

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7656065号
(P7656065)

(45)発行日 令和7年4月2日(2025.4.2)

(24)登録日 令和7年3月25日(2025.3.25)

(51)国際特許分類

F I

H 0 4 L 9/08 (2006.01) H 0 4 L 9/08 B

G 0 6 F 21/60 (2013.01) G 0 6 F 21/60 3 6 0

請求項の数 15 (全20頁)

(21)出願番号	特願2023-554853(P2023-554853)	(73)特許権者	523380173
(86)(22)出願日	令和4年1月20日(2022.1.20)		ヒタチ・エナジー・リミテッド
(65)公表番号	特表2024-515154(P2024-515154 A)		H I T A C H I E N E R G Y L T D
(43)公表日	令和6年4月5日(2024.4.5)		スイス、8 0 5 0 チューリッヒ、プラ
(86)国際出願番号	PCT/EP2022/051217	(74)代理人	110001195
(87)国際公開番号	WO2022/189053		弁理士法人深見特許事務所
(87)国際公開日	令和4年9月15日(2022.9.15)	(72)発明者	マルティネス・サラサル、ハロルド・
審査請求日	令和5年10月16日(2023.10.16)		ロベルト
(31)優先権主張番号	21161344.3		スイス、8 9 5 3 チューリッヒ、ディ
(32)優先日	令和3年3月8日(2021.3.8)		ーティコン、ボルフスマットシュトラ
(33)優先権主張国・地域又は機関	欧州特許庁(EP)	(72)発明者	ース、9
			ポーランド、3 1 - 1 1 5 クラクフ、
			ガルンツァルカ、8 / 7 ・ベ
			最終頁に続く

(54)【発明の名称】 セキュアキー管理デバイス、認証システム、広域ネットワーク、およびセッションキーを生成する方法

(57)【特許請求の範囲】

【請求項1】

エンドデバイス（E D）と、ネットワークサーバ（N S）と、アプリケーションサーバ（A S）と、参加サーバ（J S）とを備える広域ネットワーク用のセキュアキー管理デバイス（S K M D）であって、

- － 秘密キー情報の保存のためのセキュアストレージコンポーネント（S S C）と、
- － 前記参加サーバ（J S）とセキュアにデータを交換するためのセキュアインターフェース（I / F）と、
- － 少なくとも1つの処理コンポーネント（P C）であって、
- － 少なくとも1つのマスターキー（K a）を生成し、前記セキュアストレージコンポーネント（S S C）に保存し、
- － 前記少なくとも1つのマスターキー（K a）と、前記エンドデバイス（E D）の一意識別子（S / N）とに基づいて、少なくとも1つのルートキー（R K e y）を生成し、生成された前記少なくとも1つのルートキー（R K e y）を前記エンドデバイス（E D）に提供し、
- － 前記参加サーバ（J S）から、前記セキュアインターフェース（I / F）を介して、前記エンドデバイス（E D）の前記一意識別子（S / N）と、セッション情報（S I D）とを含む第1のリクエスト（R E Q 1）を受信し、
- － 前記セキュアストレージコンポーネント（S S C）に保存されている前記少なくとも1つのマスターキー（K a）と、前記第1のリクエストに含まれている前記エンドデ

バイス（E D）の前記一意識別子（S / N）および前記セッション情報（S I D）とに基づいて、少なくとも1つのセッションキー（S K e y）を生成し、

－ 前記少なくとも1つのセッションキー（S K e y）を、前記セキュアインターフェース（I / F）を介して前記参加サーバ（J S）に提供するように構成されている、少なくとも1つの処理コンポーネント（P C）と、

を備える、セキュアキー管理デバイス（S K M D）。

【請求項2】

広域ネットワークにおいてエンドデバイス（E D）を認証するための認証システムであって、

－ 請求項1に記載のセキュアキー管理デバイス（S K M D）と、

－ 前記セキュアインターフェース（I / F）を介して前記セキュアキー管理デバイス（S K M D）に接続された参加サーバ（J S）と、

を備え、

－ 前記参加サーバ（J S）の少なくとも1つの処理コンポーネントは、

－ 前記エンドデバイス（E D）から、前記エンドデバイス（E D）のアドレス情報を含む第2のリクエストを受信し、

－ 前記セキュアインターフェース（I / F）を介して前記セキュアキー管理デバイス（S K M D）に、前記第2のリクエストの前記アドレス情報に基づいて前記第1のリクエスト（R E Q 1）を提供し、

－ 前記セキュアキー管理デバイス（S K M D）から前記セキュアインターフェース（I / F）を介して受信した前記少なくとも1つのセッションキー（S K e y）を、前記ネットワークサーバ（N S）および前記アプリケーションサーバ（A S）のうちの少なくとも一方に転送するように構成されている、認証システム。

【請求項3】

－ 事前登録手順中に、前記エンドデバイス（E D）と、前記セキュアキー管理デバイス（S K M D）とに接続可能な登録デバイス（R D）を更に備え、

－ 前記登録デバイス（R D）の少なくとも1つの処理コンポーネントは、前記事前登録手順中に、

－ 前記エンドデバイス（E D）の前記一意識別子（S / N）を決定するステップと、

－ 前記エンドデバイス（E D）の前記一意識別子（S / N）を含む第3のリクエストを前記セキュアキー管理デバイス（S K M D）に提供するステップと、

－ 前記セキュアキー管理デバイス（S K M D）によって提供された前記少なくとも1つのルートキー（R K e y）を受信するステップと、

－ 前記少なくとも1つのルートキー（R K e y）を前記エンドデバイス（E D）にセキュアに保存するステップと、

を実行するように構成されている、請求項2に記載の認証システム。

【請求項4】

前記登録デバイス（R D）の前記少なくとも1つの処理コンポーネントは、前記事前登録手順中に、

－ 前記広域ネットワークにおける前記エンドデバイス（E D）をアドレス指定するためのエンドデバイスアドレス識別子（D e v E U I）を決定するステップと、

－ 前記エンドデバイスアドレス識別子（D e v E U I）を前記エンドデバイス（E D）に保存するステップと、

－ 前記参加サーバ（J S）に登録メッセージを提供するステップであって、前記登録メッセージは、前記エンドデバイス（E D）の前記一意識別子（S / N）と、前記エンドデバイスアドレス識別子（D e v E U I）と、任意選択で、前記少なくとも1つのルートキー（R K e y）を生成するために使用された前記マスターキー（K a）に関連するバージョンデータ（K n）とを含む、提供するステップと、

を実行するように更に構成されている、請求項3に記載の認証システム。

【請求項5】

広域ネットワークであって、

- － 請求項 2 から 4 のいずれか 1 項に記載の認証システムと、
- － 少なくとも 1 つのエンドデバイス (E D) と、
- － 少なくとも 1 つのネットワークサーバ (N S) と、
- － 少なくとも 1 つのアプリケーションサーバ (A S) と、

を備え、

－ 前記少なくとも 1 つのエンドデバイス (E D) は、前記ネットワークサーバ (N S) にデータパケットを送るよう構成され、前記データパケットは、ネットワーク層上およびアプリケーション層上で暗号化され、

－ 前記少なくとも 1 つのネットワークサーバ (N S) は、前記参加サーバ (J S) から受信した少なくとも 1 つのネットワークセッションキー (F N w k S I n t K e y、S N w k S I n t K e y、N w k S E n c K e y) を使用して前記ネットワーク層上の前記データパケットを復号し、前記復号されたデータパケットを前記アプリケーションサーバ (A S) に転送するよう構成され、

－ 前記少なくとも 1 つのアプリケーションサーバ (A S) は、前記参加サーバ (J S) から受信した少なくとも 1 つのアプリケーションセッションキー (A p p S K e y) を使用して、前記アプリケーション層上の前記データパケットを復号するよう構成されている、広域ネットワーク。

