

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第6452205号
(P6452205)

(45) 発行日 平成31年1月16日 (2019. 1. 16)

(24) 登録日 平成30年12月21日 (2018. 12. 21)

(51) Int. Cl.	F I
HO 4 L 9/36 (2006. 01)	HO 4 L 9/00 6 8 5
HO 4 L 9/08 (2006. 01)	HO 4 L 9/00 6 0 1 B
HO 4 L 9/32 (2006. 01)	HO 4 L 9/00 6 0 1 E
	HO 4 L 9/00 6 7 5 B

請求項の数 12 (全 26 頁)

(21) 出願番号	特願2016-504704 (P2016-504704)	(73) 特許権者	514238135
(86) (22) 出願日	平成26年3月28日 (2014. 3. 28)		エアバス・ディフェンス・アンド・スペース・リミテッド
(65) 公表番号	特表2016-514914 (P2016-514914A)		イギリス・SG1・2AS・ハートフォードシャー・スティーヴネージ・グネルス・ウッド・ロード・(番地なし)
(43) 公表日	平成28年5月23日 (2016. 5. 23)	(74) 代理人	100107456
(86) 国際出願番号	PCT/EP2014/056354		弁理士 池田 成人
(87) 国際公開番号	W02014/154890	(74) 代理人	100162352
(87) 国際公開日	平成26年10月2日 (2014. 10. 2)		弁理士 酒巻 順一郎
審査請求日	平成29年2月7日 (2017. 2. 7)	(74) 代理人	100123995
(31) 優先権主張番号	13275084.5		弁理士 野田 雅一
(32) 優先日	平成25年3月28日 (2013. 3. 28)	(74) 代理人	100148596
(33) 優先権主張国	欧州特許庁 (EP)		弁理士 山口 和弘

最終頁に続く

(54) 【発明の名称】 衛星システムにおける鍵配布

(57) 【特許請求の範囲】

【請求項 1】

衛星と前記衛星から信号を受信するように構成されているデバイスとを備える衛星システムにおいてセッション鍵を送信する方法であって、前記方法が、

前記衛星において前記セッション鍵を得るステップと、

前記衛星の秘密鍵及び前記デバイスの公開鍵に基づいて、前記衛星において前記セッション鍵を保護するステップと、

前記保護セッション鍵を前記衛星から前記デバイスに送信するステップであって、前記保護セッション鍵を送信するステップが、複数の所定部分を含むデータストリームを通じて、前記保護セッション鍵の所定数のバイトを前記複数の所定部分の各々に挿入することによって、前記保護セッション鍵を送信するステップを含む、ステップと、

を含む、方法。

【請求項 2】

前記保護セッション鍵を送信するステップが、前記保護セッション鍵、及び、前記保護セッション鍵が以前に送信されているか否かを判定するためのリプレイ検出情報を送信するステップを含む、請求項 1 に記載の方法。

【請求項 3】

前記保護セッション鍵及び前記リプレイ検出情報が、鍵配布メッセージに含まれる、請求項 2 に記載の方法。

【請求項 4】

10

20

前記得られたセッション鍵が、現在のセッションに後続する次のセッションに使用するための次のセッション鍵であり、前記方法が、

前記現在のセッションに使用するための現在のセッション鍵を得るステップと、

前記衛星の秘密鍵及び前記デバイスの公開鍵に基づいて、前記衛星において前記現在のセッション鍵を保護するステップと、

前記データストリームを通じて前記現在のセッション鍵を送信するステップと、

前記データストリームを通じて有効性情報を送信するステップであって、前記有効性情報が、前記現在のセッション鍵が有効である期間及び前記次のセッション鍵が有効である期間を規定する、送信するステップと、

をさらに含む、請求項 1、2 又は 3 に記載の方法。

10

【請求項 5】

衛星と前記衛星から信号を受信するように構成されているデバイスとを備える衛星システムにおいてセッション鍵を得る方法であって、当該方法が、

前記デバイスにおいて、前記衛星からデータストリームを受信するステップであり、前記データストリームは複数の所定部分を含む、ステップと、

前記複数の所定部分の各々から保護セッション鍵の所定数のバイトを抽出するステップと、

前記保護セッション鍵の前記抽出されたバイトを結合して、前記保護セッション鍵を得るステップと、

前記衛星の公開鍵及び前記デバイスの秘密鍵に基づいて、前記デバイスにおいて、前記受信された保護セッション鍵から前記セッション鍵を得るステップと、
を含む、方法。

20

【請求項 6】

前記保護セッション鍵が送信されたときの前記衛星の予測位置に関する情報を得るステップと、

前記保護セッション鍵が受信された位置が所定の誤差範囲内で前記衛星の前記予測位置と一致する場合には、前記受信された保護セッション鍵が真正であると判定するステップと、

をさらに含む、請求項 5 に記載の方法。

【請求項 7】

30

前記得られたセッション鍵が、現在のセッションに後続する次のセッションに使用するための次のセッション鍵であり、当該方法が、

前記データストリームを通じて、前記現在のセッションに使用するための現在の保護セッション鍵、及び、前記現在のセッション鍵が有効である期間及び前記次のセッション鍵が有効である期間を規定する有効性情報を受信するステップと、

前記衛星の公開鍵及び前記デバイスの秘密鍵に基づいて、前記デバイスにおいて前記現在の保護セッション鍵から前記現在のセッション鍵を得るステップと、

前記データストリームを通じて保護データが送信された時刻に関する情報を得るステップと、

前記得られた情報が、前記現在のセッション鍵が有効である前記期間の間に前記保護データが送信されたことを示す場合、前記現在のセッション鍵に基づいて前記保護データにアクセスするか、又は、前記得られた情報が、前記次のセッション鍵が有効である前記期間の間に前記保護データが送信されたことを示す場合、前記次のセッション鍵に基づいて前記保護データにアクセスするステップと、

40

をさらに含む、請求項 5 又は 6 に記載の方法。

【請求項 8】

コンピュータプログラムを格納するように構成されているコンピュータ可読記憶媒体であって、前記コンピュータプログラムは、衛星によって実行されると、前記衛星に、請求項 1～4 のいずれか一項に記載の方法を実施させる、コンピュータ可読記憶媒体。

【請求項 9】

50

コンピュータプログラムを格納するように構成されているコンピュータ可読記憶媒体であって、前記コンピュータプログラムは、衛星から信号を受信するように構成されているデバイスによって実行されると、前記デバイスに、請求項 5～7 のいずれか一項に記載の方法を実施させる、コンピュータ可読記憶媒体。

【請求項 10】

衛星であって、

セッション鍵を得るように構成されている鍵取得モジュールと、

前記衛星の秘密鍵、及び、保護されたセッション鍵が送信されるべきデバイスの公開鍵に基づいて、前記得られたセッション鍵を保護するように構成されている鍵保護モジュールと、

前記保護セッション鍵を前記デバイスに送信するように構成されている送信機であり、該送信機が、複数の所定部分を含むデータストリームを通じて、前記保護セッション鍵の所定数のバイトを前記複数の所定部分の各々に挿入することによって、前記保護セッション鍵を送信するように構成されている、送信機と、
を備える衛星。

【請求項 11】

前記衛星が、前記保護セッション鍵が以前に送信されているか否かを判定するためのリプレイ検出情報を生成するように構成されているリプレイ情報生成器をさらに備え、

前記送信機が、前記保護セッション鍵及び前記リプレイ検出情報を前記デバイスに送信するように構成されている、請求項 10 に記載の衛星。

【請求項 12】

衛星から信号を受信するためのデバイスであって、前記デバイスが、

前記衛星からデータストリームを受信するように構成されている受信機であり、前記データストリームは複数の所定部分を含む、受信機と、

前記複数の所定部分の各々から保護セッション鍵の所定数のバイトを抽出し、前記保護セッション鍵の前記抽出されたバイトを結合して、前記保護セッション鍵を取得し、前記デバイスの秘密鍵、及び、前記保護セッション鍵が受信された前記衛星の公開鍵に基づいて前記保護セッション鍵から前記セッション鍵を得るように構成されている鍵抽出モジュールと、
を備えるデバイス。

【発明の詳細な説明】

【発明の分野】

【0001】

本発明は、衛星システムにおける鍵配布に関する。特に、本発明は、公開鍵暗号化を使用することによって衛星システムにおいて鍵を配布することに関する。

【発明の背景】

【0002】

衛星は、広範な用途に使用されている。数例として、通信衛星は、テレビ放送、又は、電話、ビデオ若しくは無線通信のような他のサービスを提供することができ、地球観測衛星は、地表の詳細なリアルタイム画像化を可能にすることができ、全地球的航法衛星システム（GNSS）における測位衛星は、受信者の位置が三角法によって正確に計算されることを可能にすることができる。

【0003】

任意のタイプの衛星について、衛星と安全に通信することができることは特に重要である。許可されていない第三者が衛星からの送信を受信及び解読することを防止し、攻撃者が自身の制御信号を衛星に送信することによって衛星の制御を掌握することを防止するために、対称暗号化が使用されることが多い。対称暗号化方式は、同じセッション鍵が、衛星自体、制御局、及び、衛星からの送信を受信する必要がある任意のエンドユーザのような、衛星システム内の任意の許可されたデバイスに提供されることを必要とする。システム内の許可されたデバイスは、セッション鍵を用いてメッセージを暗号化し、暗号化メッ

セージを送信すること、並びに、同じセッション鍵を使用して受信された暗号化メッセージを解読及び／又は認証することによって、安全に通信することができる。

【0004】

許可されていないパーティがセッション鍵を得ることができたとすると、このシステムの安全性は損なわれることになる。この攻撃に対して防御するために、セッション鍵は定期的に失効され、新たなセッション鍵と交換される。従来のシステムにおいては、衛星システム内のデバイスに新たな鍵を配布するためには複雑な鍵管理インフラストラクチャが必要とされる。各デバイスは、ルート鍵暗号化鍵（KEK）を事前にロードされていなければならない、信頼できる第三者である鍵管理システムが、システム内のすべてのデバイスのルートKEKを格納する。鍵管理システムはその後、更新されたセッション鍵を各デバイスに、そのデバイスのルートKEKを使用して定期的に配布することができる。

10

【0005】

本発明は、この配布の文脈において行われる。

【発明の概要】

【0006】

本発明によれば、第1のデバイス及び第2のデバイスを備える衛星システムにおいてセッション鍵を送信する方法が提供され、第1のデバイス及び第2のデバイスのうちの一方が衛星であり、第1のデバイス及び第2のデバイスのうちの他方が、衛星に信号を送信し、及び／又は、衛星から信号を受信するように構成されているデバイスであり、方法が、第1のデバイスにおいてセッション鍵を得るステップと、第1のデバイスの秘密鍵及び第2のデバイスの公開鍵に基づいて、第1のデバイスにおいてセッション鍵を保護するステップと、保護セッション鍵を第1のデバイスから第2のデバイスに送信するステップと、を含む。

