータを作成する際に使用したHマトリクスと同じでHマトリクスである。この認証センタ120が生成したパリティデータは、QZS衛星3が送信するパリティデータ、すなわち、受信パリティデータそのものである。

[0088] よって、S26で作成した比較パリティデータが、S21で取得した受信パリティデータと一致する場合、S26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。

[0089] そして、各RANDメッセージが一致していることは、S22で取得したRANDメッセージの元となった航法メッセージM、すなわち、図4のS3で取得した航法メッセージが、認証センタ120がRANDメッセージを作成する時に用いた航法メッセージMと一致していることを意味する。

[0090] すなわち、S 2 6 で作成した比較パリティデータが、S 2 1 で取得した受信パリティデータと一致する場合、図 4 の S 3 で取得した航法メッセージ M は、認証センタ 1 2 0 も取得している正規の航法メッセージ M であることを意味する。

[0091] 以上で述べた理由より、S 2 6 で作成した比較パリティデータと、S 2 1 で取得した受信パリティデータとが一致する場合（S 2 7 で Y E S）には、S 2 8 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（S 2 7 で N O）には、S 2 9 に進み、認証不成立とする。S 2 8 又は S 2 9 を実施すると、その認証結果を保持して、当該認証演算処理の呼び出し元（図 6 S 2 0）に戻る。

[0092] 図 6 に戻り、認証関連処理の説明を続ける。以上の説明によって、S 2 0 までの処理を説明した。S 2 0 が完了すると、S 4 0 に移る。S 4 0 では、認証演算処理の結果、認証が成功したか否かを判定する。認証が成功している場合、S 4 0 が Y E S となって S 4 1 に移る。一方、認証が失敗している場合、S 4 0 が N O となって S 4 2 に移る。

[0093] S 4 1 では、NMA 要求データ R q から抽出した R A N D データ、及び受信パリティデータの組み合わせを、NMA 情報として新たに NMA 情報 D B 3 4 0 に追加保存する。これによって、他の車載機から同一の R A N D メッセージと受信パリティデータを含む NMA 要求データ R q が送信されてきた場合には、S 1 3、S 1 4 が Y E S となって、認証成功と判定することができる。すなわち、S 2 0 での認証演算処理を次回からは省略することができるようになる。S 4 1 での追加保存処理が完了すると本フローを終了する。

[0094] S 4 2 では、NMA 要求データ R q から抽出した R A N D データ、及び受信パリティデータは、破棄する。すなわち、認証に失敗した R A N D データ、及び受信パリティデータについては、NMA 情報 D B 3 4 0 に保存しない。S 4 2 での処理が完了すると本フローを終了する。

[0095] （実施形態 1 のまとめ）

以上の構成では、車載機 2 0 0 は、航法メッセージ M を受信すると、その

航法メッセージMがGPS衛星2が送信した航法メッセージMであるのかの認証を実施するように要求するNMA要求データRqを生成して、NMA情報管理センタ300に送信する。このNMA要求データには、RANDメッセージと、そのRANDメッセージに対応する受信パリティデータが含まれている。

[0096] つまり、本開示の一例に係る航法メッセージ認証システムにおける受信端末は、第1航法メッセージを受信すると、第1航法メッセージから、認証処理に必要な認証用データを抽出する。また、第2航法メッセージからは、その第1航法メッセージの認証で用いられる検査用データを抽出する。そして、当該認証用データと検査用データとを含む認証要求信号を認証処理装置に送信する。

[0097] NMA情報管理センタ300は、NMA要求データRqに含まれるRANDメッセージ及び受信パリティデータを用いて、車載機200が受信している航法メッセージMが正規の航法メッセージであるかの認証処理を実施する。

[0098] つまり、本開示の一例に係る航法メッセージ認証システムにおける認証処理装置は、認証要求信号を受信すると、その認証要求信号に含まれる認証用データと、検査用データに基づいて認証処理を実施する。

[0099] より具体的には、NMA情報DB340にアクセスし、NMA要求データRqに含まれるPRNIDとTOWに対応するNMA情報を検索する(S13)。NMA要求データRqに含まれるPRNIDとTOWに対応するNMA情報が存在する場合には、該当NMA情報と、NMA要求データRqに含まれるRANDメッセージを用いて認証処理を実施する(S14~16)。

[0100] また、NMA要求データRqに含まれるPRNIDとTOWに対応するNMA情報がNMA情報DB340に存在しない場合には、NMA要求データRqに含まれるRANDメッセージ及び受信パリティデータを用いた認証演算処理(S20)を実施する。