【請求項 6】

前記広域ネットワークは、前記エンドデバイス (E D) を含む低電力ワイヤレスアクセスネットワークドメインと、前記アプリケーションサーバ (A S) を含むコアネットワークドメインと、を備え、前記セキュアインターフェース (I / F) は、前記低電力ワイヤレスアクセスネットワークドメインおよび／または有線の前記コアネットワークドメインの外部にある前記参加サーバ (J S) とデータを交換するために構成されている、請求項 5 に記載の広域ネットワーク。

【請求項 7】

前記広域ネットワークは、L o R a W A N ネットワークであり、前記セキュアインターフェース (I / F) は、前記 L o R a W A N ネットワークのアドレス空間の外部の前記参加サーバ (J S) とデータを交換するために構成され、前記セッション情報 (S I D) は、参加ノンス、ネットワーク i d、およびデバイスノンスのうちの少なくとも 1 つを含む、請求項 5 または 6 に記載の広域ネットワーク。

【請求項 8】

セキュアキー管理デバイス (S K M D) に事前登録されたエンドデバイス (E D) と、ネットワークサーバ (N S) と、アプリケーションサーバ (A S) と、参加サーバ (J S) とを備える広域ネットワークで使用するセッションキー (S K e y) を生成する方法であって、

－ 前記セキュアキー管理デバイス (S K M D) によって、前記参加サーバ (J S) から、セキュアインターフェース (I / F) を介して、前記エンドデバイス (E D) の一意識別子 (S / N) と、セッション情報 (S I D) とを含む第 1 のリクエスト (R E Q 1) を、受信することと、

－ 前記セキュアキー管理デバイス (S K M D) によって、前記セキュアキー管理デバイス (S K M D) に保存されている少なくとも 1 つのマスターキー (K a) と、前記第 1 のリクエスト (R E Q 1) に含まれている前記エンドデバイス (E D) の前記一意識別子 (S / N) および前記セッション情報 (S I D) とに基づいて、少なくとも 1 つのセッションキー (S K e y) を生成することと、

－ 前記セキュアキー管理デバイス (S K M D) によって、前記生成された少なくとも 1 つのセッションキー (S K e y) を、前記セキュアインターフェース (I / F) を介して前記参加サーバ (J S) に提供することと、

を含む、方法。

【請求項 9】

前記セキュアキー管理デバイス（SKMD）によって、少なくとも1つのネットワークセッションキー（FNwkSIntKey、SNwkSIntKey、NwkSEncKey）および少なくとも1つのアプリケーションセッションキー（AppSKey）が生成され、前記参加サーバ（JS）に提供される、請求項8に記載の方法。

【請求項10】

前記少なくとも1つのセッションキー（SKey）を生成することは、

－ 前記セキュアキー管理デバイス（SKMD）によって、前記セキュアキー管理デバイス（SKMD）に保存されている前記少なくとも1つのマスターキー（Ka）と、前記第1のリクエスト（REQ1）に含まれている前記エンドデバイス（ED）の前記一意識別子（S/N）とを使用する少なくとも1つの第1の暗号関数（FA、FB）に基づいて、前記エンドデバイス（ED）の少なくとも1つのルートキー（RKey）を生成することと、

－ 前記セキュアキー管理デバイス（SKMD）によって、生成された前記少なくとも1つのルートキー（RKey）と、前記第1のリクエストに含まれている前記セッション情報（SID）とを使用する少なくとも1つの第2の暗号関数に基づいて、前記少なくとも1つのセッションキー（SKey）を生成することと、

を含む、請求項8または9に記載の方法。

【請求項11】

前記エンドデバイス（ED）は、事前登録手順において、前記セキュアキー管理デバイス（SKMD）によって前記第1のリクエスト（REQ1）を受信することの前に、前記セキュアキー管理デバイス（SKMD）に事前登録され、前記事前登録手順は、

－ 前記セキュアキー管理デバイス（SKMD）によって、前記少なくとも1つのマスターキー（Ka）を生成し、前記少なくとも1つのマスターキー（Ka）を前記セキュアキー管理デバイス（SKMD）内に保存することと、

－ 前記セキュアキー管理デバイス（SKMD）によって、前記少なくとも1つのマスターキー（Ka）と、前記セキュアキー管理デバイス（SKMD）に提供された前記エンドデバイス（ED）の前記一意識別子（S/N）とに基づいて、少なくとも1つのルートキー（RKey）を生成することと、

－ 生成された前記少なくとも1つのルートキー（RKey）を前記エンドデバイス（ED）に提供することと、

を含む、請求項8から10のいずれか1項に記載の方法。

【請求項12】

－ 前記少なくとも1つのマスターキー（Ka）を生成することは、所定条件の後に繰り返され、

－ 前記事前登録手順中に、前記少なくとも1つのルートキー（RKey）を生成するために使用された前記マスターキー（Ka）に関連するバージョンデータ（Kn）が前記エンドデバイス（ED）に提供され、

－ 前記参加サーバ（JS）から受信した前記第1のリクエスト（REQ1）は、前記バージョンデータ（Kn）を更に含む、請求項11に記載の方法。

【請求項13】

－ 前記参加サーバ（JS）によって、前記エンドデバイス（ED）から、前記エンドデバイス（ED）のアドレス情報を含む第2のリクエストを受信することと、

－ 前記参加サーバ（JS）によって、前記セキュアインターフェース（I/F）を介して、前記セキュアキー管理デバイス（SKMD）に、前記第2のリクエストの前記アドレス情報に基づいて前記第1のリクエスト（REQ1）を提供することと、

－ 前記セキュアインターフェース（I/F）を介して、前記セキュアキー管理デバイス（SKMD）から受信した前記少なくとも1つのセッションキー（SKey）を、前記ネットワークサーバ（NS）および前記アプリケーションサーバ（AS）のうちの少なくとも一方に転送することと、

を更に含む、請求項8から12のいずれか1項に記載の方法。

【請求項 14】

前記第2のリクエストの前記アドレス情報は、前記エンドデバイス（E D）のエンドデバイスアドレス識別子（D e v E U I）を含み、前記方法は、

－ 前記事前登録手順中に、前記エンドデバイス（E D）の前記一意識別子（S / N）と、前記エンドデバイスアドレス識別子（D e v E U I）と、任意選択で、前記少なくとも1つのルートキー（R K e y）を生成するために使用された前記マスターキー（K a）に関連するバージョンデータ（K n）とを、前記参加サーバ（J S）に提供することと、
－ 前記参加サーバ（J S）によって、前記第2のリクエストに含まれている前記エンドデバイスアドレス識別子（D e v E U I）を、前記エンドデバイス（E D）の前記一意識別子（S / N）にマッピングすることと、

10

－ 前記参加サーバ（J S）によって、前記エンドデバイスアドレス識別子（D e v E U I）の前記一意識別子（S / N）への前記マッピングに基づいて、前記第1のリクエスト（R E Q 1）を生成することと、

を更に含む、請求項 11 または 12 のいずれか 1 項を引用する請求項 13 に記載の方法。

【請求項 15】

命令を保存するデータストレージデバイスであって、前記命令は、ネットワーク化されたコンピューティングデバイスの少なくとも1つの処理デバイスによって実行されると、請求項 8 から 14 のいずれか 1 項に記載の方法のステップを実施する、データストレージデバイス。

20

【発明の詳細な説明】

【技術分野】

【0001】

本開示は、セキュアなセッションキー管理のためのデバイス、システム、および方法に関する。

【背景技術】

【0002】

米国特許出願公開第 2020 / 0 288 312 号には、端末と、端末にネットワークサービスを提供できる通信ネットワークサーバと、ネットワークおよびネットワークサーバを介して端末にアプリケーションサービスを提供できるアプリケーションサーバを含む通信システムが開示されている。

