(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6727131号
(P6727131)

(45)発行日　令和2年7月22日(2020.7.22)　(24)登録日　令和2年7月2日(2020.7.2)

(51)Int.Cl.		F I		
G01S 19/21	(2010.01)	G01S	19/21	
G01S 19/02	(2010.01)	G01S	19/02	
G01S 19/30	(2010.01)	G01S	19/30	
H04L 9/08	(2006.01)	H04L	9/00	601B
H04L 9/32	(2006.01)	H04L	9/00	601E

請求項の数 23　(全 20 頁)　最終頁に続く

(21)出願番号　特願2016-561353(P2016-561353)
(86)(22)出願日　平成27年3月23日(2015.3.23)
(65)公表番号　特表2017-517720(P2017-517720A)
(43)公表日　平成29年6月29日(2017.6.29)
(86)国際出願番号　PCT/EP2015/056120
(87)国際公開番号　WO2015/154981
(87)国際公開日　平成27年10月15日(2015.10.15)
審査請求日　平成30年2月2日(2018.2.2)
(31)優先権主張番号　14163902.1
(32)優先日　平成26年4月8日(2014.4.8)
(33)優先権主張国・地域又は機関
欧州特許庁(EP)

(73)特許権者　510304715
ザ　ヨーロピアン　ユニオン、リプレゼンテッド　バイ　ザ　ヨーロピアン　コミッション
The European Union, represented by the European Commission
ベルギー、１０４９　ブリュッセル、リュ　ド　ラロワ、２００
(74)代理人　100110319
弁理士　根本　恵司

最終頁に続く

(54)【発明の名称】無線航法信号の認証を最適化する方法及びシステム

(57)【特許請求の範囲】

【請求項１】

それぞれが別の衛星に搭載された複数の送信機(110,114,118,122)と、少なくとも１つの地上ベースの受信機(104)を含む無線航法システム(100;400)であって、

前記受信機(104)は、前記複数の送信機(110,114,118,122)のそれぞれからの無線航法信号(112,116,120,124;412,416,420,424)を受信するように適合されており、かつ前記送信機(110,114,118,122)のそれぞれ及び前記受信機(104)は、所定の第１のキーチェーンにアクセスするように適合されており、前記第１のキーチェーンは、第１の暗号化キー(K;K_j)と１つ以上のさらなる暗号化キー(K;$K_{j,1}$,$K_{j,2}$,$K_{j,3}$,$K_{j,4}$)を含み、

前記無線航法システムは：

前記複数の送信機(110,114,118,122)からの第１のグループの送信機であって、前記第１のグループの各送信機は、第１の無線航法信号(112,116,120,124;412,416,420,424)を送信するように動作可能であり、前記第１の無線航法信号は、ある与えられた時点又は与えられたサブフレーム(k,k+1)の間、無線航法データ、メッセージ認証符号（ＭＡＣ）（ＭＡＣ1,ＭＡＣ2,ＭＡＣ3,ＭＡＣ4）、及び前記１つ以上のさらなる暗号化キー(K;$K_{j,1}$,$K_{j,2}$,$K_{j,3}$,$K_{j,4}$)の１つを含む、前記第１のグループの送信機を含み；

前記ＭＡＣ（ＭＡＣ1,ＭＡＣ2,ＭＡＣ3,ＭＡＣ4）は、各送信機(110,114,118,122)に対してユニークであり、かつ前記第１の暗号化キー(K;K_j)を用いて生成され；

前記１つ以上のさらなる暗号化キー(K;$K_{j,1}$,$K_{j,2}$,$K_{j,3}$,$K_{j,4}$)の１つは、前記ＭＡＣの送信の所定時間後に送信され、そして

前記受信機(104)は、前記第１のグループの送信機(110,114,118,122)の１つ以上からの前記第１の無線航法信号(112,116,120,124;412,416,420,424)の全部又は一部を受信次第、その送信機又は他の任意の前記第１のグループの送信機から受信された前記１つ以上のさらなる暗号化キー(K;$K_{j,1}$,$K_{j,2}$,$K_{j,3}$,$K_{j,4}$)の１つに基づいて、前記第１のグループの送信機の１つから受信された第１の無線航法信号を認証するように、動作可能な無線航法システム。

【請求項２】

請求項１に記載された無線航法システムにおいて、

前記受信機(104)は、前記受信された１つ以上のさらなる暗号化キー(K;$K_{j,1}$,$K_{j,2}$,$K_{j,3}$,$K_{j,4}$)の１つを用いるか又は前記第１の無線航法信号から派生可能な他の１つ以上のさらなる暗号化キー(K;$K_{j,1}$,$K_{j,2}$,$K_{j,3}$,$K_{j,4}$)を用いて、前記第１の無線航法信号を認証するように動作可能な無線航法システム。

【請求項３】

請求項１又は２に記載された無線航法システムにおいて、

前記受信機(104)は、少なくとも前記無線航法データ及びその第１の無線航法信号のＭＡＣ（ＭＡＣ1,ＭＡＣ2,ＭＡＣ3,ＭＡＣ4）を受信次第、前記受信された１つ以上のさらなる暗号化キー(K;$K_{j,1}$,$K_{j,2}$,$K_{j,3}$,$K_{j,4}$)の１つに基づいて、受信された前記第１の無線航法信号(112,116,120,124;412,416,420,424)を認証するように動作可能な無線航法システム。

【請求項４】

請求項１，２又は３に記載された無線航法システムにおいて、

前記送信された暗号化キー(K)は、前記第１のグループ内で全ての送信機について同じである無線航法システム。

【請求項５】

請求項１，２又は３に記載された無線航法システムにおいて、

前記送信された暗号化キー($K_{j,1}$,$K_{j,2}$,$K_{j,3}$,$K_{j,4}$)は、前記第１のグループの各送信機について、前記第１のキーチェーンとは異なるものを含む無線航法システム。

【請求項６】

請求項５に記載された無線航法システムにおいて、

前記第１の無線航法信号(112,116,120,124;412,416,420,424)の各サブフレーム(k,k+1)について、前記第１のキーチェーンの各暗号化キーは、一方向関数から再帰的に派生されるｎ個の暗号化キー(K_m…K_{m+40})の１つを含む無線航法システム。

【請求項７】

請求項６に記載された無線航法システムにおいて、

ｎは前記無線航法システム(100;400)における送信機(110,114,118,122)の総数とほぼ等しく、かついずれにしても、それよりも大きい無線航法システム。

【請求項８】

請求項１乃至７のいずれかに記載された無線航法システムにおいて、

前記第１のグループの各送信機(110,114,118,122)について、前記１つ以上のさらなる暗号化キー(K;$K_{j,1}$,$K_{j,2}$,$K_{j,3}$,$K_{j,4}$)のそれぞれは、前記第１のキーチェーンのルートキー(K_0)から派生される無線航法システム。

【請求項９】

請求項１乃至８のいずれかに記載された無線航法システムにおいて、

前記受信機(104)は、前記受信された無線航法データ及び前記受信された１つ以上のさらなる暗号化キー(K;$K_{j,1}$,$K_{j,2}$,$K_{j,3}$,$K_{j,4}$)の１つに基づいて、派生ＭＡＣを生成し、そして前記派生ＭＡＣを前記受信されたＭＡＣ（ＭＡＣ1,ＭＡＣ2,ＭＡＣ3,ＭＡＣ4）と比較することにより、受信された前記第１の無線航法信号(112,116,120,124;412,416,420,424)を認証するように適合されている無線航法システム。

【請求項１０】

請求項１乃至９のいずれかに記載された無線航法システムにおいて、

第１のグループの送信機が、前記無線航法システム(100;400)における前記複数の送信機(110,114,118,122)の全てを含む無線航法システム。

【請求項１１】

請求項１乃至９のいずれかに記載された無線航法システムにおいて、

第１のグループの送信機は、前記無線航法システム(100;400)における前記複数の送信機(110,114,118,122)の厳密なサブセットを含む無線航法システム。

【請求項１２】

請求項１１に記載された無線航法システムにおいて、

残りの送信機(110,114,118,122)は、第２のグループの送信機を含み、所定の第２のキーチェーンは、前記第２のグループの送信機及び前記受信機によってアクセス可能であり、前記第２のキーチェーンは、第１の暗号化キー(K;K_j)及び１つ以上のさらなる暗号化キー(K;$K_{j,1}$,$K_{j,2}$,$K_{j,3}$,$K_{j,4}$)を含む無線航法システム。

【請求項１３】

請求項１２に記載された無線航法システムにおいて、

前記第２のグループの各送信機(110,114,118,122)は、第２の無線航法信号(112,116,120,124;412,416,420,424)を送信するように動作可能であり、前記第２の無線航法信号は、ある与えられた時点又は与えられたサブフレームの間、無線航法データ、ＭＡＣ（ＭＡＣ1,ＭＡＣ2,ＭＡＣ3,ＭＡＣ4）、及び前記１つ以上のさらなる暗号化キー(K;$K_{j,1}$,$K_{j,2}$,$K_{j,3}$,$K_{j,4}$)の１つを含み；