[0101] すなわち、本実施形態では、車載機200が受信している航法メッセージ

Mが正規の航法メッセージであるかを判定するための認証演算処理は、NMA情報管理センタ300が実施し、車載機200は、認証演算処理を実施する必要がない。

[0102] したがって、以上の構成によれば車載機200のコストアップを抑制しつつ、車載機200が受信している航法メッセージMを認証することができる。

[0103] つまり、受信端末が認証処理を実施する必要は無く、認証処理装置が受信端末に代わって認証処理を実施する。すなわち、受信端末は、認証処理に伴う数値計算を高速に実施するための演算処理能力が高いCPUは必要としないため、受信端末のコスト増加を抑制することができる。

[0104] また、NMA情報管理センタ300が、航法メッセージ認証システム1で用いられる複数の車載機200が受信する航法メッセージMの認証を集約して行う。そして、一度認証演算処理を実施したRANDメッセージとパリティデータの組み合わせについては、NMA情報DB340に格納する。これによって、既に認証成功となったNMA要求データRqと同一のPRNIDとTOWを含むNMA要求データRqに対しては、NMA情報DB340に格納しているNMA情報と比較することで認証することができ、認証演算処理を省略することができる。したがって、このようにNMA情報管理センタ300で集約して認証処理を実施することによって、車載機200が受信した航法メッセージMは、より短時間で認証されることとなる。

[0105] 以上、本開示の実施形態を説明したが、本開示は上述の実施形態に限定されるものではなく、以降で述べる態様も本開示の技術的範囲に含まれ、さらに、下記以外にも要旨を逸脱しない範囲内で種々変更して実施することができる。

[0106] <変形例1>

なお、以上で述べた実施形態1において、NMA情報管理センタ300は、S27において、車載機200が受信した航法メッセージから生成したパリティデータ（すなわち比較パリティデータ）の比較対象とするパリティデ

ータを、車載機 200 から取得する構成としたが、これに限らない。

[0107] NMA 情報管理センタ 300 は、比較パリティデータの比較対象とするパリティデータを、データ記憶部 124 から取得してもよい。すなわち、NMA 情報管理センタ 300 は、H マトリクスを取得した手順（図 7 S 23 ~ 25）と同様にして、NMA 要求データ R_qに含まれている R AND メッセージに対応するパリティデータを、認証センタ 120 から取得してもよい。車載機 200 が Q Z S 衛星 3 から受信する受信パリティデータは、データ記憶部 124 に記憶されているパリティデータと同じものである為、比較パリティデータの比較対象とするパリティデータとして、データ記憶部 124 から取得したデータを用いても、S 27 において同じ判定結果が得られる。

[0108] また、このような変形例とすれば、車載機 200 から NMA 情報管理センタ 300 に送信する NMA 要求データ R_qに受信パリティデータを含ませる必要は無く、車載機 200 から NMA 情報管理センタ 300 に送信するデータ量を削減することができる。

[0109] <実施形態 2>

次に、本開示の第 2 の実施形態（実施形態 2 とする）について、図を用いて説明する。なお、便宜上、前述の実施形態 1 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。また、構成の一部のみを説明している場合、構成の他の部分については先に説明した実施形態 1 を適用することができる。

[0110] 実施形態 2 における航法メッセージ認証システム 1 a は、実施形態 1 の航法メッセージ認証システム 1 の構成に加えて図 8 に示すように、車載機 200 及び NMA 情報管理センタ 300 のそれぞれと通信を実施するサービスセンタ 400 を備える。また、実施形態 2 における車載機 200 は、サービスセンタ 400 に NMA 要求データ R_qを送信するとともに、車載機 200 による測位結果（すなわち位置情報）をサービスセンタ 400 に送信する。

[0111] サービスセンタ 400 は、車両外部に備えられてあって、車載機 200 から送信される位置情報を利用したサービスを提供するサービス事業者が管理

するセンターである。位置情報を利用したサービスとしては、例えば、車載機 200 を搭載した車両が有料駐車区域に駐車したと判定した場合や、その車両が有料道路を走行したと判定した場合に、その車両の利用者に自動的に課金を行うサービスなどが想定される。

[0112] もちろん、その他、位置情報を利用したサービスとしては、経路案内や現在位置周辺の観光スポットを提案するサービス、さらには、位置情報を利用したゲームなどが考えられる。ここでは、一例として、駐車場管理会社が提供する、車載機 200 を搭載した車両が有料駐車区域に駐車したと判定した場合に課金を行うサービスを想定する。

[0113] 課金を伴う位置情報を利用したサービスにおいては、車載機 200 の位置情報が改竄されていないことが重要な前提条件となる。すなわち、車載機 200 から取得する位置情報が、認証済みの航法メッセージ M に基づいた位置情報であるか否かによって、サービス事業者は、車載機 200 を利用する顧客に対するサービス提供の是非を決定する。

[0114] ここで、図 9 を用いてサービスセンタ 400 の構成について説明する。サービスセンタ 400 は、通信部 410、制御部 420、NMA 情報 DB 440、及び顧客データベース（以下、顧客 DB）450 を備える。