30

【0003】

W O 2 0 1 8 / 1 4 8 2 4 4 A 1 には、アプリケーションプロバイダが、デバイスのデプロイメント前に、グループマスターキーをネットワークプロバイダに転送するキープロビジョニング手順が開示されている。このキープロビジョニング手順により、ネットワークプロバイダは、デバイスを一意のキーで管理する必要なく、システム内の多数のデバイスを認証することができる。

【0004】

米国特許第 10 880 743 号には、モノのインターネット（I o T）デバイスのアクティベーションおよびエンドツーエンドベースの自動オンボーディングのための一元化された中立システムと、I o T デバイスと I o T プラットフォームとの間のセキュアな通信の確立のための技術について説明されている。

40

【発明の概要】

【発明が解決しようとする課題】

【0005】

広域ネットワークにおいてキーをセキュアに管理するための改良されたデバイス、システム、および方法を提供することを目的とする。

【課題を解決するための手段】

【0006】

第1の態様によれば、エンドデバイスと、ネットワークサーバと、アプリケーションサーバと、参加サーバとを備える広域ネットワーク用のセキュアキー管理デバイスが提供さ

50

れる。セキュアキー管理デバイスは、秘密キー情報の保存のためのセキュアストレージコンポーネントと、参加サーバとセキュアにデータを交換するためのセキュアインターフェースと、少なくとも1つの処理コンポーネントとを備える。少なくとも1つの処理コンポーネントは、少なくとも1つのマスターキーを生成し、セキュアストレージコンポーネントに保存し、少なくとも1つのマスターキーと、エンドデバイスの一意識別子とに基づいて、少なくとも1つのルートキーを生成し、生成された少なくとも1つのルートキーをエンドデバイスに提供し、参加サーバから、セキュアインターフェースを介して、エンドデバイスの一意識別子と、セッション情報とを含む第1のリクエストを受信し、セキュアストレージコンポーネントに保存されている少なくとも1つのマスターキーと、第1のリクエストに含まれているエンドデバイスの一意識別子およびセッション情報とに基づいて、少なくとも1つのセッションキーを生成し、少なくとも1つのセッションキーを、セキュアインターフェースを介して参加サーバに提供するように構成されている。

10

【0007】

セキュアな管理内にマスターキーを保存することで、キーの管理と保存のための一元化されたセキュアな環境を確立できる。ルートキーおよびセッションキーを、マスターキーからオンザフライで派生させて、セキュアインターフェースを介して参加サーバに提供できるため、参加サーバなどの広域ネットワークのリモートまたは公開コンポーネント内にセキュリティ上重要なデータを保存する必要がなくなる。

【0008】

第2の態様によれば、広域ネットワークにおいてエンドデバイスを認証するための認証システムが提供される。この認証システムは、第1の態様によるセキュアキー管理デバイスと、セキュアインターフェースを介してセキュアキー管理デバイスに接続された参加サーバとを備える。参加サーバの少なくとも1つの処理コンポーネントは、エンドデバイスから、エンドデバイスのアドレス情報を含む第2のリクエストを受信し、セキュアインターフェースを介してセキュアキー管理デバイスに、第2のリクエストのアドレス情報に基づいて第1のリクエストを提供し、セキュアキー管理デバイスからセキュアインターフェースを介して受信した少なくとも1つのセッションキーを、ネットワークサーバおよびアプリケーションサーバのうちの少なくとも一方に転送するように構成されている。

20

【0009】

セキュアキー管理デバイスから少なくとも1つのセッションキーをオンデマンドで要求することにより、認証システムの参加サーバは、ルートキーへのローカルアクセスなしで、標準に準拠した方法で広域ネットワークからのクエリに応答できる。

30

【0010】

第3の態様によれば、第2の態様による認証システムと、少なくとも1つのエンドデバイスと、少なくとも1つのネットワークサーバと、少なくとも1つのアプリケーションサーバとを備える広域ネットワークが提供される。少なくとも1つのエンドデバイスは、ネットワークサーバにデータパケットを送るように構成され、データパケットは、ネットワーク層上およびアプリケーション層上で暗号化され、少なくともネットワークサーバは、参加サーバから受信した少なくとも1つのネットワークセッションキーを使用してネットワーク層上のデータパケットを復号し、部分的に復号されたデータパケットをアプリケーションサーバに転送するように構成され、少なくともアプリケーションサーバは、参加サーバから受信した少なくとも1つのアプリケーションセッションキーを使用して、アプリケーション層上のデータパケットを復号するように構成されている。

40

【0011】

上記の広域ネットワークは、ルートキーなどのセキュリティ上重要なデータを中間ネットワークコンポーネントから隠すことで高度なネットワークセキュリティを提供し、したがって、エンドデバイスとアプリケーションサーバとの通信のエンドツーエンドのセキュリティを確保する。

【0012】

第4の態様によれば、広域ネットワークで使用するセッションキーを生成する方法が提

50

供される。広域ネットワークは、セキュアキー管理デバイスに事前登録されたエンドデバイスと、ネットワークサーバと、アプリケーションサーバと、参加サーバとを備える。この方法は、セキュアキー管理デバイスによって、参加サーバから、セキュアインターフェースを介して、エンドデバイスの一意識別子と、セッション情報とを含む第1のリクエストを受信することと、セキュアキー管理デバイスによって、セキュアキー管理デバイスに保存されている少なくとも1つのマスターキーと、第1のリクエストに含まれているエンドデバイスの一意識別子およびセッション情報とに基づいて、少なくとも1つのセッションキーを生成することと、セキュアキー管理デバイスによって、生成された少なくとも1つのセッションキーを、セキュアインターフェースを介して参加サーバに提供することとを含む。

10

【0013】

上記の方法では、セキュアキー管理デバイスによってセッションキーをオンザフライで生成できる。

【0014】

第5の態様によれば、広域ネットワークで使用するために、エンドデバイスをセキュアキー管理デバイスに事前登録する方法が提供される。事前登録手順は、セキュアキー管理デバイスによって、少なくとも1つのマスターキーを生成し、少なくとも1つのマスターキーをセキュアキー管理デバイス内に保存することと、セキュアキー管理デバイスによって、少なくとも1つのマスターキーと、セキュアキー管理デバイスに提供されたエンドデバイスの一意識別子とに基づいて、少なくとも1つのルートキーを生成することと、生成された少なくとも1つのルートキーをエンドデバイスに提供することとを含む。

20

【0015】

第5の態様による方法は、第4の態様による第1のリクエストを受信するステップを実行する前に、エンドデバイスをセキュアキー管理デバイスに事前登録するために使用できる。

【0016】

第6の態様によれば、命令を保存するデータストレージデバイスであって、命令は、ネットワーク化されたコンピューティングデバイスの少なくとも1つの処理デバイスによって実行されると、第4または第5の態様による方法のステップを実施する、データストレージデバイス。

30

【0017】

少なくとも1つの実施形態によれば、広域ネットワークはLoRaWANネットワークであり、セキュアインターフェースは、LoRaWANネットワークのアドレス空間の外部の参加サーバとデータを交換するために構成されているため、LoRaWANネットワークからセキュアキー管理デバイスが隠される。

【0018】

少なくとも1つの実施形態によれば、少なくとも1つのマスターキーを生成するステップは、所定条件の後に繰り返される。事前登録手順中に、少なくとも1つのルートキーを生成するために使用されたマスターキーに関連するバージョンデータがエンドデバイスに提供される。この実施形態では、参加サーバから受信した第1のリクエストは、バージョンデータを更に含む。

40

【0019】

例えば、所定の時間の経過後やセキュリティ違反の後に、マスターキーのバージョンデータを変更して追跡することで、侵害されたキーの影響を制限することができるため、サイバーセキュリティが更に強化される。

【0020】

少なくとも1つの実施形態によれば、第2のリクエストのアドレス情報は、エンドデバイスのエンドデバイスアドレス識別子を含む。事前登録手順中に、エンドデバイスの一意識別子と、エンドデバイスアドレス識別子と、任意選択で、少なくとも1つのルートキーを生成するために使用されたマスターキーに関連するバージョンデータとが、参加サーバ