20

【0007】

保護セッション鍵を送信するステップが、保護セッション鍵、及び、保護セッション鍵が以前に送信されているか否かを判定するためのリプレイ検出情報を送信するステップを含むことができる。

【0008】

保護セッション鍵及びリプレイ検出情報が、鍵配布メッセージに含まれ得、又は、第2のデバイスが衛星であり、第1のデバイスが衛星にコマンドメッセージを送信するための制御局であるとき、リプレイ検出情報が、保護セッション鍵を含む鍵配布メッセージに結合されているコマンドメッセージに含まれ得る。コマンドメッセージが、CCSDS TCプロトコルにおいて定義されているものとしてのテレコマンド（TC）であることができる。

30

【0009】

第1のデバイスが衛星であることができ、第2のデバイスが衛星から信号を受信するように構成されているデバイスであることができ、方法が、衛星から第2のデバイスにデータストリームを送信するステップをさらに含むことができ、データストリームが複数の所定部分を含み、保護セッション鍵を送信するステップが、保護セッション鍵の所定バイト数を複数の所定部分の各々に挿入することによって、データストリームを通じて保護セッション鍵を送信するステップを含むことができる。データストリームが、宇宙データシステム諮問委員会（CCSDS）TMプロトコルにおいて定義されているものとしてのテレメトリ（TM）データストリームであることができる。

40

【0010】

得られたセッション鍵が、現在のセッションに後続する次のセッションに使用するための次のセッション鍵であることができ、方法が、現在のセッションに使用するための現在のセッション鍵を得るステップと、衛星の秘密鍵及び第2のデバイスの公開鍵に基づいて、衛星において現在のセッション鍵を保護するステップと、データストリームを通じて現在のセッション鍵を送信するステップと、データストリームを通じて有効性情報を送信するステップであって、有効性情報が、現在のセッション鍵が有効である期間及び次のセッ

50

セッション鍵が有効である期間を規定する、送信するステップとをさらに含むことができる。

【0011】

第1のデバイスが衛星であることができ、方法が、衛星において、1つ又は複数の所定の鍵失効規則に従って、送信されたセッション鍵をいつ失効させるかを決定するステップをさらに含むことができる。

【0012】

本発明によれば、第1のデバイス及び第2のデバイスを備える衛星システムにおいてセッション鍵を得る方法も提供され、第1のデバイス及び第2のデバイスのうちの一方が衛星であり、第1のデバイス及び第2のデバイスのうちの他方が、衛星に信号を送信し、及び／又は、衛星から信号を受信するように構成されているデバイスであり、方法が、第2のデバイスにおいて、第1のデバイスから保護セッション鍵を受信するステップと、第1のデバイスの公開鍵及び第2のデバイスの秘密鍵に基づいて、第2のデバイスにおいて、受信された保護セッション鍵からセッション鍵を得るステップとを含む。

10

【0013】

方法が、保護セッション鍵が送信されたときの第1のデバイスの予測位置に関する情報を得るステップと、保護セッション鍵がそこから受信された位置が所定の誤差範囲内で第1のデバイスの予測位置と一致する場合には、受信された保護セッション鍵が真正であると判定するステップとをさらに含むことができる。

【0014】

方法が、保護セッション鍵が以前に送信されているか否かを判定するためのリプレイ検出情報を受信するステップをさらに含むことができる。

20

【0015】

第1のデバイスから保護セッション鍵を受信するステップは、コマンドメッセージに結合されている鍵配布メッセージにおいて保護セッション鍵を受信するステップを含むことができ、コマンドメッセージにはリプレイ検出情報が含まれており、方法が、鍵配布メッセージに結合されているコマンドメッセージが以前に送信されていないことをリプレイ検出情報が示す場合には、保護セッション鍵が以前に送信されていないと判定するステップをさらに含むことができる。

【0016】

第1のデバイスが衛星であることができ、第2のデバイスが衛星から信号を受信するように構成されているデバイスであることができ、第1のデバイスから保護セッション鍵を受信するステップが、第2のデバイスにおいて衛星からデータストリームを受信するサブステップであって、データストリームは複数の所定部分を含む、受信するサブステップと、複数の所定部分の各々から保護セッション鍵の所定バイト数を抽出するサブステップと、保護セッション鍵の抽出されたバイトを結合して、保護セッション鍵を得るサブステップと、を含むことができる。

30

【0017】

得られたセッション鍵が、現在のセッションに後続する次のセッションに使用するための次のセッション鍵であることができ、方法が、データストリームを通じて、現在のセッションに使用するための現在の保護セッション鍵、及び、現在のセッション鍵が有効である期間及び次のセッション鍵が有効である期間を規定する有効性情報を受信するステップと、衛星の公開鍵及び第2のデバイスの秘密鍵に基づいて、第2のデバイスにおいて現在の保護セッション鍵から現在のセッション鍵を得るステップと、データストリームを通じて保護データが送信された時刻に関する情報を得るステップと、得られた情報が、現在のセッション鍵が有効である期間の間に保護データが送信されたことを示す場合、現在のセッション鍵に基づいて保護データにアクセスするか、又は、得られた情報が、次のセッション鍵が有効である期間の間に保護データが送信されたことを示す場合、次のセッション鍵に基づいて保護データにアクセスするステップとをさらに含むことができる。

40

【0018】

コンピュータ可読記憶媒体が、デバイスによって実行されると、デバイスに本方法を実

50

施させるコンピュータプログラムを格納するように構成され得る。

【0019】

本発明によれば、第1のデバイスも提供され、セッション鍵を得るように構成されている鍵取得モジュールと、第1のデバイスの秘密鍵、及び、保護されたセッション鍵が送信されるべき第2のデバイスの公開鍵に基づいて、得られたセッション鍵を保護するように構成されている鍵保護モジュールと、保護セッション鍵を第2のデバイスに送信するように構成されている送信機とを備え、第1のデバイス及び／又は第2のデバイスが衛星である。

【0020】

第1のデバイスが、保護セッション鍵が以前に送信されているか否かを判定するためのリプレイ検出情報を生成するように構成されているリプレイ情報生成器をさらに備えることができ、送信機が、保護セッション鍵及びリプレイ検出情報を第2のデバイスに送信するように構成され得る。

10

【0021】

第1のデバイスが、第2のデバイスにデータストリームを送信するように構成されている衛星であることができ、データストリームが複数の所定部分を含み、送信機が、保護セッション鍵の所定バイト数を複数の所定部分の各々に挿入することによって、データストリームを通じて保護セッション鍵を送信するように構成され得る。

【0022】

代替的に、第2のデバイスが衛星であることができ、第1のデバイスが、コマンドメッセージを衛星に送信するための制御局であることができ、送信機が、保護セッション鍵を含む鍵配布メッセージに結合されているコマンドメッセージにリプレイ検出情報を含めるように構成され得る。

20

【0023】

本発明によれば、第2のデバイスから信号を受信するための第1のデバイスも提供され、第1のデバイスが、第2のデバイスから保護セッション鍵を受信するように構成されている受信機と、第1のデバイスの秘密鍵、及び、保護セッション鍵がそこから受信される第2のデバイスの公開鍵に基づいて、保護セッション鍵からセッション鍵を得るように構成されている鍵抽出モジュールとを備える。

【0024】

ここで例示のみを目的として、添付の図面を参照して本発明の実施形態を説明する。

30

【図面の簡単な説明】

【0025】

【図1】本発明の一実施形態による、衛星と、衛星と通信するためのデバイスとを含むシステムを示す図である。

【図2】本発明の一実施形態による、図1のシステムにおいて対称鍵を提供する方法を示す図である。

【図3】本発明の一実施形態による、衛星システムにおいて対称鍵配布を管理する方法を示す図である。

【図4】本発明の一実施形態による、衛星システムにおいて対称鍵を失効させる方法を示す図である。

40

【図5】本発明の一実施形態による、衛星システムにおいて対称鍵を配布するための鍵配布メッセージを示す図である。

【図6】本発明の一実施形態による、宇宙データシステム諮問委員会（CCSDS）パケットテレコマンド規格に従って動作するシステムにおける鍵配布メッセージを示す図である。

【図7】本発明の一実施形態による、CCSDSテレメトリストリームを通じた鍵配布メッセージの送信を示す図である。

【図8】本発明の一実施形態による、衛星システムにおいて対称鍵を受信する方法を示す図である。

50

【図 9】本発明の一実施形態による、リプレイ検出情報を使用する方法を示す図である。

【図 10】本発明の一実施形態による、衛星システムにおいて対称鍵を送信するためのデバイスを示す図である。

【図 11】本発明の一実施形態による、衛星システムにおいて対称鍵を受信するためのデバイスを示す図である。

【図 12】本発明の一実施形態による、受信されたセッション鍵を認証する方法を示す図である。

【詳細な説明】

【0026】

ここで図 1 を参照すると、本発明の一実施形態による、衛星と、衛星と通信するためのデバイスとを含むシステムが示されている。システム 100 は、衛星システムとして参照され得る。本実施形態において、デバイス 101 は、信号の送信と受信の両方を行うように構成されている地上の制御局であり、それによって、制御局 101 は、衛星 102 に信号 103 を送信し、また、衛星 102 から信号 104 を受信することが可能である。しかしながら、別の実施形態において、デバイス 101 は、衛星に信号を送信するようにのみ構成されてもよく、又は、衛星から信号を受信するようにのみ構成されてもよい。たとえば、デバイス 101 は、衛星 102 からテレビ放送信号又は他のタイプの信号を受信するための受信専用アンテナであってもよく、又は、別の衛星であってもよい。本発明の実施形態は、限定ではないが、通信衛星、全地球的航法衛星システム（GNSS）に使用するための測位衛星、科学観測衛星、又は地球観測衛星を含む任意のタイプの衛星との通信に適用することができる。図 1 は、1 つの他のデバイスと通信する衛星を示しているが、本発明の実施形態は、任意の数のデバイス、たとえば、任意の数の衛星、地上局、受信アンテナなどを含むことができる。

【0027】

本実施形態のシステム 100 において、制御局 101 は、衛星 102 に制御信号 103 を送信し、衛星 102 から戻ってくるテレメトリ信号 104 を受信するように構成されている。制御局 101 によって送信することができる制御信号 103 の例は、衛星 102 の位置及び／又は向きに調整を行い、衛星 102 を新たな軌道に動かすためのテレコマンドを含む。テレメトリ信号 104 は、衛星 102 の現在の状態、たとえば、衛星構成、電力、又は熱監視データに関する情報を提供することができる。