[0115] 通信部 410 は、受信信号の復調などを行う受信部 411 と、制御部 420 から入力されたデータを変調して送信する送信部 412 と、を備える。サービスセンタ 400 は、この通信部 410 を介して車載機 200 や NMA 情報管理センタ 300 と通信を実施することができる。この受信部 411 が本開示に記載のサービスセンタ側受信部に相当する。なお、本開示において、サービスセンタは、簡略のため、SC と称することもある。

[0116] NMA 情報 DB 440 は、書き換え可能な大容量記憶装置であって、NMA 情報管理センタ 300 が備える NMA 情報 DB 340 と同様に、NMA 情報を格納している。より具体的に、NMA 情報 DB 340 は、NMA 情報として認証成功となる RAND メッセージ及びパリティデータを、その RAND メッセージに含まれる PRN ID と TOW から特定できるように対応付け

て記憶する。

[0117] NMA情報DB440に保存されているNMA情報は、後述するサービスセンタ側認証関連処理（以降、SC側認証関連処理）において随時追加される。このNMA情報DB440が本開示に記載のSC側認証済みデータ記憶部に相当する。

[0118] 顧客DB450は、書き換え可能な大容量記憶装置であって、当該サービスセンタ400が提供するサービスを利用する顧客についての情報（顧客情報とする）を記憶している。顧客情報は、顧客毎に区別して管理されており、その顧客が利用する車載機200の情報（登録車載機情報とする）、及びその車載機200から取得する位置情報を、それぞれ対応付けて記憶している。

[0119] 車載機情報は、当該車載機200を他の車載機と区別するための識別番号や、認証状態情報を含む。認証状態情報とは、例えば、当該車載機200が認証済みの航法メッセージを受信しているか否かや、車載機200が測位に用いたGPS衛星2の数のうちの、認証済みのGPS衛星2の数や割合などである。車載機の識別番号としては、例えば車載機200の製造番号やMACアドレスなどを用いればよい。

[0120] サービスセンタ400は、この車載機情報に基づいて、その車載機200を利用する顧客に対して、位置情報を利用したサービスを提供するか否かを判定する。例えば、認証済みのGPS衛星2が送信する信号を用いて測位している場合や、測位に用いているGPS衛星2の数のうち、認証済みのGPS衛星2の割合が一定の閾値（例えば75%）以上である場合に、サービスを提供すると判定する。

[0121] 制御部420は、CPU、ROM、RAM等を備えたコンピュータであり、通信部410の動作を制御したり、NMA情報DB440が格納しているデータの追加、削除、読み出しなどを実施したりする。また、制御部420の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後述するSC側認証関連処理などを実行する。

[0122] サービスセンタ４００とＮＭＡ情報管理センタ３００との主たる違いは、サービスセンタ４００は、サービス事業者が管理する設備であることに加えて、認証演算処理を実施する機能を備えていない点にある。すなわち、ＮＭＡ情報ＤＢ４４０に格納されているＮＭＡ情報を用いた認証は実施可能であるが、ＮＭＡ情報ＤＢ４４０に格納されていないＰＲＮＩＤ及びＴＯＷの組み合わせについては、自設備内では認証することができない。この場合の処理については、ＳＣ側認証関連処理の説明の中で言及する。

[0123] 次に、実施形態２において車載機２００が受信した航法メッセージＭを認証するための一連の処理について説明する。まず、車載機２００は、航法メッセージＭを受信すると、図４に示す認証要求関連処理を実施する。実施形態２においても、この認証要求関連処理の流れは実施形態１と同様であるが、Ｓ８におけるＮＭＡ要求データＲｑの送信先は、ＮＭＡ情報管理センタ３００ではなく、サービスセンタ４００である。

[0124] そして、車載機２００からＮＭＡ要求データＲｑを受信したサービスセンタ４００は、ＳＣ側認証関連処理を実施する。なお、車載機２００とサービスセンタ４００との間の通信は、暗号化されたセキュアな通信で実施される。

[0125] ここで、図１０に示すフローチャートを用いて、サービスセンタ４００の制御部４２０が実施する、ＳＣ側認証関連処理について説明する。図１０に示すフローチャートは、前述のとおり車載機２００からＮＭＡ要求データＲｑを受信したときに実行されればよい。

[0126] まずＳ５１では、車載機２００が送信した暗号化されているＮＭＡ要求データＲｑを通信部４１０から取得する。そして、暗号化されているＮＭＡ要求データＲｑを、その暗号化に用いた公開鍵に対応する秘密鍵を用いて復号し、Ｓ５２に移る。このＳ５１が本開示に記載のＳＣ側認証要求信号受信処理部に相当する。