前記ＭＡＣ（ＭＡＣ1,ＭＡＣ2,ＭＡＣ3,ＭＡＣ4）は、各送信機(110,114,118,122)に対してユニークであり、かつ前記第１の暗号化キー(K;K_j)を用いて生成され；

前記１つ以上のさらなる暗号化キー(K;$K_{j,1}$,$K_{j,2}$,$K_{j,3}$,$K_{j,4}$)の１つは、前記ＭＡＣの送信の所定時間後に送信され、かつ

前記受信機(104)は、前記第２のグループの送信機の１つ以上から前記第２の無線航法信号(112,116,120,124;412,416,420,424)の全部又は一部を受信次第、その送信機又は他の任意の前記第２のグループの送信機から受信された前記１つ以上のさらなる暗号化キー(K;$K_{j,1}$,$K_{j,2}$,$K_{j,3}$,$K_{j,4}$)の１つに基づいて、前記第２のグループの送信機の１つから受信された第２の無線航法信号を認証するように、動作可能な無線航法システム。

【請求項１４】

請求項１３に記載された無線航法システムにおいて、

前記受信機(104)は、前記受信された１つ以上のさらなる暗号化キー(K;$K_{j,1}$,$K_{j,2}$,$K_{j,3}$,$K_{j,4}$)の１つを用いるか又は前記第１の無線航法信号から派生可能な他の１つ以上のさらなる暗号化キー(K;$K_{j,1}$,$K_{j,2}$,$K_{j,3}$,$K_{j,4}$)を用いて、前記第１の無線航法信号を認証するように動作可能な無線航法システム。

【請求項１５】

請求項１４に記載された無線航法システムにおいて、

前記受信機は、少なくとも前記無線航法データ及びその第２の無線航法信号のＭＡＣ（ＭＡＣ1,ＭＡＣ2,ＭＡＣ3,ＭＡＣ4）を受信次第、前記受信された暗号化キー(K;$K_{j,1}$,$K_{j,2}$,$K_{j,3}$,$K_{j,4}$)に基づいて、前記受信された第２の無線航法信号(112,116,120,124;412,416,420,424)を認証するように動作可能な無線航法システム。

【請求項１６】

請求項１３、１４又は１５に記載された無線航法システムにおいて、

前記送信された暗号化キー(K)は、前記第２のグループ内で全ての送信機について同じである無線航法システム。

【請求項１７】

請求項１３、１４又は１５に記載された無線航法システムにおいて、

前記送信された暗号化キー($K_{j,1}$,$K_{j,2}$,$K_{j,3}$,$K_{j,4}$)は、前記第２のグループの各送信機について、前記第２のキーチェーンとは異なるものを含む無線航法システム。

【請求項１８】

請求項１乃至１７のいずれかに記載された前記第１の無線航法信号(112,116,120,124;4

12,416,420,424)及び/又は請求項１３乃至１７のいずれかに記載された前記第２の無線航法信号は、予想不能なビットを含む信号の部分(68)が予測可能なビットを含む部分とインターリーブされるように送信される無線航法システム。

【請求項１９】

無線航法システム(100;400)のための送信機であって、

前記無線航法システム(100;400)は、それぞれが別の衛星に搭載された複数の送信機(110,114,118,122)、及び少なくとも１つの地上ベースの受信機(104)を含み、

前記受信機(104)は、前記複数の送信機(110,114,118,122)のそれぞれからの無線航法信号(112,116,120,124;412,416,420,424)を受信するように適合されており、前記送信機(110,114,118,122)のそれぞれ及び前記受信機(104)は、所定の第１のキーチェーンにアクセスするように適合されており、前記第１のキーチェーンは、第１の暗号化キー(K;K_j)及び１つ以上のさらなる暗号化キー(K;$K_{j,1}$,$K_{j,2}$,$K_{j,3}$,$K_{j,4}$)を含み、前記受信機(104)は、第１のグループの送信機(110,114,118,122)の１つ以上から第１の無線航法信号(112,116,120,124;412,416,420,424)の全て又は一部を受信次第、その送信機又は他の任意の前記複数の送信機から受信された前記１つ以上のさらなる暗号化キー(K;$K_{j,1}$,$K_{j,2}$,$K_{j,3}$,$K_{j,4}$)の１つに基づいて、前記送信機の１つから受信された前記第１の無線航法信号を認証するように動作可能である、前記送信機(110,114,118,122)及び地上ベースの受信機(104)を含み：

前記送信機は、前記第１の無線航法信号(112,116,120,124;412,416,420,424)を送信するように動作可能であり、前記第１の無線航法信号は、ある与えられた時点又は与えられたサブフレーム(k,k+1)の間、無線航法データ、ＭＡＣ（ＭＡＣ1,ＭＡＣ2,ＭＡＣ3,ＭＡＣ4）、及び前記１つ以上のさらなる暗号化キー(K;$K_{j,1}$,$K_{j,2}$,$K_{j,3}$,$K_{j,4}$)の１つを含み；

前記ＭＡＣ（ＭＡＣ1,ＭＡＣ2,ＭＡＣ3,ＭＡＣ4）は、各送信機(110,114,118,122)に対してユニークであり、かつ前記第１の暗号化キー(K;K_j)を用いて生成されており；かつ

前記１つ以上のさらなる暗号化キー(K;$K_{j,1}$,$K_{j,2}$,$K_{j,3}$,$K_{j,4}$)の１つは、前記ＭＡＣの送信の所定時間後に送信される送信機。

【請求項２０】

無線航法システム(100;400)のための受信機(104)であって、

前記無線航法システム(100;400)は、それぞれが別の衛星に搭載された複数の送信機(110,114,118,122)、及び少なくとも１つの前記受信機(104)であって、

前記送信機(110,114,118,122)のそれぞれ及び前記受信機(104)は、所定の第１のキーチェーンにアクセスするように適合されており、前記第１のキーチェーンは、第１の暗号化キー(K;K_j)及び１つ以上のさらなる暗号化キー(K;$K_{j,1}$,$K_{j,2}$,$K_{j,3}$,$K_{j,4}$)を含み、各送信機(110,114,118,122)は、第１の無線航法信号(112,116,120,124;412,416,420,424)を送信するように動作可能であり、前記第１の無線航法信号は、ある与えられた時点又は与えられたサブフレーム(k,k+1)の間、無線航法データ、ＭＡＣ（ＭＡＣ1,ＭＡＣ2,ＭＡＣ3,ＭＡＣ4）、及び前記１つ以上のさらなる暗号化キー(K;$K_{j,1}$,$K_{j,2}$,$K_{j,3}$,$K_{j,4}$)の１つを含む、前記送信機及び前記受信機を含み；

ＭＡＣ（ＭＡＣ1,ＭＡＣ2,ＭＡＣ3,ＭＡＣ4）は、各送信機(110,114,118,122)に対してユニークであり、かつ前記第１の暗号化キー(K;K_j)を用いて生成されており；

前記１つ以上のさらなる暗号化キー(K;$K_{j,1}$,$K_{j,2}$,$K_{j,3}$,$K_{j,4}$)の１つは、前記ＭＡＣの送信の所定時間後に送信され、

前記受信機(104)は、前記複数の送信機(110,114,118,122)のそれぞれからの無線航法信号(112,116,120,124;412,416,420,424)を受信するように適合されており；かつ

前記受信機(104)は、前記送信機(110,114,118,122)の１つ以上から前記第１の無線航法信号(112,116,120,124;412,416,420,424)の全て又は一部を受信次第、その送信機又は他の任意の前記複数の送信機(110,114,118,122)から受信された前記１つ以上のさらなる暗号化キー(K;$K_{j,1}$,$K_{j,2}$,$K_{j,3}$,$K_{j,4}$)の１つに基づいて、前記送信機の１つから受信された前記第１の無線航法信号を認証するように動作可能な受信機。