50

に提供される。参加サーバは、第2のリクエストに含まれているエンドデバイスアドレス識別子をエンドデバイスの一意識別子にマッピングし、エンドデバイスアドレス識別子の一意識別子へのマッピングに基づいて、第1のリクエストを生成する。これにより、セキュアキー管理デバイスからエンドデバイスアドレス識別子が隠される。

【0021】

本開示の更なる態様および実施形態は、添付の特許請求の範囲に記載されている。

上記および添付の特許請求の範囲に記載されているデバイスならびにシステムは、セッションキーを生成する方法に適している。したがって、デバイスおよびシステムに関連して説明されている特徴および利点は、この方法で使用でき、その逆も同様である。

【0022】

本開示は、いくつかの態様から構成されている。これらの態様のうちの1つに関して記載されているどの特徴も、それぞれの特徴が特定の態様のコンテキストで明示的に言及されていない場合でも、他の態様に関しても本明細書では開示されている。

【0023】

更に理解を深めるために、添付の図が含まれている。図では、同じ構造および／または機能の要素を、同じ参照記号で参照する場合がある。図に示す実施形態は例示的な表現であり、必ずしも縮尺どおりに描かれていないことを理解されたい。

【図面の簡単な説明】

【0024】

【図1】本開示の一実施形態によるセキュアキー管理デバイスの概略ブロック図である。

【図2】本開示の実施形態による様々な方法のステップの概略シーケンス図である。

【図3】LoRaWANシステムに典型的であるWANアーキテクチャの概略ブロック図である。

【図4】LoRaWANエンティティにおけるセキュアな通信フローの概略ブロック図である。

【図5】本開示の一実施形態による認証システムを含む広域ネットワークの概略ブロック図である。

【図6】本開示の一実施形態による広域ネットワークにおける、セキュアキー管理デバイスの初期化、エンドデバイスの事前登録および参加処理の概略シーケンス図である。

【発明を実施するための形態】

【0025】

本開示は、様々な修正や代替形態に対応することができるが、その具体的な内容は図中の例によって示されており、詳細に説明する。ただし、その意図は、本開示を説明した特定の実施形態に限定することではないことを理解する必要がある。反対に、添付の特許請求の範囲に定義された本開示の範囲内にあるすべての修正、均等物、および代替物を対象にすることを意図している。

【0026】

本開示は、低電力およびワイヤレスベースのLoRaWANベースのシステムなど、広域ネットワークにおいてルートキーを初期化、生成、およびプロビジョニングするための改良されたシステムおよび方法を示すことを目標とする。

【0027】

例として、このセクションでは、LoRaWANベースのシステムのワークフローの背景と、そのキー管理における既存の課題について説明する。本開示は、この既存の課題に取り組み、サイバーセキュリティを向上させることに重点を置いている。

【0028】

図1は、本開示の一実施形態によるセキュアキー管理デバイスSKMDの概略ブロック図を示している。セキュアキー管理デバイスSKMDは、秘密キー情報を保存するためのセキュアストレージコンポーネントSSCと、保存した命令を実行するための処理コンポーネントPCと、広域ネットワーク(WAN)の参加サーバなどの他のエンティティとセキュアにデータを交換するためのセキュアインターフェースI/Fとを備える。

10

20

30

40

50

【0029】

説明した本実施形態では、セキュアキー管理デバイスSKMDは、サーバコンピュータが1つまたはいくつかのデータネットワークにデプロイされるときに、プログラム命令の保存および実行に適した従来のコンポーネントを備えるサーバコンピュータとして実装することができる。セキュアストレージコンポーネントSSCは、私有暗号化キーおよび／または他の秘密キー情報およびパラメータなど、セキュリティ上重要な情報をセキュアに保存するように設計されたハードウェアセキュアモジュール（HSM：hardware secure module）の一部であり得る。HSMは、不正なデータアクセスから保護され、典型的には、暗号関数を実行するように構成された処理コンポーネントも備える。このようにして、私有キーなどのセキュリティ上重要な情報が、セキュアキー管理デバイスSKMDの動作中にHSMから離れることは決してない。

10

【0030】

説明した本実施例では、処理コンポーネントPCの一部または全部もHSMの一部である。例えば、処理コンポーネントPCの第1の部分がHSM内にあり得、すでに暗号化されたデータパケットの受信や送信など、セキュリティ上重要ではない動作を実行するために使用される処理コンポーネントPCの第2の部分が、サーバコンピュータの異なる部分に実装され得る。

【0031】

説明した本実施例では、セキュアインターフェースI／Fはネットワークインターフェースもしくはユーザコンソール、またはそれらの組合せであり得る。例えば、セキュアストレージコンポーネントSSCに保存された私有キーに基づく標準の暗号化方法で保護されている従来のネットワーク機器を使用して、セキュアインターフェースI／Fを介してセキュアキー管理デバイスSKMDに入るまたはそこから出る情報を保護できる。

20

【0032】

図2は、本開示の実施形態による様々な操作方法のステップの概略シーケンス図を示している。図2は、セキュアキー管理デバイスSKMDのコンポーネントSSC、コンポーネントPC、およびI／F間の内部インタラクションと、セキュアキー管理デバイスSKMDと外部ユーザとのインタラクションの両方を示している。

【0033】

図2の上部に示すセキュアキー管理デバイスSKMDの初期化中に、例えば、セキュアキー管理デバイスSKMDとして構成されたネットワークサーバを最初にセットアップまたは起動することによって、処理コンポーネントPCは、少なくとも1つのマスターキーKaを生成し、生成されたマスターキーKaをセキュアストレージコンポーネントSSCに保存する。例えば、処理コンポーネントは、事前定義された暗号関数に基づいて秘密マスターキーを生成するために、ランダムまたは擬似ランダムのシード値を取得できる。セキュリティを向上させるために、マスターキーKaは、後で詳しく説明するように、時々変更されることがある。この場合、マスターキーKaの各バージョンは、対応するバージョンデータKnとともに、セキュアキー管理デバイスSKMDのセキュアストレージコンポーネントSSCに保存される。秘密マスターキーKaデータがセキュアストレージコンポーネントSSCにセキュアに保存されると、セキュアキー管理デバイスSKMDは動作のための準備が整う。

30

40

【0034】

図2の中央部に示す別のプロセスでは、ユーザは特定のエンドデバイスをセキュアキー管理デバイスSKMDに事前登録できる。このために、ユーザはまず、処理コンポーネントPCに、登録するエンドデバイスの一意識別子S／Nを提供する。例えば、ユーザがエンドデバイスのシリアルナンバーを手動で入力してもよい。あるいは、以下に詳述するように、エンドデバイスのシリアルナンバーが、プレコミッシングデバイスを使用して、エンドデバイスの製造業者によって、製造プロセスの最後に自動的に提供されてもよい（図2には図示せず）。このようなプレコミッシングデバイスは、セキュアキー管理デバイスSKMDに直接かつセキュアに接続されたマシンツーマシン（M2M）インター

50

フェースを有し得る。

【0035】

提供されたシリアルナンバーで識別されるエンドデバイスに関連付けられた少なくとも1つのルートキーRKeyを生成するために、処理コンポーネントPCはセキュアストレージコンポーネントSSCからアクティブ秘密マスターキーKaを取得する。次に、適切な暗号関数に基づいて、エンドデバイスのルートキーRKeyが、一意識別子S／NおよびアクティブマスターキーKaに基づいて、処理コンポーネントPCによって生成される。