[0127] Ｓ５２では、Ｓ５１で復号したＮＭＡ要求データＲｑから、ＲＡＮＤメッセージとパリティデータとを抽出する。このパリティデータは、車載機２０

OがQ Z S衛星3から受信したデータ、すなわち受信パリティデータである。NMA要求データR qから抽出したR A N Dメッセージから、さらに、P R N I DとT O Wとを抽出する。

[0128] S 5 3では、NMA情報DB 4 4 0にアクセスし、S 5 2で取得したP R N I DとT O Wに対応するNMA情報を検索する。S 5 2で取得したP R N I DとT O Wに対応するNMA情報がNMA情報DB 4 4 0内に存在する場合には、S 5 3がY E SとなってS 5 4に移る。一方、S 5 2で取得したP R N I DとT O Wに対応するNMA情報がNMA情報DB 4 4 0内に存在しない場合には、S 5 3がN OとなってS 5 7に移る。このS 5 3が、本開示に記載のS C側認証済み判定部に相当する。

[0129] S 5 4では、S 5 3で発見したNMA情報の認証済みR A N Dメッセージと、S 5 2でNMA要求データR qから抽出したR A N Dメッセージとが一致するかを判定する。それぞれのR A N Dメッセージが一致する場合には、S 5 4がY E SとなってS 5 5に移る。S 5 5では、認証成功と判定してS 6 2に移る。

[0130] なお、ここでは実施形態1と同様に、認証済みR A N Dメッセージと、S 5 2でNMA要求データR qから抽出したR A N Dメッセージとが一致すれば認証成功とする構成とするがこれに限らない。さらに、受信パリティデータと認証済みパリティデータとが一致する場合に認証成功と判定する構成としてもよい。

[0131] 一方、S 5 4において、S 5 3で発見した認証済みR A N Dメッセージと、NMA要求データR qから抽出したR A N Dメッセージとが一致しない場合には、S 5 4がN OとなってS 5 6に移って認証失敗と判定し、S 6 2に移る。これらS 5 4～5 6が、本開示に記載のS C側認証済みデータ照合認証部に相当する。

[0132] S 5 7では、S 5 1で取得して復号化したNMA要求データR qを、NMA情報管理センタ3 0 0が配布する公開鍵を用いて再び暗号化し、NMA情報管理センタ3 0 0に送信する。すなわち、車載機2 0 0から送信されてき

たNMA要求データR_qをNMA情報管理センタ300に転送する（これを二次NMA要求処理とする）。このS57が本開示に記載のSC側認証要求信号送信処理部に相当する。

[0133] NMA情報管理センタ300は、サービスセンタ400からNMA要求データR_qを受信すると、図6に示すNMA認証関連処理を実施する。このNMA認証関連処理は、実施形態1と同様である。ただし、S15、S16、S28、S29における認証結果は、サービスセンタ400に送信する。すなわち、NMA情報管理センタ300は、サービスセンタ400からのNMA要求データR_qに対する応答として、認証成功か認証失敗かを返送する。このNMA情報管理装置が送信する認証結果を示すデータが、本開示に記載の認証結果データに相当する。

[0134] 再び図10に戻り、サービスセンタ400の制御部420は、S58においてNMA情報管理センタ300から認証処理の結果を受信するとS59に移る。このS58が本開示に記載の認証結果取得部に相当する。

[0135] S59では、NMA情報管理センタ300から受信した認証結果が、認証成功であるか否かを判定する。認証結果が認証成功である場合にはS59がYESとなってS60に移る。一方、認証失敗である場合にはS59がNOとなってS61に移る。

[0136] S60では、S51で取得したNMA要求データR_qから抽出したRANDデータ、及び受信パリティデータの組み合わせを、NMA情報として新たにNMA情報DB440に追加保存する。これによって、他の車載機から同様のRANDメッセージと受信パリティデータを含むNMA要求データR_qが送信されてきた場合には、S53、S54がYESとなって、認証成功と判定することができる。すなわち、S57での二次NMA要求処理を次回からは省略することができるようになる。このS60が本開示に記載のSC側認証済みデータ追加処理部に相当する。S60での保存処理が完了するとS62に移る。

[0137] S61では、NMA要求データから抽出したRANDデータ、及び受信パ

リティデータは破棄する。すなわち、認証に失敗したR A N Dデータ、及び受信パリティデータについては、NMA情報D B 4 4 0に保存しない。S 6 1での処理が完了するとS 6 2に移る。

[0138] S 6 2では、NMA要求データR qに対する認証処理、すなわち車載機2 0 0が受信した航法メッセージMの認証が成功したか否かを、車載機2 0 0に送信してS 6 3に移る。このS 6 2が本開示に記載の認証結果送信処理部に相当する。

[0139] S 6 3では、車載機2 0 0の認証状態情報を更新して本フローを終了する。例えば、認証処理が成功であった場合には、車載機2 0 0は、そのNMA要求データR qが含むP R N I Dから特定されるG P S衛星2が送信する正規の航法メッセージMを受信していることを認証状態情報に保存する。