【請求項２１】
無線航法システム(100;400)のための無線航法の方法であって、
前記無線航法システム(100;400)は、それぞれが別の衛星に搭載された複数の送信機(110,114,118,122)、及び少なくとも１つの地上ベースの受信機(104)を含み、前記受信機(104)は、前記複数の送信機(110,114,118,122)のそれぞれからの無線航法信号(112,116,120,124;412,416,420,424)を受信するように適合されており、
前記方法は：
前記送信機(110,114,118,122)のそれぞれ及び前記受信機(104)に対して、第１の暗号化キー($K;K_j$)及び１つ以上のさらなる暗号化キー($K;K_{j,1},K_{j,2},K_{j,3},K_{j,4}$)を含む所定の第１のキーチェーンへのアクセスであって、
前記複数の送信機(110,114,118,122)のそれぞれから、第１の無線航法信号(112,116,120,124;412,416,420,424)を送信し、前記第１の無線航法信号は、ある与えられた時点又は与えられたサブフレーム(k,k+1)の間、無線航法データ、ＭＡＣ（ＭＡＣ1,ＭＡＣ2,ＭＡＣ3,ＭＡＣ4）、及び前記１つ以上のさらなる暗号化キー($K;K_{j,1},K_{j,2},K_{j,3},K_{j,4}$)の１つを含み、前記ＭＡＣ（ＭＡＣ1,ＭＡＣ2,ＭＡＣ3,ＭＡＣ4）は、各送信機(110,114,118,122)に対してユニークであり、かつ前記第１の暗号化キー($K;K_j$)を用いて生成されており、前記１つ以上のさらなる暗号化キー($K;K_{j,1},K_{j,2},K_{j,3},K_{j,4}$)の１つは、前記ＭＡＣの送信の所定時間後に送信される、前記所定の第１のキーチェーンへのアクセスを提供し；
前記受信機(104)で、前記複数の送信機(110,114,118,122)の１つ以上から前記第１の無線航法信号の全て又は一部を受信し、かつ前記受信機(104)で、前記複数の送信機におけるその送信機又は他の任意の送信機から受信された前記１つ以上のさらなる暗号化キー($K;K_{j,1},K_{j,2},K_{j,3},K_{j,4}$)の１つに基づいて、前記複数の送信機の１つから受信された第１の無線航法信号を認証する、
ことを含む無線航法システムのための無線航法の方法。
【請求項２２】
処理回路による実行のため、および少なくとも請求項２１におけるステップに対応する命令を定義するかまたは変換可能なデータが記録または蓄積された、記録可能、書き換え可能または蓄積可能な媒体。
【請求項２３】
通信装置と記憶装置を含み、オンデマンドまたは他の方法で、処理回路による実行のため、および少なくとも請求項２１におけるステップに対応する命令を定義するかまたは変換可能なデータを送信するように構成されたコンピューターサーバー。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は衛星無線航法信号の認証に関し、特に、困難な受信条件を伴う環境で衛星航法信号の認証を最適化するための方法及びシステムに関する。
【背景技術】
【０００２】
ＧＰＳのようなシステムの使用によって、衛星航法が社会と経済の重要な要素になっている。
しかしながら、それらの高い重要性にもかかわらず、全地球航法衛星システムズ（ＧＮＳＳ）の民生用信号は偽造することが非常に容易である。
それらは、低電力で偽の信号を送信する機器がＧＮＳＳ受信機を支配することが可能であることを意味する、極めて低い電力（ほぼ－１６０ｄＢＷ、又は10^{-16}ワット）で送信及び受信される。
将来、このような攻撃を防ぐための機能がいくつかのＧＮＳＳに実装されるかもしれないと信じられているものの、現在、民生用のＧＮＳＳ信号は、このような攻撃を防ぐために、これらの信号の真正性（authenticity）を決定するためのいかなる手段も提供してい

ない。
しかしながら、以下に論じられるように、いくつかのＧＮＳＳ信号とデータ認証基準(authentication measures)が提案された。
【０００３】
衛星航法分野における用語「認証」は、一般に航法衛星信号から計算された位置の真正性を表す。
位置を認証するため、位置計算に用いられる信号が真正であることが保証されることが必要であり、それに加えて、受信機は、その位置を計算する内部処理が偽造されなかったことを保証しなければならない。
ここに使われている「認証」は、主として信号認証を意味する。
受信機がＧＮＳＳ信号から抽出する２つの主な情報は、衛星位置と時刻情報（航法メッセージに含まれている）、及び到着時刻信号（符号位相測定によって、殆どの受信機で取得される）である。
そのため、無線航法信号の認証とは、衛星から送信されたデータの真正性及び保全性の確認、並びに受信機で測定された信号の到着時刻（ＴＯＡ）の認証を表す。
【０００４】
直接連続拡散スペクトラム（ＤＳＳＳ）符号分割多元接続（ＣＤＭＡ）信号として、ＧＮＳＳ信号は、信号電力がある帯域幅にわたって拡散する拡散符号上で変調されたデータのビットストリームを含み、かつ到着時刻の計算にも用いられる。
認証基準は、拡散符号に関するものと航法データに関するものとに分けられており、航法メッセージ認証（ＮＭＡ）とも呼ばれる。
【０００５】
本発明の要素は、無線航法メッセージの認証のためのＴＥＳＬＡ（Time Efficient Stream Loss-Tolerant Authentication：時間効率ストリームロス許容認証）プロトコルの局面(aspect)に基づいている。
【０００６】
A. Perrig et al. “Timed Efficient Stream Loss-Tolerant Authentication (ＴＥＳＬＡ): Multicast Source Authentication Transform Introduction, (2005, Carnegie Mellon University, Network Working Group) は、送信者(sender)からのマルチキャスト又はブロードキャスト情報の受信機に保全性をチェックし、かつ情報を認証することを可能にする方法としてのＴＥＳＬＡのコンセプトを紹介している。
ＴＥＳＬＡは、非対称属性を達成し、それによってキーの管理タスクを最小にするために、対称的な暗号と時間遅延されたキーの開示を用いる。
その論文は、特にネットワーク通信の環境でデータパッケージの認証でのＴＥＳＬＡの使用に言及する。
それは無線標定あるいは無線航法へのその応用、又は衛星通信に言及しない。
著者は、無線航法でのＴＥＳＬＡプロトコルの使用を提案していないし、フェージングし、シャドウイングしている送信チャネルの利用可能性を分析していない。
【０００７】
Sherman C. Lo, et al., "Assessing the Security of a Navigation System: A Case Study using Enhanced Loran", Stanford Universityは、例えば高性能ロランで１つの与えられたのキーが、いくつかのＭＡＣsのために用いられる航法チャネルのためにＴＥＳＬＡの変更されたバーションを論じている。
ロランの安全性を高めるために、認証が他の手法と同様、重要な暗号に関して論じられている。
ＴＥＳＬＡデータ認証手法は１つのセクションで論じられている。そして、それはこれまで論じられた既知の手法である。
著者は、それをロランにより適したものにするために、航法チャンネルのためのＴＥＳＬＡの改変を開示した。
メッセージロスに対する耐性をデータ的に効率よく高めるための１つの変更は、与えら

れたキーをいくつかのＭＡＣsのために用いることであると述べられている。

【０００８】

C Wullems et al.: "Signal Authentication and Integrity Schemes for Next Generation Global Navigation Satellite Systems", Proceedings of the European Navigation Conference GNSS, 22 July 2005 (2005-07-22), 頁1-11, XP055141309, Munichは、ＴＥＳＬＡに基づくＮＭＡベースのＧＮＳＳ信号の認証のための手法を開示している。

送信機がハッシング関数Ｆによってキーチェーンを生成する。(i)前のタイムスロットの間に、第１(データ)タイプのメッセージから取得されたＭＡＣsから導出されたＭＡＣ(MAC'_{n+2})、及び現在のタイムスロットの間に、第２タイプのメッセージから取得されたキー（K_{n+2}）に対して暗号化されたキー生成関数Ｆ’を適用することで生成されたキー(K'_{n+2}）と、(ii)前のタイムスロットの間に第２タイプのメッセージから取得されたＭＡＣ(MAC'_{n+2})とが整合するか否かを、現在のタイムスロットの間に決定することにより、認証が実行される。

【０００９】

無線航法信号の認証のためにＴＥＳＬＡを利用している既知のシステムは次のステップに基づく：

・各送信機について、初期のランダムなシード(seed)$K_{i,n}$から、一方向(one-way)関数を通して再帰的に生成される$K_{i,n}$から$K_{i,0}$を生成すること、及び前記一方向チェーンを逆の順序($K_{i,0}$から$K_{i,n}$)で用いることであって、それによって、あるタイムスロットjにおいて、前記無線航法システムの送信機iが、前記一方向チェーンから前記キー$K_{i,j}$を用いるメッセージ認証符号($MAC_{i,j}$）でそのブロードキャストデータの認証を行うこと；

・各送信機iにより、前記ＭＡＣと共に、そして、前記キー$K_{i,j}$のある期間が経過した後、認証するデータを送信すること；

・前記受信機により、各送信機から、前記送信データである前記$MAC_{i,j}$及び前記キー$K_{i,j}$を受信すること；

・前記受信機により、データ自身と$K_{i,j}$から$MAC_{i,j}$を生成すること、及び衛星iから受信された前記$MAC_{i,j}$と比較することにより、衛星データの真正性を検証すること；