【0028】

従来のシステムと同様に、アップリンクチャネル 103 及びダウンリンクチャネル 104 の両方での送信が、許可されていないユーザが衛星を制御するか、又は衛星からテレメトリデータを得ることを防止するために、セッション鍵を使用して暗号化される。セッション中、送信は、送信機及び受信機（複数可）に知られている現在のセッション鍵を使用して暗号化される。セッションの終わりに、現在のセッション鍵は失効され、その後の送信は、次のセッション鍵を使用して暗号化される。しかしながら、新たなセッション鍵が信頼できる第三者によって定期的に配布されることを必要とする従来のシステムとは対照的に、本実施形態において、更新されたセッション鍵の配布は、別個の鍵管理インフラストラクチャを必要とすることなく、デバイス 101 及び／又は衛星 102 によって、公開鍵暗号法を使用して処理することができる。

【0029】

公開鍵暗号法の基本原理は既知であり、ここでは詳細には説明しない。簡潔には、図 1 の衛星システム 100 内のデバイス 101 及び衛星 102 のような、衛星システム内の各デバイスに秘密鍵及び公開鍵が生成される。デバイス 101 及び衛星 102 は各々、それ自体の秘密鍵、及び、他方のデバイス 101、102 の公開鍵を格納するように構成されている。一般的に、衛星システム内の各デバイスの公開鍵は、衛星システム内の任意の他のデバイスにとって利用可能にされる。

【0030】

本発明の実施形態において、衛星システム内のデバイスは、デバイス自体の秘密鍵、及

10

20

30

40

50

び、意図されている受信者の公開鍵に基づいてセッション鍵を保護し、保護セッション鍵を送信することによってセッション鍵を配布することができる。セッション鍵に与えることができるタイプの保護の例は、公開鍵暗号化及び／又は認証を含む。公開鍵暗号化は、共有秘密を真正に導き出すのに使用することができ、パディングを用いる高度暗号化規格（AES）鍵ラップのようなアルゴリズムが、共有秘密を使用して、共有秘密に機密性及び完全性をもたらすことができる。

【0031】

暗号化は、セッション鍵又は他の暗号化データが許可されていない第三者に露出することを防止することによって、機密性をもたらす。認証は、送信が信頼できるソースから入来することの保証をもたらす。暗号化アルゴリズムの一例が、高度暗号化規格暗号ブロック連鎖（AES-CBC）アルゴリズムであり、暗号化認証アルゴリズムの一例が、高度暗号化規格の暗号に基づくメッセージ認証コード（AES-CMAC）アルゴリズムである。CBC-MACを用いる高度暗号化規格カウンタ（AES-CCM）アルゴリズムは、暗号化及び認証の両方を可能にする。暗号化又は認証のいずれか、又は、暗号化及び認証の両方を可能にする他のアルゴリズムも、当該技術分野において既知である。

【0032】

セッション鍵を解読又は暗号化するために、デバイスは、必要に応じて、それ自体の秘密鍵及び送信者又は受信者の公開鍵に基づいて共有秘密を導き出す。共有秘密はその後、セッション鍵を暗号化するか、又は、受信された暗号化セッション鍵を解読するのに使用することができる。共有秘密は、鍵暗号化鍵、すなわち、セッション鍵を暗号化するのに使用される鍵として参照され得る。共有秘密を導き出すための例示的なメカニズムは、楕円曲線ディフィーヘルマン（ECDH）法及び高性能安全ディフィーヘルマンプロトコル（HMQV）を含む。秘密鍵はデバイス間で共有されないため、暗号化セッション鍵は、その公開鍵がメッセージを暗号化するのに使用されたデバイス101、102のみによって解読することができる。

【0033】

セッション鍵を送信する制御局の例において、認証は暗号化とともに、又は、暗号化なしで使用され得る。認証は、衛星が、受信されたセッション鍵が信頼できるソースから入来していることを検証することを可能にする。別の例において、衛星は、認証とともに、又は、認証なしで暗号化を使用してセッション鍵を送信することができる。この例において、認証は、衛星からの信号のなりすましが困難であることに起因して、必要とされない場合がある。詳細には、衛星からの信号になりすますには、攻撃者は、衛星と同じ位置から信号を送信しなければならないことになり、目下実行不可能である。同時に、暗号化は、衛星から信号を受信する任意の許可されていない第三者によってセッション鍵が得られるのを防止する。

【0034】

公開鍵暗号法を使用して保護されている、受信されたセッション鍵を解読及び／又は認証するために、受信機は、いずれの公開鍵を解読／認証に使用すべきかを知っている必要があることが理解されよう。2つのデバイスのみを含む衛星システムにおいて、各デバイスは、他方のデバイスの公開鍵である1つの公開鍵だけ格納すればよい。そのようなシステムにおいて、各デバイスは、任意の受信されたメッセージがシステム内の唯一の他のデバイスから入来していると仮定し、格納されている他方のデバイスの公開鍵を使用して、任意の受信されたメッセージを解読することができる。しかしながら、3つ以上のデバイスを含む衛星システムにおいて、各デバイスは、複数の公開鍵、詳細には、システム内の他のデバイス毎に1つの公開鍵を格納し得る。そのような実施形態において、デバイスが公開鍵暗号法を使用してメッセージ、たとえば、鍵配布メッセージを送信するとき、デバイスは、送信がそこに由来する発信元デバイスを識別するための識別子も送信することができる。その後、メッセージを受信する、システム内の任意のデバイスが、含まれている識別子に基づいて発信元デバイスを識別し、メッセージ内に含まれるセッション鍵を解読及び／又は認証するために、識別されたデバイスに対応する公開鍵を選択することができ

る。受信デバイスが、発信元デバイスの公開鍵を使用する必要なしに識別子を得ることができるように、識別子は、公開鍵保護なしで送信されるべきである。

【0035】

代替形態として、セッション鍵は、識別子なしで送信されてもよい。この場合、受信機は、システム内の可能性のある送信機の各々と関連付けられるセキュリティ属性の各セットを用いて鍵配布メッセージを解読及び／又は認証するよう試行することによって、トライアルアンドエラーによって適切な公開鍵を識別し、解読及び／又は認証に成功したものを処理し得る。代替的に、デバイスは、送信機の物理的位置、又は、それを通じてメッセージが受信された特定のアンテナのような、何らかの他の既知のパラメータに基づいてセキュリティ属性の適切なセットを選択してもよい。

10

【0036】

本実施形態において、デバイス101及び衛星102のいずれか一方が、衛星システム100におけるセッション鍵配布の役割を担い得る。詳細には、デバイス101、102のうちの一方が、上述したように公開鍵暗号化を使用して新たなセッション鍵を暗号化し、暗号化セッション鍵を他方のデバイス101、102に送信することができる。このように、両方のデバイス101、102が同じセッション鍵を得ることができ、その後、公開鍵暗号化よりも効率的である対称鍵暗号化を使用して通信することができる。同時に、セッション鍵を送信するために公開鍵暗号化を使用することによって、許可されていない第三者がセッション鍵を得ることが防止される。

【0037】

20

ここで、「セッション」という用語は、対称鍵暗号化のための同じセッション鍵を使用してデバイス間で1つ又は複数の通信が交換される規定の期間を指す。現在のセッション中に使用中のセッション鍵は「現在のセッション鍵」として参照され得、後続のセッションに使用するためのセッション鍵は「次のセッション鍵」として参照され得る。

【0038】

任意の所与のセッションの持続時間はシステムアーキテクチャによって事前に規定することができ、時間又は任意の他の適切な変数に関連して規定される期間とすることができる。たとえば、一実施形態において、現在のセッション鍵は、所定数のテレコマンドが送信された後に失効し、次のセッション鍵と交換され得る。この場合、各セッションは、所定数のテレコマンドが送信される期間として規定することができる。別の実施形態において、各セッションは、所定の期間、たとえば、1日、1週間、又は1ヶ月とすることができる。各所定の期間の終わりに、セッションは終了し、現在のセッション鍵は失効され、次のセッションにおいてデバイスは、次のセッション鍵を使用して通信する。セッションが規定され得る方法の他の例は、送信されるデータが所定の制限、たとえば、250メガバイト(MB)、又は、衛星の所定数のオーバーヘッドパスに達することを含む。さらなる例として、1人又は複数のユーザ又はユーザグループに画像を送信する地球観測衛星の場合、各セッションは、所定数の画像にわたって継続することができる。セッションにおいて所定数の画像が送信された後、現在のセッション鍵は失効され、次のセッションが開始し、デバイスは、次のセッション鍵を使用して通信する。

30

【0039】

40

衛星システム内のデバイスは各々、上述した規則のような、その特定のシステム内でのセッションの持続時間を規定する1つ又は複数の所定の規則を与えられ得、いつ各セッションが終了し、次のセッションが開始するかを各デバイスが独立して決定することを可能にする。代替的に、いつ1つのセッションが終了し、次のセッションが開始するかを1つのデバイスが決定してもよく、このデバイスは、各セッションの終わりをシステム内の他のデバイスに信号伝達することができ、それによって、他のデバイスは、いつ現在のセッション鍵を失効させて、通信における次のセッション鍵の使用を開始すべきかを知る。

【0040】

ここで、図1のシステムにおいてセッション鍵を配布する方法を、図2を参照してより詳細に説明する。セッション鍵を送信する役割を担うデバイスが以降、第1のデバイスと

50

して参照され、セッション鍵を受信するデバイスを第2のデバイスとして参照される。たとえば、図1のシステムにおいて、衛星102及び制御局101のいずれか一方が第1のデバイスになり得、衛星102及び制御局101の他方が第2のデバイスになる。一般的に、本方法は、衛星システム内の任意の他のデバイスにセッション鍵を提供するために、衛星システム内の任意のデバイスが使用することができる。たとえば、デバイスが衛星から信号を受信することが可能である場合には、衛星が、そのデバイスにセッション鍵を提供するために本方法を使用することができ、又は、デバイスが衛星に信号を送信することが可能である場合には、デバイスが、衛星にセッション鍵を提供するために本方法を使用することができる。

【0041】

10

第1のステップS201において、送信されるべきセッション鍵が得られる。ここで、セッション鍵は、第1のデバイスによって生成することができ、又は、鍵生成器として参照され得る別個のソースから第1のデバイスによって得ることができる。本実施形態において、セッション鍵は、セッション鍵を配布するのに使用されることになる同じデバイス、すなわち、第1のデバイスによって生成される。

【0042】

セッション鍵が得られた後、ステップS202において、第1のデバイスは、それ自体の秘密鍵、及び、第2のデバイスの公開鍵、すなわち、セッション鍵が送信されるべきデバイスの公開鍵に基づいてセッション鍵を保護する。セッション鍵を保護するために、第1のデバイスは公開鍵暗号化及び／又は認証を使用することができる。その後、ステップS203において、第1のデバイスは、セッション鍵を保護するときにその公開鍵が使用されたデバイスである第2のデバイスに保護セッション鍵を送信する。暗号化が使用されるとき、暗号化セッション鍵はシステム内の複数のデバイスにブロードキャストされ得るが、第2のデバイスの秘密鍵を使用することによってのみ、解読することができる。それゆえ、たとえシステム内の他のデバイスが暗号化セッション鍵を受信しても、受信された信号を解読してセッション鍵を得ることは、第2のデバイスにしかできない。認証が使用されるとき、第1のデバイスの公開鍵を使用した認証が成功すると、第2のデバイスのみが受信されたセッション鍵を受理することができる。