[0140] 車載機2 0 0の制御部2 2 0は、受信部2 1 1を介してNMA要求データR qに対する認証結果を取得すると、その認証結果をP R N I Dと対応付けてメモリ2 2 1に保存する。このような構成によれば、制御部2 2 0は、メモリ2 2 1のうちのP R N I D毎の認証結果を記憶している記憶領域を参照することによって、そのG P S衛星2の認証状態（すなわち認証済みか否か）を認識することができる。

[0141] なお、本実施形態において車載機2 0 0は、サービスセンタ4 0 0から認証結果を取得するが、もちろん、NMA情報管理センタ3 0 0から認証結果を取得してもよい。

[0142] （実施形態2のまとめ）

以上の構成では、車載機2 0 0は、G P S衛星2から航法メッセージMを受信すると、その航法メッセージMが、本当にG P S衛星2が送信した航法メッセージMであるのかを問い合わせるNMA要求データR qを生成して、サービスセンタ4 0 0に送信する。このNMA要求データR qには、R A N Dメッセージと、そのR A N Dメッセージに対応する受信パリティデータが含まれている。

[0143] サービスセンタ4 0 0は、当該NMA要求データR qに含まれるR A N D

メッセージ及び受信パリティデータと、NMA情報DB440に格納されているNMA情報を用いて、車載機200が受信した航法メッセージMが正規の航法メッセージであるかの認証を実施する。また、NMA要求データRqに含まれるRANDメッセージ及び受信パリティデータに対応するNMA情報が、NMA情報DB440に存在しない場合には、NMA情報管理センタ300にNMA要求データRqを送信することで、認証結果を取得する。

[0144] すなわち、以上の構成によれば、車載機200のコストアップを抑制しつつ、車載機200が受信している航法メッセージMを認証することができる。

[0145] また、サービス事業者は、顧客が利用する車載機200の認証状態を把握することができるので、その認証状態に基づいてサービス提供の是非を判断することができる。

[0146] さらに、サービスセンタ400は、NMA要求データRqに対する認証結果を、車載機200に返送する(図10 S63)。これによって、車載機200は、測位演算に用いた信号の送信元の確からしさ、すなわちGPS衛星2であるのか、シミュレータであるのかを確認できるようになる。例えば、認証失敗となった航法メッセージMの送信元はシミュレータと推定できる。そして、シミュレータからの信号を演算に用いている事が分かるため、次の測位演算には、認証失敗となった送信元からの信号を用いないように対処することができる。

[0147] <変形例2>

実施形態2では、車載機200から取得したNMA要求データRqに含まれるPRNIDとTOWに対応するNMA情報が、NMA情報DB440に存在しない場合に(S53 NO)、NMA要求データRqをNMA情報管理センタ300に送信する構成としたが、これに限らない。

[0148] 図11に示すように、サービスセンタ400に、衛星受信機230と同様の衛星受信機430を備えさせ、制御部420は、GPS衛星2が送信した航法メッセージMや、QZS衛星3が送信した航法メッセージNを逐次取得

してもよい（これを変形例２とする）。この衛星受信機４３０が本開示に記載のＳＣ側衛星受信機に相当する。

[0149] この変形例２における制御部４２０は、ＮＭＡ情報ＤＢ４４０に存在しないＰＲＮＩＤとＴＯＷの組み合わせとなる航法メッセージＭ及びパリティデータを受信した場合、その航法メッセージＭに対応するＮＭＡ要求データＲｑを生成し、ＮＭＡ情報管理センタ３００に送信する。

[0150] そして、そのＮＭＡ要求データＲｑに対する認証結果が認証成功であった場合には、当該ＰＲＮＩＤ及びＴＯＷの組み合わせに対応する認証済みＲＡＮＤメッセージ及び認証済みパリティデータをＮＭＡ情報ＤＢ４４０に追加保存しておく。

[0151] このような構成によれば、車載機２００からＮＭＡ要求データＲｑを受信しなくても、ＮＭＡ情報ＤＢ４４０が備えるデータは随時更新される。したがって、制御部４２０は、車載機２００からのＮＭＡ要求データＲｑに対して二次ＮＭＡ要求処理（Ｓ５７）を実施する可能性を低減でき、車載機２００からのＮＭＡ要求データＲｑに対してより速やかに認証結果を得ることができるようになる。

[0152] ＜変形例３＞

また、実施形態２において車載機２００の制御部２２０は、図１２に示すようにＮＭＡ要求データＲｑの送信先を、複数のサービスセンタ４００ａ、４００ｂから何れか少なくとも１つを選択する機能（送信先選択部）２２２を備えていても良い。