・前記受信機により、前記各送信機iからの前記各信号について、前に受信された証明書により真正であることが証明された前のチェーンのキー、例えば$K_{i,0}$を生成するため、前記一方向関数を再帰的に実行することにより、$K_{i,j}$の真正性を検証すること。

【００１０】

したがって、無線航法のためのＴＥＳＬＡプロトコルの既知の使用が、それによって各送信機からの各信号が独立して認証されるアプローチにつながり、そして問題は、認証処理（prosess）のための全ての必要とされるデータがそのデータが認証されるべきである送信機から受信される必要があるということである。

【００１１】

従来のシステムにおけるさらなる問題は、それらが、１つの衛星からのデータを他の衛星を認証するために最適に使用し、そしていくつかの衛星の認証のために必要とされるビット数の合計を最小にする可能性を提供しないことである。

それらは、また他の衛星を認証するために潜在的により良い受信条件の衛星からのデータを使う可能性を提供しない。

【００１２】

これらのファクターは、ある地球環境、例えば都市又は郊外のエリアでの局所的な障害により受信条件が一般に低下し、そして異なる衛星のために著しく変化する可能性のある衛星航法に基づく、いくつかの無線航法システムのための重大な問題を表している。

【発明の概要】

【発明が解決しようとする課題】

【００１３】

本発明の目的は、全ての無線航法送信機からの全てのデータの正常な復調を妨害する信号受信条件及びデータ復調条件を含む環境において、最適なレベルの強固性(robustness)と利用可能性(availability)で無線航法信号の認証を可能にすることである。

【課題を解決するための手段】

【００１４】

本発明の１つの態様によれば、それぞれが別の衛星に搭載された複数の送信機と、少なくとも１つの地上ベースの受信機を含む無線航法システムであって、受信機は、前記複数の送信機のそれぞれからの無線航法信号を受信するように適合されており、前記送信機のそれぞれ及び前記受信機は、所定の第１のキーチェーンにアクセスするように適合されており、前記第１のキーチェーンは、第１の暗号化キーと１つ以上のさらなる暗号化キーを含み、前記システムは：前記複数の送信機からの第１のグループの送信機であって、第１のグループの各送信機は、第１の無線航法信号を送信するように動作可能であり、第１の無線航法信号は、ある与えられた時点又は与えられたサブフレームの間、無線航法データ、メッセージ認証符号（ＭＡＣ）、及び１つ以上のさらなる暗号化キーの１つを含む、前記第１のグループの送信機を含み；

ＭＡＣは、各送信機に対してユニークであり、かつ前記第１の暗号化キーを用いて生成され；

１つ以上のさらなる暗号化キーの１つは、ＭＡＣの送信の所定時間後に送信され、

そして、受信機は、第１のグループの送信機の１つ以上からの前記第１の無線航法信号の全部又は一部を受信次第、その送信機又は他の任意の前記第１のグループの送信機から受信された前記１つ以上のさらなる暗号化キーの１つに基づいて、前記第１のグループの送信機の１つから受信された第１の無線航法信号を認証するように、動作可能な前記無線航法システムが提供される。

【００１５】

受信機は、前記受信された１つ以上のさらなる暗号化キーの１つを用いるか、又は前記第１の無線航法信号から派生可能な他の１つ以上のさらなる暗号化キーを用いて、第１の無線航法信号を認証するように動作可能であってもよい。

【００１６】

好ましくは、受信機は、少なくとも無線航法データ及びその第１の無線航法信号のＭＡＣの受信次第、受信された１つ以上のさらなる暗号化キーの１つに基づいて、受信された第１の無線航法信号を認証するように動作可能であってもよい。

【００１７】

前記又はそれぞれの第１の無線航法は、前記暗号化キーが前記無線航法データ及び/又は前記ＭＡＣの後に予め定められた遅延で送信されるように、複数の部分になっていてもよい。

【００１８】

１つの実施形態では、前記送信された暗号化キーは、前記第１のグループ内で全ての送信機について同じである。

その他の実施形態では、送信された暗号化キーは、第１のグループの各送信機について、第１のキーチェーンとは異なるものを含む。

【００１９】

第１の無線航法信号の各サブフレームについて、第１のキーチェーンの各暗号化キーは、一方向関数から再帰的に派生（derived）されるｎ個の暗号化キーの１つを含んでもよい。好ましくは、ｎは前記無線航法システムにおける送信機の総数とほぼ等しく、かつ、いずれにしても、それよりも大きい。

【００２０】

第１のグループの各送信機について、それぞれのＭＡＣは第１のキーチェーンのルートキーから取得されてもよい。

【００２１】

受信機は、受信された無線航法データ及び受信された１つ以上のさらなる暗号化キーの

１つに基づいて、派生（derived）ＭＡＣを生成し、かつ派生ＭＡＣを受信されたＭＡＣと比較することにより、無線航法信号を認証するように適合されてもよい。

【００２２】

１つの実施形態では、第１のグループの送信機は、前記無線航法システムにおける複数の送信機の全てを含む。

【００２３】

別の実施形態では、前記第１のグループの送信機は、前記無線航法システムにおける前記複数の送信機の厳密な(strict)サブセットを含む。残りの送信機は、第２のグループの送信機を含んでもよく、所定の第２のキーチェーンは、第２のグループの送信機及び受信機によってアクセス可能であり、第２のキーチェーンは、第１の暗号化キー及び１つ以上のさらなる暗号化キーを含む。好ましくは、前記第２のグループの各送信機は、第２の無線航法信号を送信するように動作可能であり、第２の無線航法信号は、ある与えられた時点又は与えられたサブフレームの間、無線航法データ、ＭＡＣ、及び１つ以上のさらなる暗号化キーの１つを含み；

ＭＡＣは、各送信機に対してユニークであり、かつ前記第１の暗号化キーを用いて生成され；

前記１つ以上のさらなる暗号化キー（Ｋ；$K_{j,1}$，$K_{j,2}$，$K_{j,3}$，$K_{j,4}$）の１つは、前記ＭＡＣの送信の所定時間後に送信され；

かつ、受信機は、第２のグループの送信機の１つ以上から第２の無線航法信号の全部又は一部を受信次第、その送信機又は他の任意の前記第２のグループの送信機から受信された１つ以上のさらなる暗号化キーの１つに基づいて、前記第２のグループの送信機の１つから受信された第２の無線航法信号を認証するように動作可能である、前記無線航法システムが提供される。

【００２４】

受信機は、受信された１つ以上のさらなる暗号化キーの１つを用いるか又は、そこから派生可能な他の１つ以上のさらなる暗号化キーを用いて、前記第１の無線航法信号を認証するように動作可能である。

【００２５】

受信機は、少なくとも無線航法データ及びその第２の無線航法信号のＭＡＣを受信次第、前記受信された暗号化キーに基づいて、前記受信された第２の無線航法信号を認証するように動作可能であってもよい。

【００２６】

前記又はそれぞれの第２の無線航法信号は、前記暗号化キーが前記無線航法データ及び/又は前記ＭＡＣの後に予め定められた遅延で送信されるように、複数の部分になっていてもよい。

【００２７】

１つの実施形態では、前記送信された暗号化キーは、第２のグループ内で全ての送信機について同じである。

その他の実施形態では、前記送信された暗号化キーは、前記第２のグループの各送信機について、前記第２のキーチェーンとは異なるものを含む。

【００２８】

前記第１の無線航法信号及び/又は前記第２の無線航法信号は、予想不能なビットを含む信号の部分が予測可能なビットを含む部分とインターリーブされるように送信されてもよい。

【００２９】

本発明の別の態様によれば、無線航法システムのための送信機であって、前記無線航法システムは、それぞれが別の衛星に搭載された複数の送信機、及び少なくとも１つの地上ベースの受信機を含み、前記受信機は、前記複数の送信機のそれぞれからの無線航法信号を受信するように適合されており、前記送信機のそれぞれ及び前記受信機は、所定の第１のキーチェーンにアクセスするように適合されており、前記第１のキーチェーンは、第１

の暗号化キー及び１つ以上のさらなる暗号化キーを含み、前記受信機は、前記第１のグループの送信機の１つ以上から前記第１の無線航法信号の全て又は一部を受信次第、その送信機又は他の任意の前記複数の送信機から受信された前記１つ以上のさらなる暗号化キーの１つに基づいて、前記送信機の１つから受信された第１の無線航法信号を認証するように動作可能であり：

送信機は、第１の無線航法信号を送信するように動作可能であり、第１の無線航法信号は、ある与えられた時点又は与えられたサブフレームの間、無線航法データ、ＭＡＣ、及び前記１つ以上のさらなる暗号化キーの１つを含み；ＭＡＣは、各送信機に対してユニークであり、かつ第１の暗号化キーを用いて生成されており、かつ前記１つ以上のさらなる暗号化キーの１つが、前記ＭＡＣの送信の所定時間後に送信される。