20

【0043】

ここで図3を参照すると、本発明の一実施形態による、衛星システムにおいて鍵配布を管理する方法が示されている。図2と同様に、セッション鍵を得て配布する役割を担うデバイスが第1のデバイスとして参照され得、セッション鍵を受信する衛星システム内の任意のデバイスが第2のデバイスとして参照され得る。本実施形態において、第1のデバイスは図1の制御局101であり、第2のデバイスは図1の衛星102である。しかしながら、一般的に、本発明の実施形態において、衛星システムにおけるセッション鍵配布を管理する作業は、システム内の他のデバイスにデータを送信することが可能である、システム内の任意のデバイス、たとえば、衛星又は制御局のような地上施設に割り当てることができる。

30

【0044】

最初に、ステップS301において、制御局及び衛星は、現在のセッションにわたって有効であるセッション鍵である、現在のセッション鍵を使用して通信する。現在のセッション鍵は、図2に示す方法のような方法、又は異なる方法を使用して以前に配布された鍵であり得る。たとえば、衛星及び制御局は、衛星が打ち上げられる前に、衛星システムの設定中に1つ又は複数の初期セッション鍵を事前にロードされ得る。しかしながら、本発明の実施形態において、衛星が軌道に乗るとセッション鍵は安全に配布することができるため、事前ロードは必須ではない。上述したように、制御局は、現在のセッション鍵を使用してデータを暗号化し、暗号化データを衛星に送信することによって衛星と通信することができ、衛星はその後、同じ現在のセッション鍵を使用して暗号化データを解読することができる。同様に、衛星は、現在のセッション鍵を使用して暗号化されたデータを送信することによって制御局と通信することができる。

40

50

【0045】

本実施形態において、デバイスはステップS301において現在のセッション鍵を使用して通信するが、状況によっては、デバイスは最初に、現在のセッション鍵を知らない可能性がある。たとえば、デバイスが一定期間にわたって非アクティブであった後に電源投入されるとき、デバイスは、現在のセッション鍵を用いて更新されていない場合がある。同様に、システム内に新たなデバイスが追加されるとき、たとえば、新たなユーザが衛星サービスを受信するために加入したとき、デバイスは、現在のセッション鍵を知らないことになる。この問題に対処するために、本発明のいくつかの実施形態において、鍵配布の役割を担うデバイスが、現在のセッション鍵及び次のセッション鍵の両方を含む鍵配布メッセージを定期的に送信することができる。これによって、現在のセッション鍵の予備知識がないデバイスが、次のセッションを開始するのを待つ必要なく現在のセッションの間に通信を受信することが可能になることが保証される。

10

【0046】

次に、ステップS302において、制御局が、次のセッションにおいて有効になる次のセッション鍵である、第2のセッション鍵を得る。図2のステップS201と同様に、次のセッション鍵は、制御局によって生成することができる、又は、たとえば別のソース、たとえば、第三者の鍵提供者から得ることができる。本実施形態では、ステップS302において、次のセッション鍵が制御局から生成される。次のセッション鍵は、いつでも制御局から得ることができる。

20

【0047】

次のセッション鍵が得られた後、ステップS303において、制御局は、制御局の秘密鍵、及び、次のセッション鍵が送信されることになるデバイス、この場合は衛星の公開鍵を使用して次のセッション鍵を保護する。本実施形態において、制御局は、鍵暗号化アルゴリズムと併せて公開／秘密鍵確立メカニズムを使用して、機密性、完全性、及び信頼性の保護をセッション鍵に与える。他の実施形態において、鍵確立メカニズムは、別個の鍵暗号化アルゴリズムを使用することなく、セッション鍵の直接の保護を与えることができる。次に、ステップS304において、次の保護セッション鍵が衛星に送信される。ステップS303及びS304は、図2の方法のステップS202及びS203と同様に実施することができる。

30

【0048】

ステップS304において次の保護セッション鍵が衛星に送信された後の任意の時点において、ステップS305において現在のセッション鍵が失効され得る。ここで、「失効」とは、現在のセッション鍵がもはや、第1のデバイスと第2のデバイスとの間の通信に使用することができないことを意味する。たとえば、失効したセッション鍵は、メモリから消去することができるか、又は、保持されるが、将来その鍵が使用されることを防止するために「失効」としてフラグ付けされ得る。上述したように、デバイスは、いつ1つのセッションが終了し、別のセッションを開始するかを規定する所定の規則に従って、いつセッション鍵を失効させるべきかを決定することができる。現在のセッション鍵は現在のセッションの終わりに失効され、次のセッションが開始すると次のセッション鍵が使用される。次のセッションは、現在のセッションが終了した直後に開始してもよく、又は、現在のセッションが終了した後の何らかの時点において開始してもよい。

40

【0049】

現在のセッション鍵は失効されているが、この時点で両方のデバイスが、ステップS304において以前に送信された次のセッション鍵を有している。それゆえ、ステップS306において、第1のデバイス及び第2のデバイスは、次のセッション鍵を使用して通信を暗号化することによって、次のセッションにおいて通信し続けることができる。それゆえ、衛星システム内のデバイスは、図3の方法を使用して、第三者の鍵管理インフラストラクチャを必要とすることなく、安全な方法で新たなセッション鍵を定期的に配布することができる。暗号化に使用されるセッション鍵を定期的に変更することによって、同じ鍵によって暗号化されるデータの量が制御され、攻撃者が総当たり攻撃に使用するのに所

50

与の時間内で利用可能なデータの量が低減するため、さらなる安全性がもたらされる。

【0050】

図3の方法は上記において、制御局と衛星との間の通信に関連して説明されているが、他の実施形態では、方法は、衛星システム内の任意のデバイスによって使用されてもよい。

【0051】

鍵失効は、必ずしも新たなセッション鍵を配布する役割を担う同じデバイスである必要がない、衛星システム内の任意のデバイスによって処理することができる。本実施形態では、鍵失効は衛星によって処理され、鍵配布は制御局によって処理される。鍵失効の役割を衛星が担うようにすることによって、衛星が、衛星へのセキュリティアクセスを強化することが可能になる。ここで、衛星システムにおいてセッション鍵を失効させる方法を、図4を参照して説明する。

【0052】

最初にステップS401において、デバイスが、衛星システム内の通信を暗号化するために現在のセッション鍵の使用を開始する。たとえば、デバイスは、図3を参照して上述したように、以前のセッション鍵が失効した後に現在のセッション鍵の使用を開始することができる。

【0053】

現在のセッション鍵が使用されている間、デバイスは、所定の規則に基づいて新たなセッションを開始すべきか否かを繰り返しチェックすることができる。本実施形態において、所定の規則は、複数の使用状況指標に対する所定の制限を規定し、所定の制限のいずれかに達したか、又は超えた場合に、デバイスは、現在のセッション鍵が失効され、新たなセッションが開始されるべきであると判定する。たとえば、デバイスは、定期的にチェックを実施することができ、及び／又は、現在のセッション鍵を使用して暗号化データが送信又は受信される度毎にチェックを実施することができる。本実施形態において、使用状況指標は、現時点までに現在のセッション鍵を用いて暗号化されたデータの量、及び、現在のセッション鍵が使用された合計期間を含むが、異なる使用状況指標が使用されてもよい。他の実施形態において、異なる所定の規則又は複数の規則が使用されてもよい。

【0054】

詳細には、ステップS402において、デバイスは、現在のセッション鍵を使用して送受信されたデータの総量が所定のデータ制限に達したか又は超えたか否かチェックし、そうでない場合、ステップS403において、デバイスは、現在のセッション鍵が所定の期間にわたって使用されたか否かをチェックする。両方のチェックの結果が否である場合、デバイスはステップS401に戻り、現在のセッション鍵を使用し続ける。一方、いずれかのチェックの結果が是である場合、デバイスは、ステップS404において現在のセッション鍵を失効させる。

【0055】

現在のセッション鍵を使用して暗号化された総データ量は、デバイスによって受信されたデータ及びデバイスによって送信されたデータを含むことができる。一例として、デバイスが、テレコマンドとして参照される場合もあるコマンドメッセージを衛星に送信するように構成されている制御局であるとき、現在のセッション鍵を使用して暗号化されたコマンドメッセージの総量が、総データ量として記録され得る。別の例として、デバイスが、データストリームを通じて地球観測データを地上のユーザに送信するように構成されている地球観測衛星であるとき、総データ量は、現在のセッション鍵を使用してデータストリームを通じて送信されているデータの総量であり得る。

【0056】

たとえば、総当たり手法を使用して暗号化を破る第三者によってセッション鍵が損なわれる危険性は、現在のセッション鍵を使用してより多くのデータが暗号化及び送信されるとき、並びに、現在のセッション鍵がより長い期間にわたって使用されるときに増大するおそれがある。それゆえ、図4に示すもののような方法は、セキュリティ違反の危険性が

10

20

30

40

50

高くなりすぎる前に、現在のセッション鍵が失効され、新たなセッション鍵と交換されることを保証することができる。

【0057】

ここで図5を参照すると、本発明の一実施形態による、衛星システムにおいてセッション鍵を配布するための鍵配布メッセージが示されている。鍵配布メッセージ500は、鍵データ部分501と、完全性部分502とを含む。他の実施形態において、完全性部分502は省かれてもよい。鍵データ部分501は、ユーザ識別子(ID)503と、短期データ504と、保護鍵データ505とを含む。短期データ504は、使用される暗号アルゴリズムに応じて変わり、共有秘密を導き出すのに使用するための短期鍵を含み得る。

【0058】

本実施形態において、保護鍵データ505は、送信されているセッション鍵に関するセキュリティ属性506、及び、セッション鍵自体507を保持する。他の実施形態において、セキュリティ情報506は省かれてもよく、暗号化鍵データ505は、暗号化鍵507のみを含んでもよい。セキュリティ属性は、暗号化又は解読のようなセキュリティ機能又はサービスを有効にするために使用することができる。鍵配布メッセージ500において送信することができるセキュリティ属性の例は、次のセッション鍵、完全性検証情報、鍵が有効である期間を規定するための鍵有効性情報、及び、鍵が以前に使用されていなかったことを保証するためのリプレイ検出情報を含む。セキュリティ属性は、ユーザの役割と関連付けられる権限、及び、異なるユーザの公開鍵とともに格納することができる異なるユーザのアクセス権限のような、他の情報も含むことができる。これらの情報は、たとえば、衛星に命令すること、衛星上の暗号モジュールを制御すること、他のユーザの公開鍵をアップロード又は消去することなどを許可されているユーザを識別するために使用することができる。