【0036】

最後のステップでは、セキュアキー管理デバイスSKMDによって生成されたルートキーRKeyがエンドデバイスに提供される（図2には図示せず）。例えば、ルートキーRKeyをエンドデバイスに直接プログラミングするために、ルートキーRKeyは、プレコミッショニングデバイスのM2Mインターフェースを介して電子的に通信し返されてもよい。したがって、エンドデバイスの登録中に、送信された情報のペーパートレイルを保持する必要がない。

【0037】

特定のデバイスおよびアプリケーションのセキュリティ要件に応じて、ルートキーRKeyおよび一意識別子S／N、ならびにエンドデバイスアドレス識別子などの任意の他のセキュリティ上重要なデータは、エンドデバイスのセキュアエレメント（SE：secure element）に保存され得る。比較的低いセキュリティレベルの場合、この情報はエンドデバイスの従来の不揮発性メモリに保存されることもある。この場合、対応するハッシュ値をエンドデバイスに保存して、保存したデータが後で操作されるのを回避することができる。

【0038】

このプロセスの最後には、エンドデバイスは、セキュアキー管理デバイスSKMDのアクティブマスターキーKaに関連付けられ、カスタマに対してデプロイしたり、以下により詳しく説明するように、WANアプリケーションでエンドデバイスとして使用したりすることができる。また、以下に詳述するように、参加サーバなどの更なるエンティティが関与する追加のアクティベーション手順によって、セキュアキー管理デバイスSKMDに間接的にリンクすることもできる。

【0039】

エンドデバイスの動作中に、エンドデバイスは、WANのアプリケーションサーバで実行されている特定のアプリケーションにコンタクトしようとする場合がある。エンドデバイスとアプリケーションサーバとの間に、対応する通信チャネルが確立される前に、データパケットのルーティングを担当するネットワークサーバまたはアドレス指定されたアプリケーションサーバは、エンドデバイスとのセキュアな通信のために1つまたは複数のセッションキーを要求し得る。この手順の一部として、図2の下部に示すように、エンドデバイスとネットワークサーバまたはアプリケーションサーバとの間の通信をセキュアにするためのセッションキーがそれぞれ、更なるプロセスにおいて生成される。

【0040】

したがって、セキュアキー管理デバイスSKMDの処理コンポーネントPCは、セキュアインターフェースI／Fを介して、一意識別子S／Nおよびセッション情報SIDを含む第1のリクエストREQ1を受信し得る。リクエストREQ1は、以下により詳細に説明するように、ネットワークサーバまたはアプリケーションサーバにセッションキーを提供するための対応する参加リクエストを受信した参加サーバから出され得る。第1のリクエストREQ1に応答して、処理コンポーネントPCはセキュアストレージコンポーネントSSCからマスターキーKaを取得する。次に、一意識別子S／N、セッション情報SID、およびマスターキーKaに基づいて、処理コンポーネントPCはエンドデバイスに固有の1つまたは複数のセッションキーSKeyを生成する。このキーは、第1のレスポンスRSP1の一部として、セキュアインターフェースI／Fを介して要求側エンティティに返される。特に、処理コンポーネントPCはレスポンスRSP1を参加サーバに返す

10

20

30

40

50

ことができ、次に参加サーバはセッションキー $SKey$ を要求側エンティティ（エンドデバイスと通信するネットワークサーバやアプリケーションサーバなど）に提供する。

【0041】

マスターキー Ka がセキュアキー管理デバイス $SKMD$ から決して離れることがないという事実に注目する。更に、事前登録時にエンドデバイスに提供されるルートキー $RKey$ は、セキュアインターフェース I/F を介してセッションキーを要求するエンティティに提供されない。したがって、参加サーバは、基盤となるマスターキーまたはルートキーの知識を得ることはない。そのため、参加サーバが、例えばハッキングされて侵害された場合でも、潜在的な侵入者は、エンドデバイスが使用する秘密マスターキー Ka またはルートキー $RKey$ に関するいかなる情報も得ることはできない。

10

【0042】

本発明の更なる実施形態をより詳細に説明する前に、まず、図3および図4に関して、リモートセンシングアプリケーションで使用する例示的な WAN の一般的な動作について以下に説明する。

【0043】

図3は、 $LoRaWAN$ ベースのシステムの参加エンティティの各々を示している。プロセス全体のワークフローについては、以下のセクションでも説明する。このセクションでは、この図とリストされているワークフローの両方は、 $LoRaWAN$ 仕様バージョン 1.1 に従って指定されている。この内容は本明細書に含まれている。

【0044】

図3のシステムは、エンドデバイス ED と、ネットワークサーバ NS と、アプリケーションサーバ AS と、アプリケーション App と、参加サーバ JS とを備えている。わかりやすくするために、図3には、これらのエンティティのうちの1つだけを示している。しかし、実際の実装では、説明する各エンティティの多くのインスタンスが存在する可能性がある。

20

【0045】

エンドデバイス ED は、 $LoRaWAN$ 通信ネットワークを介してデータを転送できる $LoRaWAN$ 通信インターフェースを有するデバイスである。ネットワークサーバ NS は、 $LoRaWAN$ 通信プロトコルを介して転送されるエンドデバイス ED からのデータパケットをリッスンする $LoRaWAN$ 通信ネットワークプロバイダサーバである。ネットワークサーバ NS は、任意のデータパケットを受信すると、そこに含まれる $LoRaWAN$ アプリケーションデータペイロードをアプリケーションサーバ AS に更に転送する。アプリケーションサーバ AS は、ネットワークサーバ NS からアプリケーションレベルのデータを取得し、次にデータペイロードをエンドアプリケーション App に更に転送するサーバであり、このエンドアプリケーション App から、データがモニタリングされるか、制御されるか、または他の方法で消費される。例えば、アプリケーション App は、エネルギー分配ネットワークの動作状態をモニタリングするモニタリングアプリケーションであるか、またはエンドデバイスとして機能する多数のスマートメーターをクエリする課金アプリケーションであり得る。

30

【0046】

参加サーバ JS は、従来、ネットワークセッションキーの配布、すなわち、1つまたは複数のネットワークサーバへの「ネットワークレベル」セッションキーのセットの配布、および1つまたは複数のアプリケーションサーバ AS への、「アプリケーションセッションキー」とも呼ばれ、 $LoRaWAN$ 仕様では「 $AppKey$ 」と参照される「アプリケーションレベル」キーの配布を管理するキー管理サーバである。

40

【0047】

このために、従来のセットアップでは、参加サーバ JS は、1つまたは複数のルートキー、すなわち、初期キーまたはベースキーを保存する。 $LoRaWAN$ 仕様バージョン 1.1 で使用される初期キーは、ネットワークルートキー ($NwkKey$) とアプリケーションキー ($AppKey$) であり、これらは $AES128$ ビットキーである。これらのキ

50

ーを更に使用して、WANのネットワーク層とアプリケーション層の両方で、サイバー攻撃からLoRaWANトラフィックの転送をセキュアにするために使用されるセッションキーが派生される。LoRaWAN仕様バージョン1.0によれば、すべてのセッションキーを派生させるために、単一のルートキー、すなわち、アプリケーションキー（AppKey）のみが使用されるという事実に注目する。

【0048】

標準によれば、LoRaWAN通信インフラストラクチャへのLoRaWAN参加手順は、「オーバジエアーアクティベーション」（OTAA）または「アクティベーションバイパーソナライゼーション」（ABP）と呼ばれる2つの方法のいずれかで実行できる。対応する手順については、LoRaWAN 1.1仕様2、2017、LoRa Alliance, Inc. のセクション6.2および6.3で説明している。この内容は、参照により含まれている。

【0049】

デバイスのアクティベーション中に、エンドデバイスEDを次のデータ項目で初期化する必要がある。

【0050】

a. JoinEUI：これは、エンドデバイスEDが適切な参加サーバJSと通信できるように、参加サーバJSのIEEE EUI64アドレスの形式の識別子である。これは、OTAAを選択したい場合にのみ、各エンドデバイスED内に保存する必要がある。