【００３０】

本発明の別の態様によれば、無線航法システムのための受信機であって、前記無線航法システムは、それぞれが別の衛星に搭載された複数の送信機、及び少なくとも１つの前記受信機を含み、前記送信機のそれぞれ及び前記受信機は、所定の第１のキーチェーンにアクセスするように適合されており、前記第１のキーチェーンは、第１の暗号化キー及び前記１つ以上のさらなる暗号化キーを含み、各送信機は、第１の無線航法信号を送信するように動作可能であり、前記第１の無線航法信号は、ある与えられた時点又は与えられたサブフレームの間、無線航法データ、ＭＡＣ、及び前記１つ以上のさらなる暗号化キーの１つを含み；ＭＡＣは、各送信機に対してユニークであり、かつ前記第１の暗号化キーを用いて生成されており；前記１つ以上のさらなる暗号化キーの１つは、前記ＭＡＣの送信の所定時間後に送信され；前記受信機は、前記複数の送信機のそれぞれからの無線航法信号を受信するように適合されており、かつ、前記受信機は、前記送信機の１つ以上から前記第１の無線航法信号の全て又は一部を受信次第、その送信機又は他の任意の前記複数の送信機から受信された前記１つ以上のさらなる暗号化キーの１つに基づいて、前記送信機の１つから受信された前記第１の無線航法信号を認証するように動作可能である、前記受信機が提供される。

【００３１】

本発明の別の態様によれば、無線航法システムのための無線航法の方法であって、無線航法システムは、それぞれが別の衛星に搭載された複数の送信機、及び少なくとも１つの地上ベースの受信機を含み、前記受信機は、前記複数の送信機のそれぞれからの無線航法信号を受信するように適合されており、

前記方法は、前記送信機のそれぞれ及び前記受信機に対して、第１の暗号化キー及び１つ以上のさらなる暗号化キーを含む所定の第１のキーチェーンへのアクセスであって、前記複数の送信機のそれぞれから第１の無線航法信号を送信し、前記第１の無線航法信号は、ある与えられた時点又は与えられたサブフレームの間、無線航法データ、ＭＡＣ、及び前記１つ以上のさらなる暗号化キーの１つを含み、前記ＭＡＣは、各送信機に対してユニークであり、かつ前記第１の暗号化キーを用いて生成されており、前記１つ以上のさらなる暗号化キーの１つは、前記ＭＡＣの送信の所定時間後に送信される、前記アクセスを提供し；

受信機で、前記複数の送信機の１つ以上から第１の無線航法信号の全て又は一部を受信し、かつ前記受信機で、前記複数の送信機におけるその送信機又は他の任意の送信機から受信された１つ以上のさらなる暗号化キーの１つに基づいて、前記複数の送信機の１つから受信された第１の無線航法信号を認証すること、を含む前記方法が提供される。

【００３２】

本発明の別の態様によれば、処理回路による実行のため、および少なくとも請求項２１におけるステップに対応する命令を定義するかまたは変換可能なデータが記録または蓄積された、記録可能、書き換え可能または蓄積可能な媒体が提供される。

【００３３】

本発明の別の態様によれば、通信装置と記憶装置を含み、オンデマンドまたは他の方法で、処理回路による実行のため、および少なくとも請求項２１におけるステップに対応す

る命令を定義するかまたは変換可能なデータを送信するように構成されたサーバーコンピューターが提供される。

【００３４】

本発明の実施形態は、無線航法の認証のためのＴＥＳＬＡプロトコルの最適化された実装を提供する。

本発明の実施形態は、各無線航法信号送信機のための単一の一方向チェーンの使用とは対照的に、全て又は複数の無線航法信号送信機のための単一の一方向チェーンを用いる。

本発明の実施形態は、以下のとおりに要約することができる（この文献において、“送信機”と”送信者”は置き換え可能に用いられる。）。

【００３５】

１）無線航法システムは以下のステップを実行する（送信者側）：

・一方向関数Ｈを通して再帰的に生成されるK_nからK_0までのキーである単一のチェーンが、初期のシードK_nから、前記ＴＥＳＬＡプロトコルに従って、前記システムによって計算される；

・前記一方向チェーンを構成する前記キーは、複数の送信者からの前記送信者データを以下のように認証するために、逆の順序（K_0からK_n）で用いられる：

・ある期間jで、前記システムは、前記チェーンの１つのキーK_jを用いる；

・前記１つのキーK_jは、各送信者iに対してアプリオリに異なるメッセージ認証符号$MAC_{(j,i)}$を生成する、複数の送信者のそれぞれの送信者iによって送信された現在又は最近のデータD_iを認証するために用いられる；

・前記送信者は、それぞれの自身の航法データD_iに加えて、全ての送信者について同じ単一のキーK_jで生成される前記メッセージ認証符号$MAC_{(j,i)}$を、そしてその後、全ての送信者からの前記単一のキーK_jを送信する。

【００３６】

２）無線航法受信機は以下のステップを実行する：

・可視の送信者のそれぞれからの航法データＤiは受信され、蓄積される；

・前記システムからの前記送信者からの前記メッセージ認証符号$MAC_{(i,j)}$は受信され、蓄積される；

・ひとたび全ての送信者からの前記単一のキーK_jが成功裏に受信されると、それらのいくつか、又はそれらのどれもが、前に受信された前記メッセージ認証符号$MAC_{(j,i)}$を生成することにより、各送信者からの前記航法データD_iの認証に用いられる；

・受信機は、それらの真正性が任意、いくつか又は全ての前記送信者から受信された前の証明書、又は他の任意の手段により証明されているK_{j-1}からK_0の間の前記チェーン内の前のキーにそれを関連付ける一方向関数を実行することにより、前記間隔で適用可能な前記単一のキーK_jの真正性を検証できる。

【００３７】

本発明の利点は、単一のキー、又は数個の無線航法信号送信機からの同じチェーンからの複数のキーを用いることによる、無線航法サービスにおける性能向上である。

【００３８】

さらなる利点は、前記システムが、前記送信者又は他の任意の送信者からの前記キーを用いている間に、前記送信者からの前記キーが前記無線航法信号から適切に復調されなくても、前記送信者からの前記データ及びＭＡＣを用いることにより、ある特定の送信者からの無線航法データ及び信号を認証可能なことである。

その結果としての利点は、低品位の受信状態で前記認証エラーレート（ＡＥＲ）を徹底的に低減することである：前記同じキー又は前記同じチェーンを介して全ての前記衛星が認証されるのを可能にすることにより、ユーザーは、全ての衛星を認証するために、サブフレーム毎に１つの衛星から正しいキーだけを受信することが必要なだけである。これは、認証された送信者を使って計算された、位置及び確定時刻（time fix）のために必要なビットの量を劇的に減らす。

【００３９】

実施形態では、単一のキー使用は、静的状態（即ち、前記チェーンの前のキーが正しいと証明された後）での前記認証エラーレートの低減に有益なだけでなく、初期化(initialisation)を支援する。任意の送信者又は任意のソースからのただ１つの証明されたキーが必要とされるからである。

【００４０】

上記のことに加えて、本発明の実施形態は、１つ又は少数の衛星が良好な受信状態で低ビットエラーレートで観測され、ずっと高いビットエラーレートを伴う別のより低い仰角（elevation）又はより視程（visibility）の悪い衛星に囲まれたところで特に有利である。受信機は、認証されるべき各々の視認性の悪い衛星からの前記キーを受信することが必要であることと反対に、少数のＭＡＣビットが視認性の悪い衛星から受信されている限り、視認性の良い衛星からのキーを視認性の悪い衛星の認証に用いることができるからである。

【図面の簡単な説明】

【００４１】

ここで、本発明の実施形態が添付図面を参照する参考例によって記述される。即ち：

【００４２】

【図１】図１は、本発明の実施形態に従う無線航法システムの概略図である；

【００４３】

【図２】図２は、図１の実施形態及び別の既知の実装についての与えられた（given）ビットエラーレート（ＢＥＲ）に対する認証エラーレート（ＡＥＲ）性能のグラフを示すものである；

【００４４】

【図３】図３は、異なる衛星から異なるキーを送信するための単一のキーの使用を示す、本発明の別の実施態様に従う無線航法システムを基本とする技術の概略図である；

【００４５】

【図４】図４は、本発明の別の実施態様に従う無線航法システムであって、それによって、各衛星が前記同じチェーンからの異なるキー（$K_{j,1}$，$K_{j,2}$，その他）を送信しており、これらが図３に示されていように用いられたチェーンキーである無線航法システムの概略図である；