【0059】

本実施形態において、受信デバイスは、衛星システム内の複数の他のデバイスの公開鍵を格納する。受信デバイス、たとえば、図1の衛星又は制御局は、受信されたデータから鍵配布メッセージ500を得て、ユーザ識別子503に基づいて鍵配布メッセージ500の発信元を識別し、暗号化鍵データ505を解読するために、ユーザと関連付けられる共有秘密を導き出す。このように、デバイスは、共有秘密を使用してセキュリティ属性506及びセッション鍵507を得ることができる。非対称暗号化が使用されるため、鍵配布メッセージ500が意図されているデバイスのみがセキュリティ属性506及びセッション鍵507を得ることが可能である。共有秘密を導き出すための例示的なメカニズムは、ECDH及びHMQVを含む。セキュリティ属性は、たとえば、パディングを用いる高度暗号化規格(AES)鍵ラップを使用することによって得ることができる。

【0060】

衛星システムにおけるセッション鍵配布の役割を担うデバイスは、衛星システム内の複数の異なるデバイスの別個のセキュリティ属性を格納することができる。他の各デバイスに対して格納することができるセキュリティ属性の例は、他のデバイスのユーザID、他のデバイスの公開鍵、リプレイ検出情報、他のデバイスによって現在使用されているセッション鍵、及び、現在のセッション鍵が有効である期間を規定する鍵有効性情報を含む。

【0061】

リプレイ検出情報は、鍵配布メッセージ500を受信するデバイスによって、同じ鍵配布メッセージ500が以前に送信されているか否かを判定するために使用することができる。この情報は、受信されたメッセージが、攻撃者によってたとえば、受信デバイスをだまして誤ったセッション鍵を使用させるために再生されているものであることの指標となり得る。メッセージが再生されている場合、これは、鍵配布メッセージ500に含まれる暗号化セッション鍵507が以前に送信されていることを意味する。鍵配布メッセージがいつ再生されたかを検出するために、新たなセッション鍵を配布する役割を担うデバイスは、鍵配布メッセージが送信される度毎に、固有のリプレイ検出情報をメッセージ内に含めることができる。

【0062】

リプレイ検出情報は、予測可能な様式で1つのメッセージから次のメッセージへと変化する。リプレイ検出情報の一例が、カウンタ、すなわち、鍵配布メッセージの所定の位置に含まれる数値である。カウンタの値は、1つの鍵配布メッセージから次の鍵配布メッセージへと増分される。たとえば、システムが始動された後に送信される第1のメッセージはカウンタ値1を含むことができ、第2のメッセージはカウンタ値2を含むことができ、第3のメッセージはカウンタ値3を含むことができ、以下同様である。リプレイ検出情報の一例に過ぎず、別の例として、送信者及び受信者の両方に知られているアルゴリズムによって得られる擬似乱数（PRN）が挙げられ得ることが理解されよう。リプレイ検出情報の使用は、図9を参照してより詳細に後述する。

10

【0063】

鍵配布メッセージの1つの例示的な構造が図5に示されているが、本発明はこの特定の構造には限定されず、本発明の他の実施形態において、異なるメッセージ構造が鍵配布メッセージに使用されてもよいことが理解されよう。たとえば、特定の通信規格との互換性が必要とされる場合、本発明の実施形態は、その規格において規定されているメッセージ構造を、鍵配布メッセージとして構成してもよい。

【0064】

ここで図6を参照すると、本発明の一実施形態による、宇宙データシステム諮問委員会（CCSDS）規格に従って動作するシステムにおける鍵配布メッセージが示されている。本実施形態において、図5の鍵配布メッセージ500が、暗号化転写層テレコマンド600に追加され、CCSDS符号化層データ601として送信される。この送信手法は、たとえば、衛星を制御するためにテレコマンドを衛星に送信するように構成されている制御局によって使用することができる。同様の手法がまた、CCSDS以外のプロトコルに従って動作するシステムにおいて鍵配布メッセージを送信するのに使用することもでき、スタック内の異なる位置にある他のセキュリティ層に適用することができることが理解されよう。

20

【0065】

衛星が、テレコマンドメッセージ600に結合されている鍵配布メッセージ500を含む図6に示す送信を受信すると、衛星は、衛星と、送信がそこから受信された発信元デバイスとの間の送信に現在有効である現在のセッション鍵を使用して、テレコマンドメッセージ600を解読する。現在のセッション鍵は、以前に受信されており、テレコマンド600が受信された期間中に有効であるものとして使用でき、又は、受信されたテレコマンド600に追加されている鍵配布メッセージ500において規定されている新たなセッション鍵とすることができる。本発明の一実施形態において、制御局は、新たなセッションを開始するときに衛星に鍵配布メッセージを送信するようにのみ構成されている。この実施形態において、衛星は、以前のセッション鍵を失効させ、受信されたセッション鍵を現在のセッション鍵として使用することによって、鍵配布メッセージに応答するように構成されている。それゆえ、新たなセッションの開始は、鍵配布メッセージの存在によって伝達され、これは、各セッション鍵が有効である期間を規定する有効性情報をも送信する必要はないことを意味する。

30

40

【0066】

本実施形態において、リプレイ検出情報は、図5を参照して上述したように鍵配布メッセージ500に含まれている。衛星は、受信されたリプレイ検出情報をチェックして、鍵配布メッセージ500が真正であるか否かを判定することができる。

【0067】

鍵配布メッセージ500も、図6に示すようにテレコマンド600に結合され得る。これによって、衛星が、鍵配布メッセージ500も真正であると判定される場合に、テレコマンド600が真正であると判定することが可能になる。鍵配布メッセージ500及びテレコマンド600の信頼性が確認されると、テレコマンド600は、宇宙船内のその宛先機能、たとえば、宇宙船コンピュータ、観測機器、又は暗号コントローラに渡され得る。

50

【0068】

別の実施形態において、リプレイ検出情報は、鍵配布メッセージ500の代わりにテレコマンド600に含まれる。衛星は、リプレイ検出情報を使用して、テレコマンドが真正であるか否かを判定することができ、テレコマンドが真正であると判定される場合、鍵配布メッセージ及びその中に含まれる鍵も有効であると仮定される。

【0069】

鍵配布メッセージ500がテレコマンド600に結合されているとき、リプレイ検出情報は、鍵配布メッセージ500とテレコマンド600との間で共有することができる。それゆえ、鍵配布メッセージ500及びテレコマンド600の両方にリプレイ検出情報を含む必要はない。

10

【0070】

本実施形態が、テレコマンドメッセージを衛星に送信する制御局に関連して説明されているが、他の実施形態において、図6において使用されているものと同様の手法が、テレコマンドであり得るか又は任意の他のタイプのメッセージであり得る別のメッセージに結合されている鍵配布メッセージを送信することによって、衛星システムにおける任意の2つのデバイスの間の通信に適用され得る。

【0071】

ここで図7を参照すると、本発明の一実施形態による、CCSDSテレメトリストリームを通じた鍵配布メッセージの送信が示されている。衛星からのCCSDSテレメトリストリームが、衛星の状態を監視するために、たとえば、制御局のような地上施設によって受信され得る。本実施形態はCCSDSテレメトリストリームに関連して説明されているが、本発明はCCSDS規格には限定されず、実施形態は、任意のタイプのデータストリームを通じてセッション鍵を配布するのに使用することができることが理解されよう。

20

【0072】

図7に示すように、CCSDSテレメトリデータストリーム710は、各々が転送フレーム一次ヘッダ及び転送フレームデータを含む、複数の転送フレームに分割される。転送フレームデータは、本実施形態においてはテレメトリデータであるが、一般的には任意のタイプのデータであってもよい、データストリームを通じて送信されているデータのバイトを保持する。転送フレーム一次ヘッダは、CCSDS規格において規定される標準的な転送フレームヘッダである。

30

【0073】

加えて、本実施形態において、各転送フレームは、鍵配布ストリームを1つ又は複数の受信機に提供するのに使用される転送フレーム二次ヘッダ711を含む。特に、各転送フレーム二次ヘッダ711は、ヘッダID712と、タイムスタンプ(TS)713と、鍵配布ストリーム715の所定バイト数を保持する鍵配信部分714とを含む。このように、鍵配布ストリーム715は、部分整流されて、テレメトリストリーム710になる。テレメトリデータストリーム710を受信するデバイスは、各フレームの転送フレーム二次ヘッダ711から鍵配信バイト714を抽出し、抽出されたバイトを組み合わせることによって、鍵配布ストリーム715を再構築することができる。

40

【0074】

鍵配信バイト714及び転送フレームデータは、関連するパーティの公開／秘密鍵を使用して保護され、受信者は、TS713を使用して、転送フレームデータを解読及び／又は認証するためにいずれのセッション鍵を使用すべきかを識別することができる。詳細には、TS713は、衛星がその転送フレームを送信した時刻を示し、それゆえ、転送フレーム内のデータを保護するために衛星がいずれのセッション鍵を使用したかを判定する。

【0075】

たとえば、衛星は、ユーザA向けの鍵配布メッセージ及びユーザB向けの鍵配布メッセージを含むテレメトリストリームを送信し得る。各鍵配布メッセージは、下記に示すように、現在のセッション鍵及び次のセッション鍵、並びに、各鍵が有効である期間を規定する有効性情報を含む。

50

ユーザ A 鍵配布メッセージ：

鍵 1、ユーザ A 向けに暗号化、12:00～14:59 の間有効

鍵 2、ユーザ A 向けに暗号化、15:00～17:59 の間有効

ユーザ B 鍵配布メッセージ：

鍵 1、ユーザ B 向けに暗号化、12:00～14:59 の間有効

鍵 2、ユーザ B 向けに暗号化、15:00～17:59 の間有効

【0076】

有効期間は、衛星の内部クロックを参照して規定される。たとえば、受信者の内部クロックが 14:59 の時刻を示すときに 15:00 のタイムスタンプを有する転送フレームが受信された場合、受信者は、たとえ受信者の内部クロックが、現在のセッション鍵が実

10

際には鍵 1 であることを示すように見えるとしても、受信されたタイムスタンプに基づいて鍵 2 が現在のセッション鍵であると判定する。

【0077】

上記の例において、ユーザ A がタイムスタンプ「12:20」を含む転送フレームを受信した場合、受信者は、現在のセッション鍵が、12:00～14:59 の間有効な鍵 1 であると判定することができる。それゆえ、受信者は、鍵 1 を使用して、現在の転送フレーム内の鍵配信バイト及び転送フレームデータを解読及び／又は認証する。しかしながら、ユーザ A が後にタイムスタンプ「15:00」を含む転送フレームを受信すると、受信者は、この時点では鍵 2 が現在のセッション鍵であると判定し、したがって、鍵 2 を使用して鍵配信バイト及び転送フレームデータを解読及び／又は認証する。