【0051】

b. DevEUI：これは、LoRaWAN通信トラフィックをリッスンしているネットワークサーバNSが各エンドデバイスEDを正しく識別できるように、各エンドデバイスEDのIEEE EUI64アドレスの形式の識別子である。このデータは、エンドデバイスEDがOTAAを選択したい場合に必要であるが、ABPでは必須ではない。ただし、このデータは各エンドデバイスED内に保存することが推奨される。

【0052】

・NwkKey：これは、「ネットワークセッションキー」、すなわち、ネットワークレベルセッションキーのセット、例えば、LoRaWAN標準バージョン1.1におけるFNwkSIntKey、SNwkSIntKey、およびNwkSEncKeyを派生させるために使用されるキーである。これらのネットワークレベルセッションキーは、ネットワーク層でのLoRaWAN通信トラフィック、すなわち、エンドデバイスEDとネットワークサーバNSとの間の通信を保護するために使用される。このデータは、ABPモードで動作するときには、各エンドデバイスED内に保存する必要はない。

【0053】

・AppKey：これは、「アプリケーションセッションキー」とも呼ばれる「アプリケーションレベル」セッションキー（例えば、LoRaWAN標準のバージョン1.1におけるAppSKey）を派生させるためのキーである。アプリケーションセッションキーは、アプリケーション層でのLoRaWAN通信トラフィック、すなわち、OSIアプリケーション層7でのネットワークサーバを介したエンドデバイスEDとアプリケーションサーバASとの間の通信を保護するために使用される。このデータは、エンドデバイスEDをABPモードで動作するときには、エンドデバイスED内に保存する必要はない。

【0054】

図4は、LoRaWANベースの通信システムの以下に示す参加エンティティの各々に配置されたセッションキーに支援されるこのセキュアな通信のフローを示している。

【0055】

LoRaWAN通信ネットワークでは、エンドデバイスEDは、ルートネットワークキー（すなわち、NwkKey）から派生する「ネットワークセッションキー」（すなわち、転送ネットワークセッション整合性キーFNwkSIntKey、サービングネットワークセッション整合性キーSNwkSIntKey、およびネットワークセッション暗号化キーNwkSEncKey）に支援されて、ネットワークサーバNSとセキュアに通信

10

20

30

40

50

する。したがって、エンドデバイスEDは、例えば、MACペイロードおよびコマンドの暗号化により、LoRaWANデータをネットワークサーバNSにセキュアに送信する。同様に、エンドデバイスEDとアプリケーションサーバASとの間で交換されるアプリケーションレベルデータが暗号化されている。つまり、エンドデバイスEDは、「ネットワークセッションキー」に支援されてネットワーク層と、「アプリケーションセッションキー」に支援されてアプリケーション層の両方での暗号動作を実行する。

【0056】

LoRaWANデータを受信すると、ネットワークサーバNSは更に、データをアプリケーションサーバASにセキュアに送信する。なお、このステップでは、LoRaWANデータのアプリケーションペイロードセグメントは、各エンドデバイスEDによって「アプリケーションセッションキー」に支援されてすでに暗号化されているため、ネットワークサーバNSは暗号動作を実行する必要がない。したがって、ネットワークサーバNSは単にそのLoRaWANデータを、LoRaWANデータのインダイジェストなどの更なる処理のためにアプリケーションサーバASに転送し、モニタリングかまたは制御のいずれかのために、例えば、セキュアな通信プロトコルなどの通信プロトコルによってLoRaWANデータをエンドアプリケーションAPPに送信することができる。

【0057】

図4にも示すように、LoRaWANは複数の物理ネットワークにまたがる場合があることに留意されたい。例えば、第1の物理ネットワークPHY1はLoRa低電力ワイヤレスアクセスネットワークであり、第2の物理ネットワークPHY2は有線コアネットワークである場合がある。図4に示す実施例では、ネットワークサーバNSは、第1の物理ネットワークPHY1と第2の物理ネットワークPHY2との間のゲートウェイとしても機能する。ただし、この機能は、ネットワークサーバが、第1の物理ネットワークPHY1または第2の物理ネットワークPHY2のうちのいずれか一方に配置された状態で、異なるデバイスに実装されることも可能である。

【0058】

LoRaWAN標準（仕様のバージョン1.0と1.1の両方を含む）は、LoRaWAN通信トラフィックをセキュアにするために後で使用される、オーバージエアーアクティベーション（OTAA）中にセッションキー — 「ネットワークセッションキー、すなわち、ネットワークレベルセッションキーのセット」 および「アプリケーションセッションキー」を生成するために使用されるルートキーのセット、すなわち、NwkKeyおよびAppKeyを初期化してセキュアに管理する方法を規定していない。また、この標準では、「ネットワークセッションキー」および「アプリケーションセッションキー」をセキュアに取り扱うためのメカニズムも規定していない。したがって、上記のキーをセキュアに管理するためのセキュアワークフローが規定されていない。セキュアエレメント（SE）およびハードウェアセキュリティモジュール（HSM）を使用してセキュアに保存することだけが規定されている。

【0059】

しかし、発明者によって認識されているように、それらの管理のためのワークフロー全体、すなわち、これらのルートキーおよびセッションキーの生成、転送、ならびに更新は、システムのセキュリティ全体に重要である。これらのステップを実行する際のワークフローが脆弱であると、LoRaWANベースのシステムのサイバー脆弱性につながる可能性がある。これらのルートキーの初期セットのセキュアな管理は、システムのサイバーセキュリティ管理全体に最も重要な側面である。したがって、本開示は、これらのルートキー、ならびに派生した「ネットワークセッションキー」および「アプリケーションセッションキー」をセキュアに管理するための方法およびシステムを提供する。

【0060】

次のセクションでは、図5および図6に関して、LoRaWANネットワークのコンテキストにおける特定の実施例に、開示するソリューションを適用する方法について詳述する。この開示するソリューションは、セキュアキー管理デバイスSKMDと呼ばれる別の

10

20

30

40

50

エンティティをLoRaシステムに導入することで、上記の課題のうちの少なくともいくつかに取り組む。このエンティティは、ルートキー（すなわち、NwkKeyおよびAppKey）、ならびにその派生セッションキー、つまり、ネットワークセッションキー（すなわち、FNwkSIntKey、SNwkSIntKey、およびNwkSEncKey）、およびアプリケーションセッションキー（すなわち、AppKey）のセキュアな生成と転送を処理する。

【0061】

図5は、システムのセットアップと、ステップA～Gで構成される、説明するワークフローの両方を概略的に示している。

【0062】

これらの以下のシーケンスステップでは、キーが生成されてから使用したキーが送信される。その目的を成功裏に達成するためのこれらのステップの前提条件、したがって、必要条件は、エンドデバイスEDごとに参加サーバJS内でセキュアに事前に生成されて、事前に保存されている必要のある「JoinNonce」、「NetID」、および「DevNonce」の初期化である。

【0063】

ステップA～Fは、セキュアキー管理デバイスSKMDに関する図5に関して以下に説明されている。セキュアキー管理デバイスSKMDは、LoRaWANシステムの他の参加者から物理的に分離している別個のエンティティである。図5に示すように、以下にリストする個々のステップA～Gは、セキュアキー管理デバイスSKMDの処理コンポーネントPCによって実行される。ただし、ステップBおよびEは除く。

【0064】

ステップA：起動時に、セキュアキー管理デバイスSKMDはマスターキーKaを生成して保存する。K1はマスターキーKaの第1のバージョンを表す。第1のマスターキーK1は、対応するバージョンデータKnとともに、例えば、セキュアキー管理デバイスSKMDのハードウェアセキュリティモジュールに保存され得る。このキーK1は更に、以下に更に説明するようにエンドデバイスEDごとに異なるルートキー（すなわち、NwkKeyおよびAppKey）の生成に使用される。この第1のマスターキーK1を一定回数反復して使用した後、セキュアキー管理デバイスSKMDは第2のマスターキーK2を生成する。このマスターキーK2も、対応するバージョンデータKnとともに、セキュアキー管理デバイスSKMDによって保存され、この傾向は継続する。この特定回数は、ローカルセキュリティポリシーによって決定することができる。当然ながら、他のセキュリティ違反の侵入が検出された後など、手動で新しいマスターキーの生成を強制することも可能である。