【００４６】

【図５】図５は、航法データ認証の送信の典型的な実装を示すものである；そして、

【００４７】

【図６】図６は、予測不能及び予測可能なビットが最大予測可能時間を最小にするためにインターリーブされた、本発明の別の実施態様を基本とする概念の概略図である。

【発明を実施するための形態】

【００４８】

以下、同じ番号は同じ要素を表すためにも用いられる。

【００４９】

図１は、本発明の実施形態に従う無線航法システム100であり、それによって各衛星が最初に自身のＭＡＣ、そして次に同じキーを送信している無線航法システムの概略図である。

この実施形態の目的は、ＡＥＲを最小化することによって、少なくとも４つの衛星を用いて位置及び確定時刻を計算するために、全ての衛星から復調されることが必要なビット数を少なくすることによって、認証の利用可能性を最適化することである。

【００５０】

複数の衛星上の送信機（図示されていない）は、それぞれの無線航法信号を送信し、それらはアンテナ108を通り、地上106をベースとする受信機104で受信される。（この実施形態では、４つの衛星が示されている；しかしながら、当業者は、より多くの、あるいはより少ない衛星が実際には用いられてもよいことを理解するであろう。この文書では、説明の目的で、「衛星」と「送信機」が置き換え可能に用いられる。）

【００５１】
第１の衛星110は、第１の衛星110とユニークに対応し、キーＫが続くＭＡＣ符号ＭＡＣ1を含む第１の無線航法信号112を送信する。
第２の衛星114は、第２の衛星114とユニークに対応し、キーＫが続くＭＡＣ符号ＭＡＣ2を含む第２の無線航法信号116を送信する。
第３の衛星118は、第３の衛星118とユニークに対応し、キーＫが続くＭＡＣ符号ＭＡＣ3を含む第３の無線航法信号120を送信する。
第４の衛星122は、第４の衛星122とユニークに対応し、キーＫが続くＭＡＣ符号ＭＡＣ4を含む第４の無線航法信号124を送信する。
【００５２】
この実施形態の所期の成果－ＡＥＲの最小化－は、ＮＭＡがあらゆる種類のユーザー及び受信環境のために動作（work）しなければならないとすれば、前記ＮＭＡソリューションは、困難な受信環境で動作するように最適化されなければならないことを意味する。
標準的な量販の受信機がフルの航法データ構造を構成するために、異なるサブフレームからのメッセージブロックを混合することができることに留意しなければならない。
これは、１つの単一フレーム内で前記認証ビットの全体が正確に受信されなければならないＮＭＡにとって可能ではない。それらは強固さを改良するために異なるサブフレームで異なるからである。
【００５３】
次の表記と用語が用いられる：
・K_n：一方向チェーンのシード、即ち、前記一方向チェーンの最初の値；
・K_0：一方向チェーンのルート（root）、即ち、前記一方向チェーンの最後の値（又は前記K_0により正しいと証明された最新の値）；
・K_j：あるサブフレームjで送信された全てのMACsと関連したキー；
・$ＭＡＣ_i$：衛星iからの認証データで生成され、そして衛星i航法信号内で送信されたメッセージ認証符号；
・Ｈ：$K_0 = H^n(K_n)$にするために、前記チェーンを計算するために用いられる一方向関数、ここで、H^nは、関数Ｈを再帰的にｎ回実行することを意味する。
・$K_{j,i}$：サブフレームj内で衛星iによって送信されたキー。
【００５４】
これらの前提で、再び図１を参照し、そしてこの実施形態についての手順は次のように記述される。
・あるキーＫに関連するある30-秒間、各衛星iは、K_j及び衛星データ、又はそのサブセットである$Ｄ_i$を用いて$ＭＡＣ_i$を送信する。認証される前記データ$Ｄ_i$は、少なくとも衛星時刻、軌道及びクロックを含んでよく、そして衛星ＩＤ、コンテキスト情報、電離層補正、他の衛星コンステレーションに対するオフセット時間又はＵＴＣのような時刻基準、又はブロードキャスト信号の群遅延のような他の情報を付加してもよい。
・$ＭＡＣ_i$の前記送信の後、前記衛星は、それぞれの前記$ＭＡＣ_j$を生成するために用いられた全ての同じキーＫを送信する。即ち、前記キーＫは$ＭＡＣ_i$の前記送信の所定時間後に送信される。実際には、前記キーＫの送信は、$ＭＡＣ_i$の前記送信の完了の所定時間後に始まることを意味してもよい。
前記所定時間は、１又は数ミリ秒から数分のオーダーでよく、そしてより好ましくは、30-秒間に適合させるため、１から30秒未満のオーダーである。
・前記受信機104はデータで認証された位置、速度及びタイミング（ＰＶＴ）を計算するため、ただ１つのキーＫを成功裏に復調することが必要とされる。
図１に示されるように、Ｋを衛星２（114と表示された）－最も高い仰角にあり、それ故、アプリオリにより良い視程状態を有する－から受信することにより、他の全ての衛星110,118及び122からのデータは、それらのＭＡＣs（それぞれＭＡＣ1，ＭＡＣ3，ＭＡＣ4）が受信されさえすれば、認証することができる。
【００５５】

実施形態では、前記システムは、次の設計パラメータの１つ、いくつか又は全てを採用する。

・前記一方向チェーンは、224ビットの長さのキーのチェーン（Ｋ）を構成するために、ＳＨＡ-2ファミリーの関数、例えばＳＨＡ-256、又はそれによって最後のビットが落とされる（dropped）本質的にＳＨＡ-256であるＳＨＡ-224を使用する。これは、セキュリティ基準に従う十分なセキュリティレベル（112の対称的なビット）を可能にする。前記システムのセキュリティ要件によって、より長い又はより短いキーを用いることもできる。

・最初の（primitive）前記ＭＡＣはＨＭＡＣ-256でよい。

・前記衛星から送信された前記ＭＡＣは、最後の15ビットが切り捨てられる。前記キーを持たずに15-ビットのＭＡＣを正確に推定する確率は、このような攻撃を思いとどまらせるのに十分低いと考えられるおよそ3×10^{-5}である。

・前記キーの期間は30秒でよい。

・前記チェーンの長さは、１週間で20160個のキーをもたらす。

【００５６】

しかしながら、当業者により、他の実施形態に従い、そしてその実装に応じて、他の値が採用されてもよいことを理解されるであろう。

【００５７】

図２は、図１の実施形態及び別の既知の実装についての与えられたビットエラーレート（ＢＥＲ）に対するＡＥＲの性能のグラフを示すものである。比較の目的ために、図２は、３つのＮＭＡの実装についてのＡＥＲの性能を表す－

・標準的な466ビットのデジタル署名を介したＮＭＡを衛星毎に１つ；

・衛星毎に、１つの異なる224-ビットキー及び15-ビットが切り捨てられたＭＡＣを有する標準的なＴＥＳＬＡプロトコルのアプローチを介したＮＭＡ；及び

・全ての衛星からの同じ224-ビットキー及び15-ビットが切り捨てられたＭＡＣsを有する、本発明に従う標準的な前記単一チェーンのＴＥＳＬＡプロトコルのアプローチを介したＮＭＡ。

【００５８】

図２において、ＡＥＲはＢＥＲとＮＡから次の式によって算出される：

$$ＡＥＲ＝１－(1-ＢＥＲ)^{ＮＡ},$$

ここでＢＥＲは前記ビットエラーレートであり、ＮＡは認証のために必要とされるビットの数である。図２は次のように解釈されるべきである：所定のＢＥＲを有する受信機104の視野に４つの衛星（110,114,118,122）があり、“4-衛星ＡＥＲ”の値は、４つの衛星が、ＮＭで認証された（ＮＭ-authenticated）位置及び時刻の値（後者は時折ＰＶＴと呼ばれる）の計算を可能にする航法メッセージで認証されたものとなる（navigation-message-authenticated）確率であると仮定する。

いかなるケースでも、前記受信機104は認証されるべき航法データを既に受信したものとする。

結果は、本発明の実施形態（“224/15-1C-ＴＥＳＬＡ”のソリッドトレース（solid trace））の使用によって、他の既存の方法と比べて、大幅な向上を示している。例えば、位置と時間決定を計算するために４つの衛星を用いることで：

・466-ビットの楕円曲線署名を用いている標準的なデジタル署名により必要とされる認証ビット：446＊4＝1864ビット。

・15-ビットが切り捨てられたＭＡＣ及び224-ビットキーを使用している標準的なＴＥＳＬＡのケースに必要とされる認証ビット：（15＋224）＊4＝956ビット。

・本発明の実施形態（15-ビットが切り捨てられたＭＡＣ＋224-ビットのキー）により必要とされる認証ビット：15＊4＋224＝284ビット。

【００５９】

もし４つより多い衛星が位置及び時刻の計算のために用いられるなら、このビット差分はさらにより高い、そしてそれは標準的なケースである。例えば、もし７つの衛星が用い

られるなら、前記ビット差分は標準的なＴＥＳＬＡのケースの1673ビットに対して、本発明の実施形態の329ビットとなるであろう。即ち５倍少ない。

【００６０】

図３は、信号予測不能性特性（signal unpredictability feature）を高めるために、異なる衛星から異なるキーを送信するための一のチェーンからのキーの使用を示す本発明の別の実施形態に従う無線航法システムの概略図である。これは、以下で記述されるような場合を除いて、図１の実施形態と同じである。