20

【0078】

また、タイムスタンプが 14:59 から 15:00 へと回るとき、又はその後、鍵配布メッセージの内容は、以下のように、新たな「現在の」及び「次の」セッション鍵を反映するように変化する。

ユーザ A 鍵配布メッセージ：

鍵 2、ユーザ A 向けに暗号化、15:00～17:59 の間有効

鍵 3、ユーザ A 向けに暗号化、18:00～20:59 の間有効

ユーザ B 鍵配布メッセージ：

鍵 2、ユーザ B 向けに暗号化、15:00～17:59 の間有効

鍵 3、ユーザ B 向けに暗号化、18:00～20:59 の間有効

30

【0079】

本実施形態において、タイムスタンプ及び有効期間は時間及び分単位で規定されているが、他の実施形態において、タイムスタンプ及び有効期間は、たとえば、任意のカウンタを使用して規定されてもよい。

【0080】

また、本実施形態において、受信者は、転送フレーム内のタイムスタンプを使用して、その転送フレームにいずれのセッション鍵を使用すべきかを決定するが、他の実施形態において、タイムスタンプは省かれてもよい。たとえば、受信者は、たとえば、全地球測位システム（GPS）の測位を得るときに計算される時間のずれから、受信者の内部クロックと衛星の内部クロックとの間のズレに関する情報を得ることができる。受信者はその後、転送フレームが受信されたローカル時間、受信者クロックと衛星クロックとの間のずれ、及び、信号の推定移動時間を使用して、衛星のクロックによる、転送フレームが送信された時刻を推定することができる。

40

【0081】

図 7 に示すように、鍵配布ストリーム 715 は、複数のユーザグループ向けの鍵配布メッセージ 700 を含む。各ユーザグループは、単一のユーザを表してもよく、又は、同じセッション鍵を共有し、したがって、同じデータにアクセスすることができる複数のユーザを含んでもよい。各鍵配布メッセージ 700 は、たとえば、図 5 に示すようにフォーマット化することができる。図 7 に示すストリーム 710 のようなデータストリームにおいて、異なるユーザ向けに意図されているデータは、異なる対称鍵を使用して暗号化され、

50

データストリームを通じて送信され得る。複数の異なるユーザグループ向けに別個の鍵配布メッセージを提供することによって、各ユーザグループは、1つのグループからのユーザが別のユーザグループ向けに意図されているデータにアクセスすることを防止しながら、それ自体のデータを解読するためにそれ自体の対称鍵を供給され得る。各ユーザグループの鍵は、定期的に失効され、更新された鍵と交換され得る。

【0082】

図7に示す手法は、複数の地上ターミナルのための帯域幅効率的な鍵配信メカニズムを提供し、CCSDSパケットテレメトリ規格のような既存のプロトコルを使用して実施することができる。詳細には、各ダウンリンクフレームにおいて鍵配布ストリームの少数のバイトしか渡されないため、テレメトリデータストリーム内の帯域幅が節約される。本実施形態はそれゆえ、本実施形態においてはテレメトリデータである主要な転送ストリームデータにとって利用可能な帯域幅に何ら大きな影響を与えることなく、1人又は複数のエンドユーザにセッション鍵を供給することができる。本手法は、受信専用機能を有する衛星システム内のターミナルに鍵を配布するのに使用することができ、そのため、それらのターミナルが使用するためにそれらのターミナルが鍵をアップロードすることができるメカニズムを有しない。たとえば、地球観測衛星は、図7に示す手法を使用して、データストリームを通じて、許可されたユーザによって操作される複数の地上の受信機にセッション鍵を配布することができる。

10

【0083】

一例として、ダウンリンクが16キロビット(Kbits)のフレームで150メガビット毎秒(Mbps)で動作している一般的な地球観測システムにおいて、タイムスタンプは5日ごとにラップすることになる。各鍵が1024ビットサイズであり、500のエンドユーザがあるとすると、各ユーザが自身の現在の鍵及び次の鍵を受信するには3秒超しかかからないことになる。別の例において、ダウンリンクが4Kbitsのフレームサイズで64キロビット毎秒(Kbps)で動作している一般的なテレメトリ追跡及びコマンド(TTC)通信システムにおいて、タイムスタンプは8.5年ごとにラップすることになり、3人のエンドユーザでは、ユーザが自身の現在の鍵及び次の鍵を受信するには約12秒かかることになる。

20

【0084】

本実施形態では、複数のフレームを含むCCSDSテレメトリストリームを通じて配布されるが、他の実施形態では、セッション鍵は、たとえば、その実施形態のために選択される特定の規格によるフレーム又はパケットとして参照され得る複数の所定部分に分割される任意のデータストリームを通じて配布されてもよい。鍵配布メッセージの所定バイト数をデータストリームの各部分に含めることによって、鍵配布メッセージは、部分整流を使用してデータストリームに含まれ得る。

30

【0085】

ここで図8を参照すると、本発明の一実施形態による、衛星システムにおいてセッション鍵を受信する方法が示されている。方法は、限定ではないが、衛星又は他の宇宙船、制御局、及びエンドユーザ受信機(たとえば、テレビ放送受信機)を含む、衛星システム内の任意のデバイスによって使用することができる。

40

【0086】

最初にステップS801において、保護セッション鍵が受信される。たとえば、セッション鍵は暗号化及び／又は認証を使用して保護することができる。セッション鍵は、図5に示すもののような鍵配布メッセージにおいて受信されてもよく、図6に示すようなテレコマンドに結合されて、又は、図7に示すようなテレメトリデータストリームを通じて受信されてもよい。

【0087】

次に、ステップS802において、保護セッション鍵が、受信者の秘密鍵及び送信者の公開鍵に基づいて認証及び／又は解読される。たとえば、共有秘密が、ECDH又はHMQVを使用して得られ、セッション鍵を解読するのに使用され得る。受信されたセッショ

50

ン鍵が解読及び／又は認証されると、セッション鍵は、衛星システム内の２つのデバイス間の後続の通信に使用することができる。

【００８８】

ここで図９を参照すると、本発明の一実施形態による、リプレイ検出情報を使用する方法が示されている。図８の方法と同様に、図９の方法は、衛星システム内の任意のデバイスによって使用することができる。

【００８９】

最初に、ステップＳ９０１において、リプレイ検出情報が、暗号化セッション鍵とともに受信される。本実施形態において、リプレイ検出情報は、図６に示すように暗号化セッション鍵に結合されているコマンドに含まれている。一方、別の実施形態において、リプレイ検出情報は、図５に示すように鍵配布メッセージ内に暗号化鍵とともに含まれていてもよい。リプレイ検出情報が受信されると、その後、ステップＳ９０２において、受信デバイスは、受信されたリプレイ検出情報の値を、以前に受信された値、すなわち、現在の鍵配布メッセージに先行する最後の成功したメッセージ内のリプレイ検出情報の値と比較する。

【００９０】

ステップＳ９０３において、所定条件が満たされているか否かがチェックされる。所定条件の一例は、リプレイ検出情報の現在の値が以前の値よりも大きいか否かであり得る。現在の値がより大きい場合、メッセージは再生されていないと仮定される。一方、現在の値が以前の値以下である場合、メッセージは再生済みである以前のメッセージであると判定される。代替的な条件は、リプレイ検出情報の受信された値が、既知のシーケンス内の次の値である、予測値と一致するか否かであり得る。所定条件のまた別の例は、現在の値が、以前の値よりも大きい、以前の値の特定の範囲内に入る許容可能値の所定の窓内に入るか否かであり得る。

【００９１】

所定条件が満たされる場合、ステップＳ９０４において、受信された鍵配布メッセージに結合されているコマンドメッセージが再生されておらず、それゆえ、鍵配布メッセージも再生されていないと判定される。したがって、受信された暗号化セッション鍵は真正であり、使用できると判定され、リプレイ検出情報の格納されている以前の値が現在の値と置き換えられる。他方、所定条件が満たされていない場合、ステップＳ９０５において、受信されたコマンドメッセージ及び結合されている暗号化セッション鍵が再生されており、使用すべきではないと判定される。

【００９２】

図９に示すようにリプレイ検出情報を使用することによって、メッセージが攻撃者によって、システムを危険に晒そうとする試みにおいていつ再生されたかを検出することによって、衛星システムのセキュリティを向上することができる。

【００９３】

ここで図１０を参照すると、本発明の一実施形態による、衛星システムにおいてセッション鍵を送信するためのデバイスが示されている。本実施形態において、デバイス１０００は衛星であるが、他の実施形態において、デバイス１０００は、図１に示す制御局のような地上施設であってもよい。

【００９４】

衛星１０００は、セッション鍵を得るように構成されている鍵取得モジュール１００１と、たとえば、暗号化及び／又は認証を適用することによって、衛星の秘密鍵、及び、セッション鍵が送信されるべきデバイスの公開鍵に基づいて、得られたセッション鍵を保護するように構成されている鍵保護モジュール１００２と、保護セッション鍵をデバイスに送信するように構成されている送信機モジュール１００３とを備える。また、本実施形態において、衛星１０００は、リプレイ検出情報を生成するためのリプレイ検出情報生成器１００４を含む。送信機モジュール１００３は、鍵保護モジュール１００２から保護セッション鍵を受信し、リプレイ検出情報生成器１００４からリプレイ検出情報を受信し、保

護セッション鍵及びリプレイ検出情報を、コマンドメッセージに結合されている鍵配布メッセージとして、又は、データストリームを通じて、衛星システム内の別のデバイスに送信する。リプレイ検出情報が必要とされない場合には、他の実施形態において、リプレイ検出情報生成器1004は省かれてもよい。

【0095】

ここで図11を参照すると、本発明の一実施形態による、衛星システムにおいてセッション鍵を受信するためのデバイスが示されている。本実施形態において、デバイス1100は衛星であるが、他の実施形態において、デバイス1100は、図1に示す制御局のような地上施設であってもよい。