【0065】

ステップB：セキュアキー管理デバイスSKMDには、各エンドデバイスEDのシリアルナンバーを入力することができるインターフェースがある。これは、人間または、任意のコンピュータ化されたファイルから各エンドデバイスEDのこれらの事前定義されたシリアルナンバーを読み取り、セキュアキー管理デバイスSKMD内にそれらを入力するコンピュータ化されたスクリプトなどの任意の方法で入力できる。

【0066】

ステップC：新しいエンドデバイスEDごとに、NwkKeyが、また、LoRaWAN仕様バージョン1.1に準拠したエンドデバイスEDに対しては、AppKeyも、それらのシリアルナンバーと現在アクティブなマスターキーKaとに基づいて生成され、エンドデバイスEDに保存される。例えば、NwkKeyおよびAppKeyは、エンドデバイスEDのセキュアエレメントに保存され得る。マスターキーKa自体もそのバージョンデータKnもエンドデバイスEDには保存されないことに留意されたい。

【0067】

暗号キー生成関数で使用される入力パラメータは次のとおりである。

－ アクティブマスターキーKa

10

20

30

40

50

－ 各エンドデバイスのシリアルナンバー。一意に区別される各エンドデバイス E D の各々のデバイス識別子 S / N として機能する。

【0068】

したがって、各エンドデバイス E D について、キー生成関数は次のようになる。

$NwkKey = F_A(Ka, S/N)$

$AppKey = F_B(Ka, S/N)$ 、

ここで、 F_A および F_B は、別々に選択された任意の最新式の暗号関数である。正確な関数は、一般的に、適用される標準に依存し、本開示によって限定されるものではない。

【0069】

したがって、ステップ C を実行した後、新しいエンドデバイス E D には、異なる、一意の $NwkKey$ および $AppKey$ が含まれる。

【0070】

ステップ D : 参加サーバ J S には、インターフェースもある。このインターフェースを介して、一意識別子 S / N として機能する各エンドデバイスのシリアルナンバー、WAN 内のエンドデバイス E D のエンドデバイスアドレス識別子 DevEUI、およびステップ C で $NwkKey$ および $AppKey$ を生成するために使用したマスターキー Ka のバージョンデータ Kn (マスターキー Ka 自体ではない) を入力することができる。ここでも、これは、人間または、任意のコンピュータ化されたファイルから各エンドデバイス E D のこれらの事前定義されたシリアルナンバーを読み取り、参加サーバ J S 内にそれらを入力するコンピュータ化されたスクリプトなどの任意の方法で入力できる。

【0071】

ステップ E : 参加およびアクティベーションプロセス中に、参加サーバ J S はセキュアキー管理デバイス SKMD からネットワークセッションキー (すなわち、 $FNwkSIntKey$ 、 $SNwkSIntKey$ 、および $NwkSEncKey$)、およびアプリケーションセッションキー (すなわち、 $AppSKey$) を要求する。このために、参加サーバ J S は、Join Request 内で参加サーバ J S に提供されたエンドデバイス E D の DevEUI を使用して、エンドデバイス E D のシリアルナンバーと、ステップ D において参加サーバ J S に提供されたエンドデバイスのルートキー $NwkKey$ および $AppKey$ の生成に使用されたマスターキー Ka のバージョンデータ Kn とを見出す。次に、参加サーバ J S は、LoRaWAN 標準で説明されているように、エンドデバイス E D の一意識別子 S / N として機能するシリアルナンバー、マスターキー Ka のバージョンデータ Kn、参加ノンス (「JoinNonce」)、ネットワーク id (「NetID」)、およびデバイスノンス (「DevNonce」) を含む Session Key Request を提供する。Session Key Request の転送は、任意の最新式のセキュアな通信プロトコルによって実行される。

【0072】

ステップ F : ステップ E からそれぞれの値を得ると、セキュアキー管理デバイス SKMD は、次のステップを使用した、対応する LoRaWAN 標準で規定されたキー生成アルゴリズムを使用して、それぞれのエンドデバイス E D のネットワークセッションキー (すなわち、 $FNwkSIntKey$ 、 $SNwkSIntKey$ 、および $NwkSEncKey$) およびアプリケーションセッションキー (すなわち、 $AppSKey$) を生成する。

【0073】

－ 参加およびアクティベーションプロセスで説明されているエンドデバイス E D のステップ E からのデータを用いる F_A および F_B を使用した $NwkKey$ および $AppKey$ の生成。

【0074】

－ 「JoinNonce」、「NetID」、「DevNonce」、 $NwkKey$ 、および $AppKey$ に基づく $FNwkSIntKey$ 、 $SNwkSIntKey$ 、 $NwkSEncKey$ 、ならびに $AppSKey$ の生成。

【0075】

10

20

30

40

50

NwkKeyおよびAppKey、ならびにFNwkSIntKey、SNwkSIntKey、NwkSEncKey、およびAppSKeyを生成する上記のステップは、オンザフライで実行することができ、すなわち、生成されたキーをセキュアキー管理デバイスSKMDに保存することなく実行することができることに留意されたい。これにより、システムセキュリティが更に向上される。

【0076】

ステップG：セキュアキー管理デバイスSKMDは、SessionKeyResponseの一部として、参加およびアクティベーションプロセスでエンドデバイスED用にステップDで生成されたセッションキーを、参加サーバJSにセキュアに送る。データは、任意の最新式のセキュアな通信プロトコルを使用して送信される。参加サーバJSは、必要に応じて、JoinAcceptの一部として、これらのセッションキーを1つまたは複数の要求側ネットワークサーバNSおよび／またはアプリケーションサーバASに転送する。参加サーバJSは、これらのセッションキーのローカルコピーを保持しない。

10

【0077】

図5に更に示すように、ステップB、C、およびDは、エンドデバイスED、セキュアキー管理デバイスSKMD、および／または参加サーバJSとの通信用に1つまたはいくつかの対応するインターフェースを有する、デバイス製造業者OEMの登録デバイスRDによって実行され得るか、またはその制御下で実行され得る。一実施形態では、これらのインターフェースは、LoRaWANネットワークアドレス空間および／または通信プロトコルの外部にあるセキュアなマシンツーマシン(M2M)インターフェースである。

20

【0078】

図6は、LoRaWANでのセキュアキー管理デバイスSKMDの初期化と、エンドデバイスEDの事前登録と参加の完全なフローを詳述した例示的なシーケンス図を示す。参照しやすくするために、開示された手順の更なるステップとともに、上記のステップA～Fを図6に再掲する。

【0079】

上記の方法は、部分的または全体としてソフトウェアで実装され得る。このために、データストレージデバイスは、命令を保存し得る。この命令は、セキュアキー管理デバイスSKMDの処理コンポーネントPCなど、ネットワーク化されたコンピューティングデバイスの少なくとも1つの処理デバイスで実行されると、コンピューティングデバイスがその役割を有する方法のそれらの部分を実装するステップ、例えば、セキュアキー管理デバイスSKMD、参加サーバJS、登録デバイスRD、エンドデバイスEDなどによって実行されるステップを実行する。

30

【0080】

上記の図1、図2、図5、および図6に示されている実施形態は、改良されたデバイス、システム、および方法の例示的な実施形態を示しており、したがって、改良されたデバイス、システム、および方法によるすべての実施形態の完全なリストを構成するものではない。実際のデバイス、システム、および方法は、例えば、配置、デバイス、交換されるメッセージ、およびパラメータに関して、示されている実施形態とは異なる場合がある。