【００６１】

この実施形態の目的は、前の実施形態のように、単一の一方向チェーンを使用するのと同じ利点を維持しつつ、前記信号を予測不能にする特性を高めることにより、リプレイ攻撃に対する強固性を最大化することである。

もし前記予測不能なシンボルが、後に認証処理によって正しいと認証される必要があるのであれば、航法シンボル又はビットの予測不能性の最大化は、リプレイ攻撃に対する強固性を提供する。

【００６２】

単一の一方向チェーンを全ての衛星（110,114,118,122；図１）に対して用いるときに生ずる１つの現象は、もし同じキーが用いられ、そして全ての衛星から同時に送信されたならば、衛星クロックのオフセット及び、主として、前記衛星から前記受信機104までの距離に関連する到着時刻によって、それは異なる時刻でユーザー（受信機104で）によって受信されることである。

例えば、天頂で23，200kmの高さの衛星からの信号は、地球表面に到達するまで、約77.3msを要する。しかし、同じ若しくは類似の円軌道上であるもののより低い仰角の衛星からの信号が地球の表面に到達するためには、いくらか多くのミリ秒を要する（地球上のユーザーについては、常にほぼ地球の半径に対する光速である21ms未満である）。

攻撃者は、これらのミリ秒を用いて最も高い衛星からのＴＥＳＬＡキーを構成している予測不能ビットを推定し、それを別の衛星からの遅れをもってリプレイすることで、前記位置の妨害を容易に行うことができるであろう。

【００６３】

したがって、もし全ての衛星が同時に同じキーを送信しているなら、天頂に最も近い衛星からのシンボルだけが予測不能であろう。攻撃者はそれらを推定し、最も仰角の低い衛星からの信号にリプレイすることができるから。

【００６４】

この問題は、キーチェーンの長さを増やし、かつ異なるキーを、しかし、異なる衛星から依然として同じチェーンから送信することによって、克服することができる。このキーは、前記一方向関数を実行することによって、あるサブフレームで全てのＭＡＣsの計算のために用いられた前記キーＫjの決定を可能にするであろう。

【００６５】

図３の実施形態では、ＭＡＣsに対するＫＥＹの関係が用いられる。

・全てのサブフレームjについて、全ての衛星により送信された全てのＭＡＣsを計算するために単一のキーが使用される。

・このキーは、前のサブフレームj-1に対して用いられた40回の一方向関数のキーである：

$K_j = H^{40}(K_j\text{-}1)$。

40がサブフレーム毎に40個のキーに対応するために用いられたことに留意されたい：即ち、１つはＭＡＣs（k，k+1，その他）に対して用いられ、他の39個は39個の衛星に対しても用いることができる。これはＧＮＳＳコンステレーションからの全ての衛星に対応するのに十分な余裕を提供する。

・全てのサブフレームjについて、各衛星iは、

$MAC_{(j,i)} = M(d_{j,i}||m_i, K_j)$

となるように前記キーK_jに基づくＭＡＣを送信する。

ここで、Mは15ビットが切り捨てられた前記ＭＡＣ関数ＨＭＡＣ-ＳＨＡ-224、$d_{j,i}$はＨＭＡＣの結果をユニークにする付加情報、そしてm_iは署名されるべき航法データである。

・全てのサブフレームjについて、各衛星iは、

$K_{j,1}=H^i(K_j)$

となるようにキー$K_{j,1}$を送信する。

【００６６】

したがって、例えば、衛星ＳＶＩＤ5は、キーK_jを取得するために５回ハッシュされる必要があるキー（$K_{j,5}$）を送信する。このようにして、任意の衛星からのＭＡＣは、他の任意の衛星から受信されたキーに対して認証することができる。一方、全てのサブフレームで送信される全てのK_jは依然として予測不能であろう。このビット予測不可能性の特徴を保持するサブフレーム毎の40個の一方向関数を持つことのさらなる負担は、標準的及び未来の受信機のために、手ごろな価格で取得可能と思われることが留意されるべきである。

【００６７】

図３に見られるように、１つのチェーンからのキーを用いて、異なるキーが異なる衛星から送信される。最初のチェーンは、各サブフレームについて、KmとKm+41の間のキーが１つのサブフレーム及び衛星コンステレーション全体に割り当てられることを示す。２番目のチェーンは、最初のキーK_jが、前のチェーンでKmと等しく、全ての衛星からの前記ＭＡＣsを計算するために用いられることを示すのに対し、$K_{j,i}$はiが１と40の間にある衛星iから送信されたキーである。

【００６８】

このアプローチを用いて、受信機104は１つのキー$K_{j,i}$を受信し、そしてＭＡＣsを計算するために用いられるキーK_jを決定するために一方向関数をi回実行することができる。それと同時に、信号のリプレイに対する強固性を最大にするので、各衛星iから送信されたキー$K_{j,i}$は予測されることはできない。

【００６９】

図４は、本発明の別の実施態様に従う無線航法システム400であって、それによって、各衛星が同じチェーンからの異なるキー（$K_{j,1}$，$K_{j,2}$，その他）を送信している無線航法システムの概略図である。これは、次に記載されていること以外は、図１の実施形態と同じである。当然ながら、この実施形態は図３に示されたチェーンキーを用いる。

【００７０】

第１の衛星110は、第１の衛星110にユニークに対応するＭＡＣ符号ＭＡＣ1と後続するキー$K_{j,1}$を含む第１の無線航法信号412を送信する。第２の衛星114は、第２の衛星114にユニークに対応するＭＡＣ符号ＭＡＣ2と後続するキー$K_{j,2}$を含む第２の無線航法信号416を送信する。第３の衛星118は、第３の衛星118にユニークに対応するＭＡＣ符号ＭＡＣ３と後続するキー$K_{j,3}$を含む第３の無線航法信号420を送信する。第４の衛星122は、第４の衛星122にユニークに対応するＭＡＣ符号ＭＡＣ4と後続するキー$K_{j,4}$を含む第４の無線航法信号424を送信する。

【００７１】

前述したように、もし受信機104が、４つの衛星110，114，118，122からＭＡＣs（ＭＡＣ1，ＭＡＣ2，ＭＡＣ3，ＭＡＣ4）及び最も高い衛星からのキー（$K_{j,2}$）のみを受信したら、それはK_j（$K_j=H^2(K_{j,2})$）を計算し、それにより、各信号からの信号リプレイに対する強固性を検証するだけでなく、ＭＡＣsに対する衛星からのデータを検証することができる。

【００７２】

あるサブフレームで送信される、しかしそのサブフレーム（例えば、図４における$K_{j,3}$と$K_{j,4}$）で正確に復調されたキーから計算することのできない、これらのキーは、次の任意のサブフレームで受信された任意の衛星からの任意のキーから計算することができる。例えば：$K_{j,3}=H^{41}(K_{j+1,4})$。