【0096】

衛星1100は、衛星システム内の別のデバイスから保護セッション鍵を受信するように構成されている受信機モジュール1101を備える。たとえば、保護セッション鍵は、図6に示すようにテレコマンドに結合されている鍵配布メッセージとして受信されてもよく、又は、図7に示すようにテレメトリデータストリームを通じて受信されてもよい。衛星1100は、たとえば、衛星の秘密鍵、及び、セッション鍵がそこから受信されたデバイスの公開鍵に基づいて、保護セッション鍵を暗号化及び／又は認証することによって、受信されたメッセージからセッション鍵を抽出するように構成されている鍵抽出モジュール1103をさらに備える。加えて、本実施形態において、衛星1100は、受信機モジュール1101からリプレイ検出情報を受信するように構成されているリプレイ検出モジュール1102をさらに備え、リプレイ検出モジュール1102は、受信された鍵配布メッセージ又はテレコマンドからリプレイ検出情報を抽出することができる。リプレイ検出モジュール1102は、図9を参照して上述したように、受信されたリプレイ検出情報を、リプレイ検出情報の予測値と比較する。図9のステップS903を参照して上述したように、受信されたリプレイ検出情報が所定条件を満たす場合、リプレイ検出モジュール1102は鍵抽出モジュール1103に、受信されたセッション鍵が真正であり、必要に応じてデバイス1100内の他の機能に安全に渡すことができることを伝達する。他の実施形態において、リプレイ検出が必要とされない場合には、リプレイ検出モジュール1102は省かれてもよい。

【0097】

ここで図12を参照すると、本発明の一実施形態による、受信されたセッション鍵を認証する方法が示されている。図12の方法は、受信されたセッション鍵が暗号化を使用して保護されているだけである実施形態に使用するのに特に適している。最初にステップS1201において、保護セッション鍵が受信される。次に、ステップS1202において、保護セッション鍵が送信された時点における送信機の予測位置に関する情報が得られる。ステップS1203において、予測位置が、たとえば、指向性アンテナによって検出されるものとしての、セッション鍵がそこから受信された検出位置と比較される。保護セッション鍵が静止軌道内の衛星から受信されるとき、予測位置は、衛星の既知の位置であり得る。他方、非静止軌道内の衛星について、予測位置は、衛星の軌道、保護セッション鍵が受信された時刻、及び、衛星から受信者への信号の推定移動時間に関する情報に基づいて求めることができる。保護セッション鍵が静止送信者、たとえば、地上の制御局から受信されるとき、予測位置は、送信者の既知の位置であり得る。

【0098】

その後、ステップS1204において、検出位置が、所定の誤差範囲内で予測位置と一致するか否かがチェックされる。検出位置が予測位置と一致する場合、ステップS1205において、受信されたセッション鍵が真正であり、受理することができると仮定される。他方、検出位置が予測位置と一致しない場合、ステップS1206において、受信されたセッション鍵は廃棄される。

【0099】

衛星システムにおけるセッション鍵配布が衛星システム内のデバイス、たとえば、衛星又は制御局のような地上の施設によって処理される、本発明の実施形態が説明された。衛

10

20

30

40

50

星システムの動作中の任意の段階において、鍵配布の役割を担うデバイスに新たなデバイスの公開鍵を送信することによって、新たなデバイスがシステムに追加され得る。その後、上述した方法のいずれかを使用して、新たなデバイスの公開鍵を使用してセッション鍵を暗号化することによって、セッション鍵が新たなデバイスに配布され得る。同様に、衛星システムの動作中の任意の段階において、デバイスがシステムから、鍵配布の役割を担うデバイスから上記デバイスの公開鍵を消去することによって除去され得る。これによって、除去されたデバイスが任意の新たな対称鍵を発行されることが防止される。

【0100】

本発明の特定の実施形態が図面を参照して上記で説明されたが、添付の特許請求の範囲に規定される本発明の範囲から逸脱することなく多くの変更及び改変が可能であることを当業者は理解しよう。

〔発明の項目〕

〔項目1〕

第1のデバイス及び第2のデバイスを備える衛星システムにおいてセッション鍵を送信する方法であって、前記第1のデバイス及び前記第2のデバイスのうちの一方が衛星であり、前記第1のデバイス及び前記第2のデバイスのうちの他方が、前記衛星に信号を送信し、及び／又は、前記衛星から信号を受信するように構成されているデバイスであり、前記方法が、

前記第1のデバイスにおいて前記セッション鍵を得るステップと、

前記第1のデバイスの秘密鍵及び前記第2のデバイスの公開鍵に基づいて、前記第1のデバイスにおいて前記セッション鍵を保護するステップと、

前記保護セッション鍵を前記第1のデバイスから前記第2のデバイスに送信するステップと、

を含む、方法。

〔項目2〕

前記保護セッション鍵を送信するステップが、前記保護セッション鍵、及び、前記保護セッション鍵が以前に送信されているか否かを判定するためのリプレイ検出情報を送信するステップを含む、項目1に記載の方法。

〔項目3〕

前記保護セッション鍵及び前記リプレイ検出情報が、鍵配布メッセージに含まれるか、又は

前記第2のデバイスが前記衛星であり、前記第1のデバイスが前記衛星にコマンドメッセージを送信するための制御局であり、前記リプレイ検出情報が、前記保護セッション鍵を含む鍵配布メッセージに結合されているコマンドメッセージに含まれる、項目2に記載の方法。

〔項目4〕

前記第1のデバイスが衛星であり、前記第2のデバイスが前記衛星から信号を受信するように構成されている前記デバイスであり、当該方法が、

前記衛星から前記第2のデバイスにデータストリームを送信するステップであって、前記データストリームが複数の所定部分を含む、ステップ
をさらに含み、

前記保護セッション鍵を送信するステップが、前記保護セッション鍵の所定数のバイトを前記複数の所定部分の各々に挿入することによって、前記データストリームを通じて前記保護セッション鍵を送信するステップを含む、項目1、2又は3に記載の方法。

〔項目5〕

前記得られたセッション鍵が、現在のセッションに後続する次のセッションに使用するための次のセッション鍵であり、前記方法が、

前記現在のセッションに使用するための現在のセッション鍵を得るステップと、

前記衛星の秘密鍵及び前記第2のデバイスの公開鍵に基づいて、前記衛星において前記現在のセッション鍵を保護するステップと、

10

20

30

40

50

前記データストリームを通じて前記現在のセッション鍵を送信するステップと、
前記データストリームを通じて有効性情報を送信するステップであって、前記有効性情報が、前記現在のセッション鍵が有効である期間及び前記次のセッション鍵が有効である期間を規定する、送信するステップと、
をさらに含む、項目 4 に記載の方法。

[項目 6]

第 1 のデバイス及び第 2 のデバイスを備える衛星システムにおいてセッション鍵を得る方法であって、前記第 1 のデバイス及び前記第 2 のデバイスのうちの一方が衛星であり、前記第 1 のデバイス及び前記第 2 のデバイスのうちの他方が、前記衛星に信号を送信し、及び／又は、前記衛星から信号を受信するように構成されているデバイスであり、当該方法が、

10

前記第 2 のデバイスにおいて、前記第 1 のデバイスから保護セッション鍵を受信するステップと、

前記第 1 のデバイスの公開鍵及び前記第 2 のデバイスの秘密鍵に基づいて、前記第 2 のデバイスにおいて、前記受信された保護セッション鍵から前記セッション鍵を得るステップと、
を含む、方法。

[項目 7]

前記保護セッション鍵が送信されたときの前記第 1 のデバイスの予測位置に関する情報を得るステップと、

20

前記保護セッション鍵が受信された位置が所定の誤差範囲内で前記第 1 のデバイスの前記予測位置と一致する場合には、前記受信された保護セッション鍵が真正であると判定するステップと、

をさらに含む、項目 6 に記載の方法。

[項目 8]

前記第 1 のデバイスから前記保護セッション鍵を受信するステップは、コマンドメッセージに結合されている鍵配布メッセージにおいて前記保護セッション鍵を受信するステップを含み、前記コマンドメッセージが、前記保護セッション鍵が以前に送信されているか否かを判定するためのリプレイ検出情報を含み、当該方法が、

前記鍵配布メッセージに結合されている前記コマンドメッセージが以前に送信されていないことを前記リプレイ検出情報が示す場合には、前記保護セッション鍵が以前に送信されていないと判定するステップをさらに含む、項目 6 又は 7 に記載の方法。

30

[項目 9]

前記第 1 のデバイスが前記衛星であり、前記第 2 のデバイスが前記衛星から信号を受信するように構成されている前記デバイスであり、前記衛星から前記保護セッション鍵を受信するステップが、

前記第 2 のデバイスにおいて前記衛星からデータストリームを受信するサブステップであって、前記データストリームは複数の所定部分を含む、サブステップと、

前記複数の所定部分の各々から前記保護セッション鍵の所定数のバイトを抽出するサブステップと、

40

前記保護セッション鍵の前記抽出されたバイトを結合して、前記保護セッション鍵を得るサブステップと、

を含む、項目 6 又は 7 に記載の方法。

[項目 10]

前記得られたセッション鍵が、現在のセッションに後続する次のセッションに使用するための次のセッション鍵であり、当該方法が、

前記データストリームを通じて、前記現在のセッションに使用するための現在の保護セッション鍵、及び、前記現在のセッション鍵が有効である期間及び前記次のセッション鍵が有効である期間を規定する有効性情報を受信するステップと、

前記衛星の公開鍵及び前記第 2 のデバイスの秘密鍵に基づいて、前記第 2 のデバイスに

50

において前記現在の保護セッション鍵から前記現在のセッション鍵を得るステップと、
前記データストリームを通じて保護データが送信された時刻に関する情報を得るステップと、

前記得られた情報が、前記現在のセッション鍵が有効である前記期間の間に前記保護データが送信されたことを示す場合、前記現在のセッション鍵に基づいて前記保護データにアクセスするか、又は、前記得られた情報が、前記次のセッション鍵が有効である前記期間の間に前記保護データが送信されたことを示す場合、前記次のセッション鍵に基づいて前記保護データにアクセスするステップと、
をさらに含む、項目 9 に記載の方法。

[項目 11]

コンピュータプログラムを格納するように構成されているコンピュータ可読記憶媒体であって、前記コンピュータプログラムは、デバイスによって実行されると、前記デバイスに、項目 1 ～ 10 のいずれか一項に記載の方法を実施させる、コンピュータ可読記憶媒体。

[項目 12]

第 1 のデバイスであって、
セッション鍵を得るように構成されている鍵取得モジュールと、
前記第 1 のデバイスの秘密鍵、及び、保護されたセッション鍵が送信されるべき第 2 のデバイスの公開鍵に基づいて、前記得られたセッション鍵を保護するように構成されている鍵保護モジュールと、
前記保護セッション鍵を前記第 2 のデバイスに送信するように構成されている送信機と、
を備え、

前記第 1 のデバイス及び／又は前記第 2 のデバイスが衛星である、第 1 のデバイス。

[項目 13]

前記第 1 のデバイスが、前記保護セッション鍵が以前に送信されているか否かを判定するためのリプレイ検出情報を生成するように構成されているリプレイ情報生成器をさらに備え、

前記送信機が、前記保護セッション鍵及び前記リプレイ検出情報を前記第 2 のデバイスに送信するように構成されている、項目 12 に記載の第 1 のデバイス。

[項目 14]