[0153] 送信先選択部２２２は、現在の位置情報及び起動しているアプリケーションなどから、ＮＭＡ要求データＲｑの送信先としてより好ましいサービスセンタ４００を選択する。例えば、現在の位置情報及び地図データから、現在、有料駐車場に存在すると判定した場合には、有料駐車場を管理するサービス事業者のサービスセンタ４００に、ＮＭＡ要求データＲｑを送信する。また、位置情報を利用したゲームのアプリケーションが起動中であれば、当該ゲームを提供するサービス事業者が管理するサービスセンタ４００にＮＭＡ

要求データ R_qを送信すればよい。

[0154] ユーザが、複数のサービス事業者が提供する位置情報を利用したサービスを利用可能な場合、そのユーザが利用する車載機 200 は、それぞれのサービス事業者が管理するサービスセンタ 400 において認証を受ける必要が生じうる。そのような場合であっても、この変形例 3 の構成によれば、ユーザの目的により適したサービスセンタ 400 で認証を受けることができるようになる。

[0155] <変形例 4>

以上では、車載機 200 は、広域通信機能を用いてサービスセンタ 400 や NMA 情報管理センタ 300 と通信する構成を示したが、もちろん路側機などを介して通信を実施してもよい。また、制御部 220 は、通信部 210 の狭域通信機能が形成する通信可能エリア内に路側機が存在しない場合には広域通信機能を利用するように、通信手段を適宜選択する機能を備えていてもよい。

[0156] 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、S1 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る、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。

[0157] 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]

第1航法メッセージを送信する少なくとも1つの第1衛星(2)と、前記第1航法メッセージの認証処理に用いられる検査用データを含む第2航法メッセージを送信する第2衛星(3)と、前記第1航法メッセージ及び前記第2航法メッセージを受信する受信端末(200)と、を備え、前記第2航法メッセージに含まれる前記検査用データを用いて前記受信端末(200)が受信した前記第1航法メッセージが、前記第1衛星(2)が送信した前記第1航法メッセージであるかの認証処理を実施する航法メッセージ認証システム(1)であって、

当該航法メッセージ認証システムは、さらに、前記受信端末(200)の外部に設けられ、前記受信端末(200)と通信する認証処理装置(300)を備え、

前記受信端末(200)は、

前記第1衛星(2)が送信した前記第1航法メッセージ及び前記第2衛星(3)が送信した前記第2航法メッセージを受信する端末側衛星受信機(230)と、

前記端末側衛星受信機(230)が受信した前記第2航法メッセージから前記検査用データを抽出する検査用データ抽出部(S2)と、

前記端末側衛星受信機(230)が受信した前記第1航法メッセージから、当該第1航法メッセージの前記認証処理に必要な認証関連データを抽出する認証関連データ抽出部(S5)と、

前記検査用データ抽出部(S2)が抽出した前記検査用データと前記認証関連データ抽出部(S5)が抽出した前記認証関連データとを含み、前記端末側衛星受信機(230)が受信した前記第1航法メッセージに対する前記認証処理を実施するように要求する認証要求信号を生成する認証要求信号生成部(S7)と、

前記認証要求信号生成部(S7)が生成した前記認証要求信号を送信する認証要求信号送信処理部(S8)と、を備え、

前記認証処理装置（３００）は、

前記認証要求信号送信処理部（Ｓ８）が送信した前記認証要求信号を受信する認証要求信号受信処理部（Ｓ１１）と、

前記認証要求信号に含まれる前記検査用データ及び前記認証関連データに基づいて、前記受信端末（２００）が受信した前記第１航法メッセージに対する認証処理を実施する認証演算部（Ｓ２０）と、を備える航法メッセージ認証システム。

[請求項２]

請求項１において、

前記第２航法メッセージに含まれる前記検査用データは、前記第１航法メッセージを取得する認証センタ装置（１００）で生成され、

前記認証センタ装置（１００）は、

前記第１航法メッセージを受信する第１航法メッセージ受信部（１１０）と、

前記第１航法メッセージ受信部（１１０）が受信した前記第１航法メッセージの前記認証関連データから認証用データを生成する認証用データ生成部（１２２１）と、

前記認証用データ生成部（１２２１）が生成した前記認証用データに対応する暗号キーを生成する暗号キー生成部（１２２３）と、

前記認証用データ生成部（１２２１）が生成した前記認証用データ、及び前記認証用データに対応する前記暗号キーを用いて前記検査用データを生成する検査用データ生成部（１２２４）と、