【００７３】
別の実施形態では、同じキーK_j（図１の実施形態を参照）を送信している送信者（衛星110，114，118，122）の全体の代わりに、各送信者が、各グループに対する異なる一方向チェーンからのグループ内で異なるキーを用いている２つ又はより多くのグループの送信者が存在してもよい。
この実施形態は、全ての送信者からの単一のキーの使用を避けることがより安全であると考えられるため、キーの管理又は他の理由でセキュリティを高めることができる。
【００７４】
別の実施形態では、同じキーK_jが、各送信者（衛星110，114，118，122）で異なり、かつエンコードされたキー情報の全体が受信されるまで受信機104で予測不能な方法でエンコードされる。
これは、例えば、キーK_jと共に、各衛星について異なり、かつ予測不能な置換及び転置（substitution and permutation）ネットワークによるK_j及びノンス（nonce）のエンコード、及びノンスの送信により達成される。
【００７５】
別の実施形態では、演算がビット及びシンボルを前記送信データのストリームの中で予測不能に拡散させることを含む。これはリプレイ攻撃に対する強固性を高めるという利点を持っている。
【００７６】
図５は、航法データ認証の送信の典型的な実装を示すものである。その上、特に図５は、前記予測不能情報ビットの全体が前記デジタル署名として送信される実装を示している。認証50は送信54の後、時間52で起こる。このことは、認証の間、前記時間52の大部分の間続く最大予測可能時間56を導く。最大予測可能時間56は、攻撃者が信号リプレイ攻撃の前に前記追尾ループを支配することができる期間である。したがって、最大予測可能時間56が短いほど、それだけ受信機104このタイプの攻撃に対してより強固になり得る。
【００７７】
図６は、航法データ認証の送信に関連して予測不能及び予測可能なビットが最大予測可能時間66を最小にするために、インターリーブされた本発明の別の実施態様を基本とする概念の概略図である。これは、以下で記述するものを除き、図１の実施形態と同じである。
【００７８】
認証60は送信64の後、時間62で起こる。図６の実施形態の目的は、信号リプレイ攻撃に対する強固性を高めることである。このような防護を提供するために、認証不能ビット68は、認証されるべきであり、かつ認証のために用いられたデータが完全に受信されるやいなや実行された認証の検証において検証されなければならない。もし信号中で送信されていれば、これはキーK_0の証明書と共にある衛星のデータ、ＭＡＣ及びキーに対して実行可能である。したがって、本実施形態では、予測不能と考えられるデータビットは：
・前記キーK_j；
・前記ＭＡＣsＭＡＣ1，ＭＡＣ2，等；及び
・K_0(前記チェーンのルートキー)の真正性を証明するため、非対称暗号化手法によって前記信号中に送信された証明書の前記デジタル署名、ＤＳ(K_0)。
【００７９】
K_0証明書の検証の目的は２通りある：第１は、前記ＭＡＣ及びキーKjが正しいことを保証することであり、第２は、信号リプレイ攻撃に対する防御を向上させることである。
もし予測不能なデジタル署名を含むK_0証明書が連続的に送信されたなら、そのことは、衛星が後に検証される予測不能なビットを連続的に送信することができるようにする、より高い反リプレイ検証性能を可能にする。
【００８０】
それぞれの実施において種々の構成要素を有する様々な実施形態を参照して、実施形態について説明してきたが、他の実施形態では、これらの構成要素および他の構成要素の組

合せおよび置換を利用することが理解されるであろう。

【００８１】

また、実施形態のいくつかは、コンピュータシステムのプロセッサによって、または機能を実行する他の手段によって実装可能な方法または方法の要素の組合せとして本明細書中に記載されている。したがって、このような方法または方法の要素を実行するために必要な命令を有するプロセッサは、方法または方法の要素を実行するための手段を構成する。さらに、装置の実施形態についての本明細書に記載の要素は、本発明を実施する目的で要素によって実行される機能を実行するための手段の一例である。

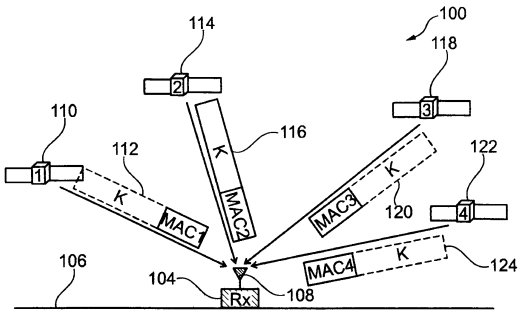
【００８２】

本明細書で提供される説明においては、多数の特定の細部が記載されている。しかしながら、本発明の実施形態は、これらの特定の細部なしに実施できることが理解される。さらに、周知の方法、構造、および技術は、この説明に対する理解を不明瞭にしないために詳細には示されていない。

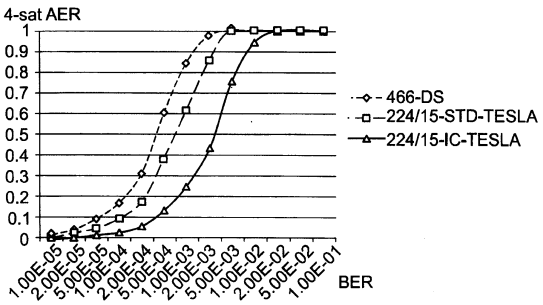
【００８３】

このように、本発明の好ましい実施形態であると考えられるものを説明してきたが、当業者は、他の変形または更なる変形が本発明の精神および範囲から逸脱することなくなされ得ることを理解するであろう。また、本発明の範囲内に入るような全ての変更及び変形は、請求を意図したものである。例えば、上記の任意の式は、使用可能な手順の単なる代表例である。ブロック図において機能を追加または削除することができるし、機能ブロック間で動作を交換することもできる。また、記載した方法において、本発明の範囲内でステップを追加または削除することができる。

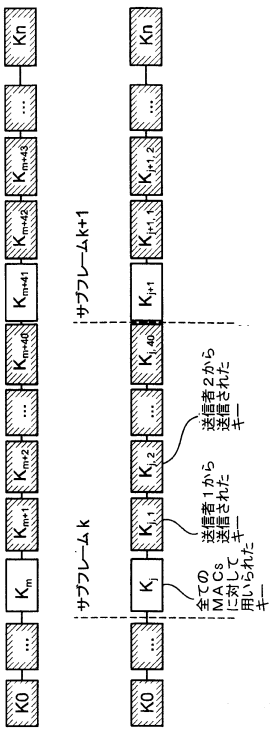
【図１】



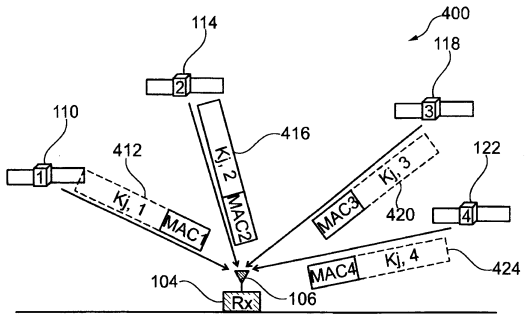
【図２】



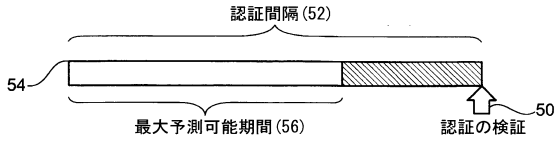
【図３】



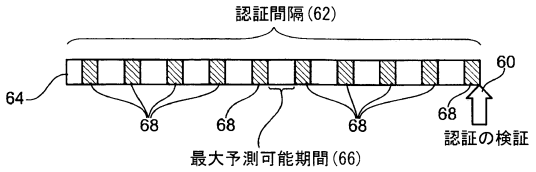
【図４】


114
400
118
110
412
416
122
Kj, 2
MAC2
Kj, 3
MAC3
420
Kj, 1
MAC1
MAC4
Kj, 4
424
104
106
Rx
1
2
3
4

【図５】


認証間隔(52)
54
50
最大予測可能期間(56)
認証の検証

【図６】


認証間隔(62)
64
60
68
68
68
68
認証の検証
最大予測可能期間(66)

フロントページの続き

(51)Int.Cl.			FI		
G09C	*1/00*	*(2006.01)*	H04L	9/00	675A
H04L	*9/16*	*(2006.01)*	G09C	1/00	640D
			H04L	9/00	643

(72)発明者 フェルナンデス ヘルナンデス、イグナシオ
ベルギー、ビー－１１７０ ワーテルマール－ボワフォール、アヴェニュー ド ヴィゼ８１

審査官 安井 英己

(56)参考文献 特表２０１３－５３４６２２（ＪＰ，Ａ）
米国特許出願公開第２０１３／０２５１１５０（ＵＳ，Ａ１）
千野 孝一 Koichi CHINO, スプーフィングを対象とした民生用衛星測位システムの脆弱性軽減方法の開発 The development of decrease of vulnerabilities of Civilian GNSS in targeting of spoofing, 電子情報通信学会技術研究報告 IEICE Technical Report SANE2013-34(2013-06), 日本, 一般社団法人電子情報通信学会 The Institute of Electronics,Information and Communication Engineers, ２０１３年 7月１２日, 第113巻, No.88, p.109-116
Wesson, K., Rothlisberger, M. and Humphreys, T. , Practical Cryptographic Civil GPS Signal Authentication, Journal of The Institute of Navigation, 米国, Institute of Navigation, ２０１２年, Vol. 59, No.3, Fall 2012, p.177-193
Wullems, C. Pozzobon, O. and Kubik, K., Signal Authentication and Integrity Schemes for Next Generation Global Navigation Satellite Systems, Proceedings of the European Navigation Conference GNSS, 2005, Munich, Germany, ベルギー, The European Group of Institute of Navigation, ２００５年, p.1-10, ＵＲＬ, https://eprints.qut.edu.au/38275/

(58)調査した分野(Int.Cl., ＤＢ名)
Ｇ０１Ｓ ５／００－ ５／１４,
Ｇ０１Ｓ １９／００－１９／５５,
Ｇ０９Ｃ １／００,
Ｈ０４Ｌ ９／００,
ＣＳＤＢ