前記第 1 のデバイスが、前記第 2 のデバイスにデータストリームを送信するように構成されている衛星であり、前記データストリームが複数の所定部分を含み、前記送信機が、前記保護セッション鍵の所定数のバイトを前記複数の所定部分の各々に挿入することによって、前記データストリームを通じて前記保護セッション鍵を送信するように構成されているか、又は

前記第 2 のデバイスが前記衛星であり、前記第 1 のデバイスが、コマンドメッセージを前記衛星に送信するための制御局であり、前記送信機が、前記保護セッション鍵を含む鍵配布メッセージに結合されているコマンドメッセージに前記リプレイ検出情報を含めるように構成されている、項目 12 又は 13 に記載の第 1 のデバイス。

[項目 15]

第 2 のデバイスから信号を受信するための第 1 のデバイスであって、前記第 1 のデバイスが、

前記第 2 のデバイスから保護セッション鍵を受信するように構成されている受信機と、
前記第 1 のデバイスの秘密鍵、及び、前記保護セッション鍵が受信された前記第 2 のデバイスの公開鍵に基づいて、前記保護セッション鍵から前記セッション鍵を得るように構成されている鍵抽出モジュールと、
を備え、

前記第 1 のデバイス及び／又は前記第 2 のデバイスが衛星である、第 1 のデバイス。

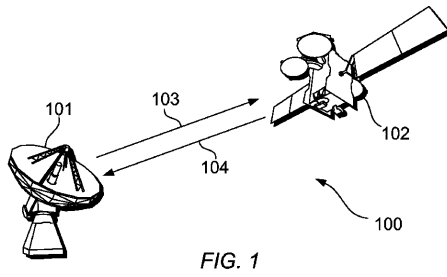
10

20

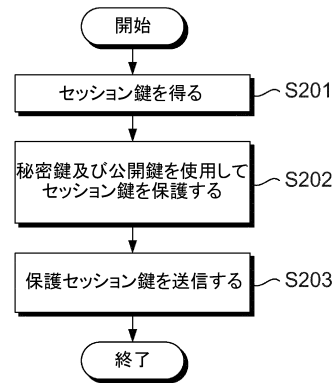
30

40

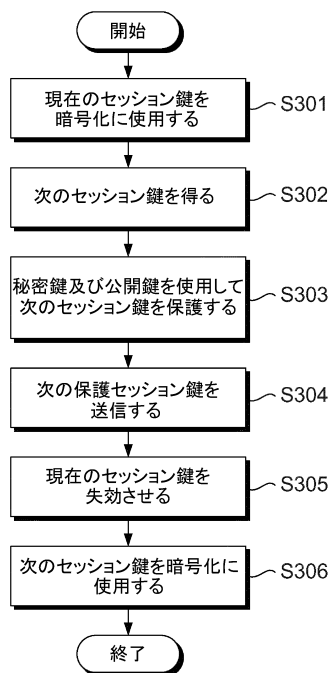
【図 1】



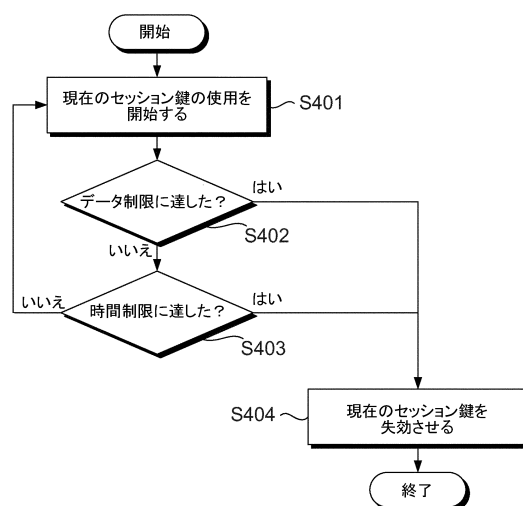
【図 2】



【図 3】



【図 4】



【図 5】

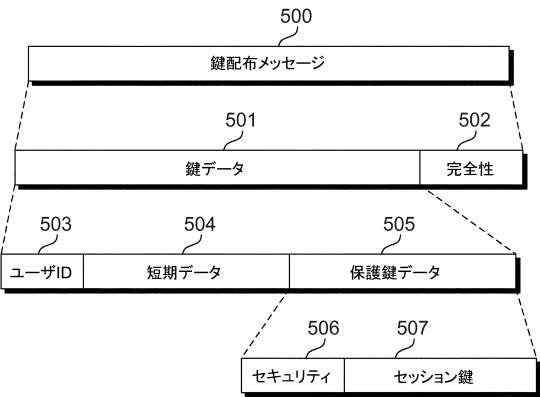


FIG. 5

【図 6】

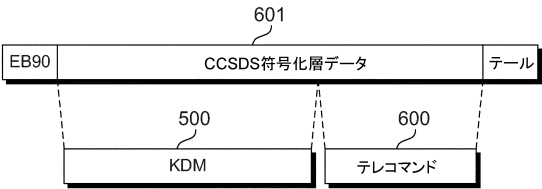


FIG. 6

【図 7】

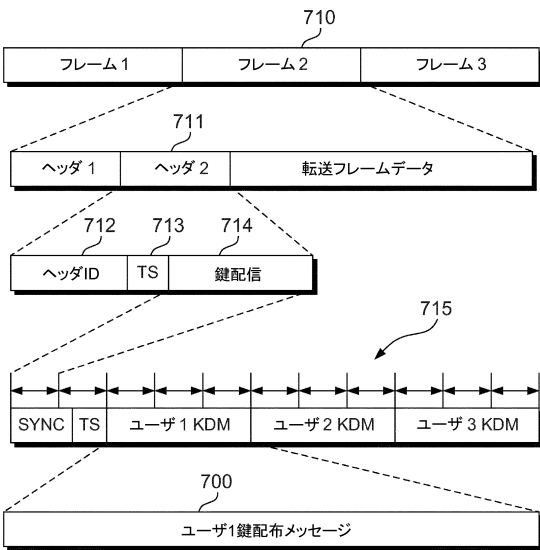


FIG. 7

【図 8】

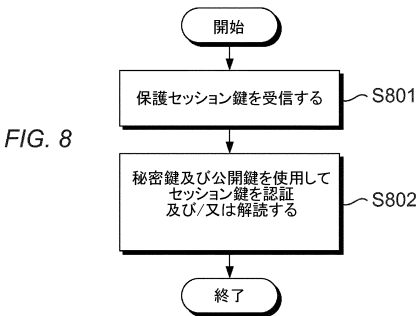
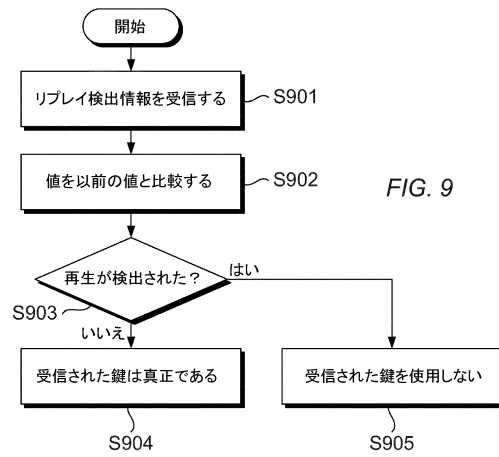
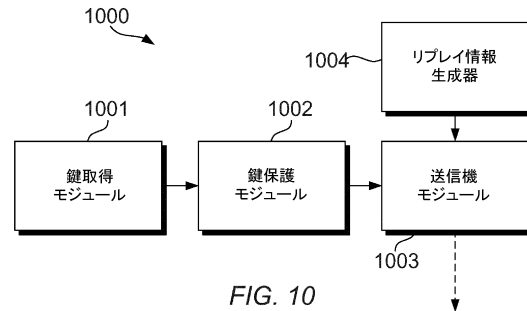


FIG. 8

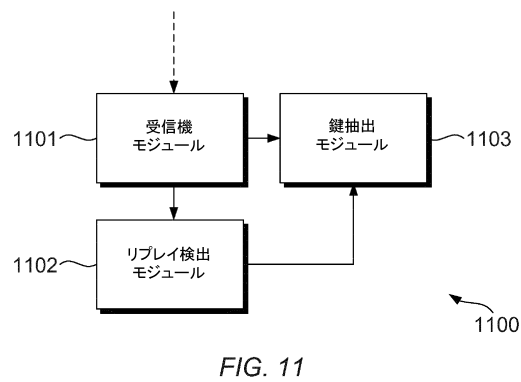
【図 9】



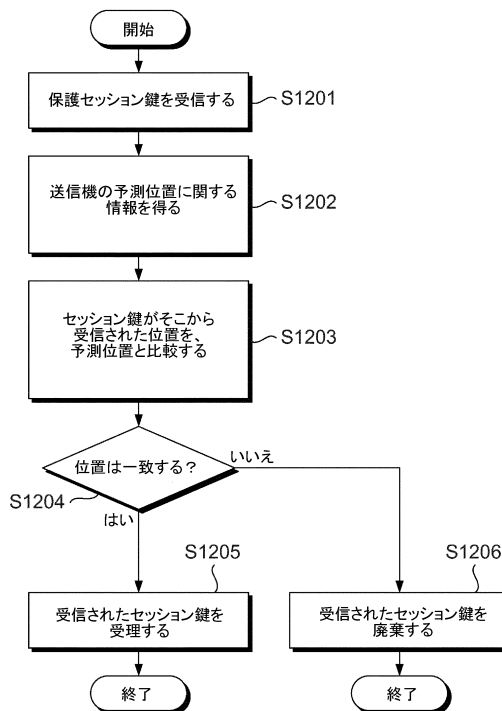
【図 10】



【図 11】



【図 12】



フロントページの続き

- (72)発明者 クラーク, スティーヴ
イギリス, エスジー１ ２エーエス ハートフォードシャー スティーヴネイジ, ガネルズ
ウッド ロード, アストリアム リミテッド
- (72)発明者 マッコイ, トーマス
イギリス, エスジー１ ２エーエス ハートフォードシャー スティーヴネイジ, ガネルズ
ウッド ロード, アストリアム リミテッド

審査官 青木 重徳

- (56)参考文献 特開２００９－１３０７４６（ＪＰ，Ａ）
特表平０９－５０５７１１（ＪＰ，Ａ）
特開２０１０－０８７８８８（ＪＰ，Ａ）
特表２００７－５３３２４８（ＪＰ，Ａ）
国際公開第２００７／０６６６６８（ＷＯ，Ａ１）
特開２００４－２８０４０１（ＪＰ，Ａ）
米国特許出願公開第２０１１／０１０３５８９（ＵＳ，Ａ１）
中国特許出願公開第１０１６２７５７５（ＣＮ，Ａ）

- (58)調査した分野(Int.Cl., DB名)
- | | |
|------|------|
| H04L | 9/36 |
| H04L | 9/08 |
| H04L | 9/32 |