前記暗号キー生成部（１２２３）が生成した前記暗号キーを、当該暗号キーを用いた前記認証用データと対応付けて記憶する記憶部（１２４）と、

前記検査用データ生成部（１２２４）が生成した前記検査用データを前記第２衛星（３）に送信する検査用データ送信部（１３０）と、

前記認証処理装置（３００）と通信する通信部（１２６）と、を備え、

前記記憶部（１２４）は、前記暗号キーを、前記検査用データ及び前記第１航法メッセージと対応付けて記憶し、

前記認証処理装置（３００）は、

前記認証要求信号に含まれる前記認証関連データに対応する前記暗号キーを前記記憶部（１２４）から取得する暗号キー取得部（Ｓ２４～２５）と、

前記認証要求信号に含まれる前記認証関連データと前記暗号キー取得部（Ｓ２４～２５）が取得した前記暗号キーから比較検査用データを生成する比較検査用データ生成部（Ｓ２６）と、を備え、

前記認証演算部（Ｓ２０）は、前記比較検査用データ生成部（Ｓ２６）が生成した前記比較検査用データと、前記認証要求信号に含まれる前記検査用データとが一致する場合に、前記受信端末（２００）が受信した前記第１航法メッセージに対して認証成功と判定し、一方、前記比較検査用データ生成部（Ｓ２６）が生成した前記比較検査用データと、前記認証要求信号に含まれる前記検査用データとが一致しない場合には認証失敗と判定する航法メッセージ認証システム。

[請求項３]

請求項１または２において、

前記認証処理装置（３００）は、

前記認証演算部（Ｓ２０）が実施した前記認証処理の結果、認証成功となった前記認証関連データ及び前記検査用データの組み合わせを、認証済みデータとして記憶する認証済みデータ記憶部（３４０）と、

前記認証済みデータ記憶部（３４０）が記憶している前記認証済みデータの中に、前記認証要求信号に含まれている前記認証関連データに対応する前記認証済みデータが存在するか否かを判定する認証済み判定部（Ｓ１３）と、

前記認証済み判定部（Ｓ１３）が、前記認証済みデータ記憶部（３４０）が記憶している前記認証済みデータの中に、前記認証要求信号

に含まれている前記認証関連データに対応する前記認証済みデータが存在すると判定した場合に、当該認証関連データと、当該認証関連データに対応する前記認証済みデータとから、前記受信端末（200）が受信した前記第1航法メッセージの認証処理を実施する認証済みデータ照合認証部（S14～16）と、を備え、

前記認証演算部（S20）は、前記認証済み判定部（S13）が、前記認証済みデータ記憶部（340）が記憶している前記認証済みデータの中に、前記認証要求信号に含まれている前記認証関連データに対応する前記認証済みデータが存在しないと判定した場合に、前記認証処理を実施する航法メッセージ認証システム。

[請求項4]

請求項3において、

前記航法メッセージ認証システムは、更に、前記認証処理装置（300）及び前記受信端末（200）と通信を実施するサービスセンタ（400、400a、400b）を少なくとも1つ備え、

前記サービスセンタ（400、400a、400b）は、

前記認証要求信号送信処理部（S8）が送信する前記認証要求信号を受信するサービスセンタ側認証要求信号受信処理部（S51）と、

前記認証演算部（S20）が実施する前記認証処理において認証成功となる前記認証関連データ及び前記検査用データの組み合わせを、認証済みデータとして記憶するサービスセンタ側認証済みデータ記憶部（440）と、

前記認証要求信号に含まれている前記認証関連データと、当該認証関連データに対応する前記認証済みデータとから、前記受信端末（200）が受信した前記第1航法メッセージの認証処理を実施するサービスセンタ側認証済みデータ照合認証部（S54～56）と、を備える航法メッセージ認証システム。

[請求項5]

請求項4において、

前記サービスセンタ（400、400a、400b）は、

前記サービスセンタ側認証済みデータ記憶部（４４０）が記憶している前記認証済みデータの中に、前記認証要求信号に含まれている前記認証関連データに対応する前記認証済みデータが存在するか否かを判定するサービスセンタ側認証済み判定部（Ｓ５３）と、

前記サービスセンタ側認証済み判定部（Ｓ５３）が、前記サービスセンタ側認証済みデータ記憶部（４４０）が記憶している前記認証済みデータの中に、前記認証要求信号に含まれている前記認証関連データに対応する前記認証済みデータが存在しないと判定した場合に、前記認証要求信号を前記認証処理装置（３００）に送信するサービスセンタ側認証要求信号送信処理部（Ｓ５７）と、を備え、

前記認証処理装置（３００）において、

前記認証要求信号受信処理部（Ｓ１１）は、前記サービスセンタ側認証要求信号送信処理部（Ｓ５７）が送信した前記認証要求信号を受信し、

前記認証演算部（Ｓ２０）及び前記認証済みデータ照合認証部（Ｓ１４～１６）の何れか一方が、当該認証要求信号に含まれている前記認証関連データ及び前記検査用データに基づいて認証処理を実施し、