【0081】

参照符号

APP エンドアプリケーション

AS アプリケーションサーバ

ED エンドデバイス

I/F セキュアインターフェース

JS 参加サーバ

NS ネットワークサーバ

OEM デバイス製造業者

PC 処理コンポーネント

SKMD セキュアキー管理デバイス

40

50

SSC セキュアストレージコンポーネント
AppKey アプリケーションルートキー
AppSKey アプリケーションセッションキー
DevEUI エンドデバイスアドレス識別子
Ka (アクティブ) マスターキー
Kn (マスターキーの) バージョンデータ
NwkKey ネットワークルートキー
NwkSEncKey、FNwkSIntKey、SNwkSIntKey ネットワークセッションキー
RKey ルートキー
REQ1 第1のリクエスト
RSP1 第1のレスポンス
SID セッション情報
SKey セッションキー
S/N (エンドデバイスの) 一意識別子

【図面】

【図1】

【図2】

Fig. 1

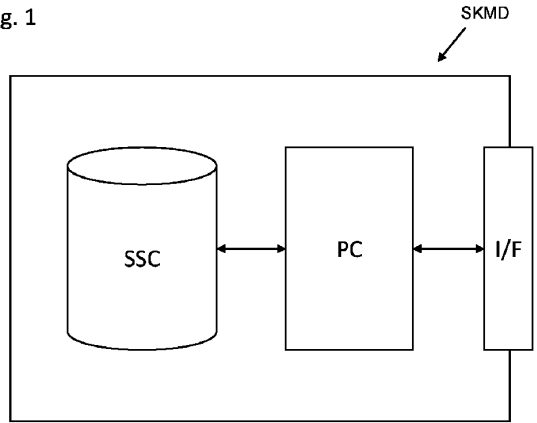
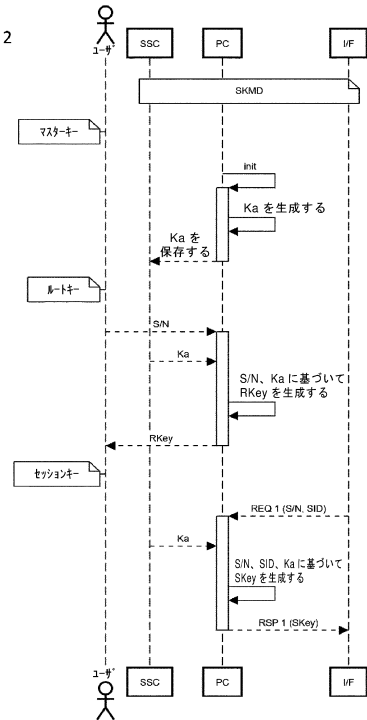


Fig. 2



10

20

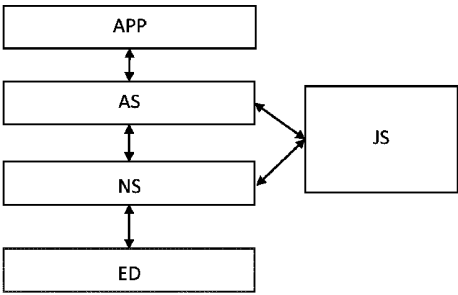
30

40

50

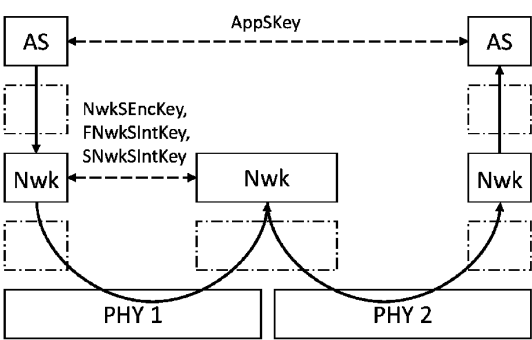
【図 3】

Fig. 3



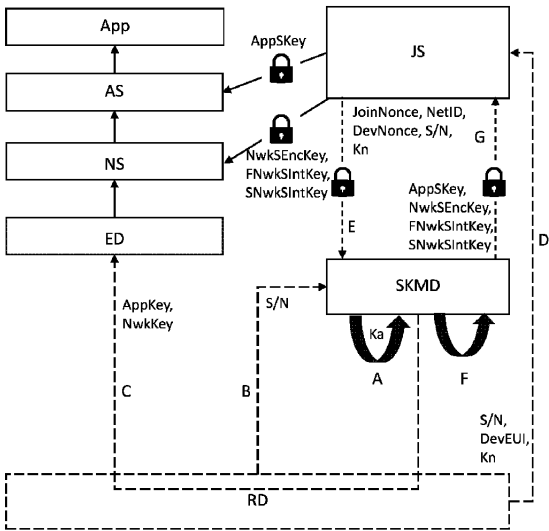
【図 4】

Fig. 4

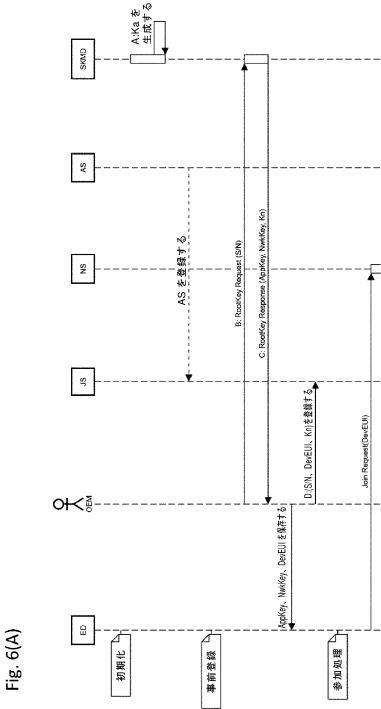


【図 5】

Fig. 5



【図 6 (A)】



10

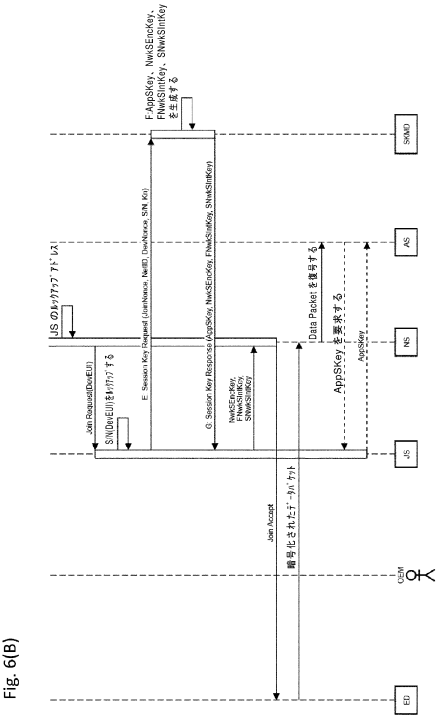
20

30

40

50

【図 6 (B)】



10

20

30

40

50

フロントページの続き

(72)発明者 オポチンスキ, パベウ

ポーランド、31-340 マウオポルスカ、クラクフ、ヘウモンスキエゴ、130・エム/8

審査官 青木 重徳

(56)参考文献 特開2020-028099 (JP, A)

特表2020-510334 (JP, A)

米国特許出願公開第2020/0177573 (US, A1)

国際公開第2019/001713 (WO, A1)

欧州特許出願公開第03306970 (EP, A1)

Sarra Naoui et al., Trusted Third Party Based Key Management for enhancing LoRaWAN Security, 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications, 米国, IEEE, 2017年10月30日, pp. 1306-1313

(58)調査した分野 (Int.Cl., DB名)

H04L 9/08

G06F 21/60

JSTPlus/JMEDPlus/JST7580 (JDreamIII)

IEEE Xplore

THE ACM DIGITAL LIBRARY