前記認証処理装置（３００）は、当該認証処理の結果を示す認証結果データを前記サービスセンタ（４００、４００ａ、４００ｂ）に送信し、

前記サービスセンタ（４００、４００ａ、４００ｂ）は、さらに、

前記認証処理装置（３００）が送信する前記認証結果データを取得する認証結果取得部（Ｓ５８）と、

前記認証結果取得部（Ｓ５８）が取得した前記認証結果データが示す結果が認証成功であった場合には、当該認証関連データ及び当該検査用データの組み合わせを、認証済みデータとして前記サービスセンタ側認証済みデータ記憶部（４４０）に追加するサービスセンタ側認証済みデータ追加処理部（Ｓ６０）と、を備える航法メッセージ認証

システム。

[請求項6]

請求項5において、

前記サービスセンタ（400、400a、400b）は、

前記認証要求信号に対する認証結果を前記受信端末（200）に送信する認証結果送信処理部（S62）を備える航法メッセージ認証システム。

[請求項7]

請求項1から6のいずれか1項において、

前記受信端末（200）は、

前記認証要求信号に対する前記認証処理の結果を受信する受信部（211）を備える航法メッセージ認証システム。

[請求項8]

請求項5から7のいずれか1項において、

前記サービスセンタ（400、400a、400b）は、

前記第1衛星（2）が送信した前記第1航法メッセージ及び前記第2航法メッセージを受信するサービスセンタ側衛星受信機（430）を備え、

前記サービスセンタ側認証要求信号送信処理部（S57）は、前記サービスセンタ側衛星受信機が受信した前記第2航法メッセージから前記検査用データを抽出するとともに、前記サービスセンタ側衛星受信機が受信した前記第1航法メッセージから前記認証関連データを抽出し、それらの検査用データ及び認証関連データを含む認証要求信号を生成し、当該認証要求信号を前記認証処理装置（300）に送信する航法メッセージ認証システム。

[請求項9]

請求項4から8のいずれか1項において、

前記航法メッセージ認証システムは、複数の前記サービスセンタ（400、400a、400b）を備え、

前記受信端末（200）は、複数の前記サービスセンタ（400、400a、400b）から前記認証要求信号の送信先を選択する送信先選択部（222）を備え、

前記認証要求信号送信処理部（Ｓ８）は、前記送信先選択部が選択した前記サービスセンタ（４００、４００ａ、４００ｂ）に前記認証要求信号を送信する航法メッセージ認証システム。

[請求項10]

請求項４から８のいずれか１項において、

前記受信端末（２００）は、

前記第１衛星（２）からの信号をもとに前記受信端末（２００）の位置を測位するとともに、測位結果である位置情報を前記サービスセンタ（４００、４００ａ、４００ｂ）に送信する端末側送信部（２１２）を備え、

前記サービスセンタ（４００、４００ａ、４００ｂ）は、前記受信端末（２００）が送信する前記位置情報を受信するサービスセンタ側受信部（４１１）を備え、前記サービスセンタ側受信部（４１１）が受信した前記位置情報を利用したサービスを実施する航法メッセージ認証システム。

[請求項11]

請求項１から１０のいずれか１項において、

前記認証関連データは、前記第１航法メッセージの送信元を特定するための送信元固有の情報、及び送信時刻を特定するための送信時刻情報を含む航法メッセージ認証システム。

[請求項12]

第１衛星（２）が送信する第１航法メッセージ、及び、第２衛星（３）が送信する、前記第１航法メッセージの認証処理に用いられる検査用データを含む第２航法メッセージを受信する端末側衛星受信機（２３０）と、

前記端末側衛星受信機（２３０）が受信した前記第２航法メッセージから前記検査用データを抽出する検査用データ抽出部（Ｓ２）と、

前記端末側衛星受信機（２３０）が受信した前記第１航法メッセージから、当該第１航法メッセージの前記認証処理に必要な部分である認証関連データを抽出する認証関連データ抽出部（Ｓ５）と、

前記検査用データ抽出部（Ｓ２）が抽出した前記検査用データと前

記認証関連データ抽出部（Ｓ５）が抽出した前記認証関連データとを含み、前記端末側衛星受信機（２３０）が受信した前記第１航法メッセージに対する前記認証処理を実施するように要求する認証要求信号を生成する認証要求信号生成部（Ｓ７）と、

前記認証要求信号生成部（Ｓ７）が生成した前記認証要求信号を送信する認証要求信号送信処理部（Ｓ８）と、を備える受信端末。

[請求項13]

第１衛星（２）が送信する第１航法メッセージのうち、当該第１航法メッセージの認証処理に必要な部分である認証関連データと、前記第１航法メッセージの認証処理に用いられる検査用データと、を含む認証要求信号を受信する認証要求信号受信処理部（Ｓ１１）と、

前記認証要求信号に含まれる前記検査用データ及び前記認証関連データに基づいて、受信端末（２００）が受信した前記第１航法メッセージに対する認証処理を実施する認証演算部（Ｓ２０）と、を備える認証処理装置。