(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2012-249293
(P2012-249293A)
(43)公開日　平成24年12月13日(2012.12.13)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601D	5J104

審査請求 有　請求項の数 21　ＯＬ　（全 13 頁）

(21)出願番号　特願2012-121019 (P2012-121019)
(22)出願日　平成24年5月28日 (2012.5.28)
(31)優先権主張番号　10-2011-0051669
(32)優先日　平成23年5月30日 (2011.5.30)
(33)優先権主張国　韓国 (KR)

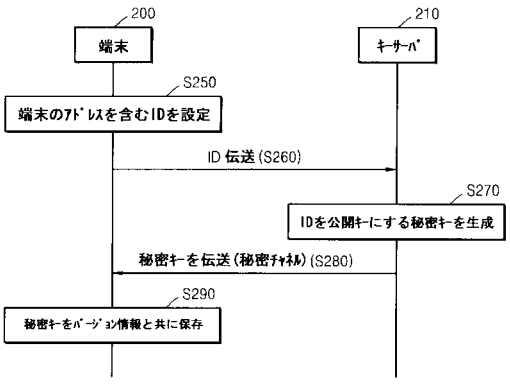
（特許庁注：以下のものは登録商標）
１．フロッピー

(71)出願人　510294195
サムソン　エスディーエス　カンパニー　リミテッド
大韓民国　ソウル　カンナム－ク　ヨクサム－２ドン　７０７－１９　イロック　ビルディング
(74)代理人　100117787
弁理士　勝沼　宏仁
(74)代理人　100107582
弁理士　関根　毅
(74)代理人　100146123
弁理士　木本　大介

最終頁に続く

(54)【発明の名称】ＩＤ基盤の暗号化方法及びその装置

(57)【要約】
【課題】ＩＤ基盤の暗号化方法及びその装置を提供する。
【解決手段】端末は、ＭＡＣアドレスを利用して生成したＥＵＩ－６４アドレス、１６ビット・ショートアドレス、または１６ビット・ショートアドレスと、端末が属したルータのプレフィックスとを含んだアドレスとバージョン情報とを含むＩＤを生成してキーサーバに伝送した後、そのＩＤを公開キーにする秘密キーを受信する、ＩＤ基盤の暗号化方法及びその装置である。
【選択図】図２



【特許請求の範囲】
【請求項１】
端末のアドレスを含むＩＤを生成する段階と、
キーサーバから、前記ＩＤを公開キーにする秘密キーを伝送される段階と、を含むことを特徴とするＩＤ基盤の暗号化方法。
【請求項２】
端末のアドレスを含むＩＤを前記端末から受信する段階と、
前記ＩＤを公開キーにする秘密キーを生成する段階と、
前記秘密キーを前記端末に伝送する段階と、を含むことを特徴とするＩＤ基盤の暗号化方法。
【請求項３】
前記端末のアドレスは、
端末のＭＡＣアドレスを利用して生成したＥＵＩ－６４アドレス、１６ビット・ショートアドレス、または１６ビット・ショートアドレスと、前記端末が属したルータのプレフィックスとを含んだアドレスであることを特徴とする請求項１または請求項２に記載のＩＤ基盤の暗号化方法。
【請求項４】
前記１６ビット・ショートアドレスは、端末のＭＡＣアドレスやＥＵＩ－６４アドレスと、バージョン情報及びインデックスとを入力とする衝突回避ハッシュ関数の１６ビット出力値であり、
前記インデックスは、前記衝突回避ハッシュ関数の１６ビット出力値が、他の端末の１６ビット・ショートアドレスと衝突する場合、その衝突を防止するために変更される値であることを特徴とする請求項３に記載のＩＤ基盤の暗号化方法。
【請求項５】
前記ＩＤは、日付形式であるか、あるいは既設定の形式によって更新されるバージョン情報を、前記端末のアドレスと共に含むことを特徴とする請求項１または請求項２に記載のＩＤ基盤の暗号化方法。
【請求項６】
端末のアドレスとバージョン情報とを含んだＩＤを公開キーとして使用するＩＤ基盤暗号化のキー更新方法において、
前記端末のアドレスに新たなバージョン情報を含んだ新たなＩＤと、以前バージョン情報とをキーサーバに伝送する段階と、
前記キーサーバから、前記新たなＩＤを公開キーにする新たな秘密キーを含んだデータを受信するが、前記データは、前記以前バージョン情報を含む以前ＩＤを利用して暗号化されたまま受信される段階と、
以前ＩＤに係わる秘密キーで前記データを復号化し、前記新たな秘密キーを確保する段階と、を含むことを特徴とするＩＤ基盤暗号化のキー更新方法。
【請求項７】
端末のアドレスとバージョン情報とを含んだＩＤを公開キーとして使用するＩＤ基盤暗号化のキー更新方法において、
端末から前記端末のアドレスと、新たなバージョン情報とを含んだ新たなＩＤ、及び以前バージョン情報を受信する段階と、
前記新たなＩＤを公開キーにする新たな秘密キーを生成する段階と、
前記端末のアドレスと、前記以前バージョン情報とを含んだ以前ＩＤを利用し、前記新たな秘密キーを暗号化する段階と、
前記暗号化された秘密キー情報を前記端末に伝送する段階と、を含むことを特徴とするＩＤ基盤暗号化のキー更新方法。
【請求項８】
前記新たなＩＤをキーサーバに伝送する段階は、
一定周期に達するか、あるいはキーの使用回数が既設定の臨界値に達した場合、前記新

たなＩＤを前記キーサーバに伝送する段階を含むことを特徴とする請求項６に記載のＩＤ基盤暗号化のキー更新方法。
【請求項９】
前記端末のアドレスは、
端末のＭＡＣアドレスを利用して生成したＥＵＩ－６４アドレス、１６ビット・ショートアドレス、または１６ビット・ショートアドレスと、前記端末が属したルータのプレフィックスとを含んだアドレスであることを特徴とする請求項６または請求項７に記載のＩＤ基盤暗号化のキー更新方法。
【請求項１０】
端末のアドレスとバージョン情報とを含んだＩＤを公開キーとして使用するＩＤ基盤暗号化を利用した通信方法において、
ＩＤ基盤暗号化が適用されたパケットを生成する段階と、
前記パケットを受信端末に伝送する段階と、を含むが、
前記ＩＤ基盤暗号化が適用されたパケットは、
前記受信端末のアドレスを含む受信者アドレスフィールドと、
ＩＤ基盤暗号化の適用いかんを示すフラグ情報とバージョン情報とを含む暗号ヘッダフィールドと、
前記受信端末のアドレス並びに前記バージョン情報を含んだＩＤを利用して暗号化されたデータを含むペイロードフィールドと、を含むことを特徴とするＩＤ基盤暗号化を利用した通信方法。
【請求項１１】
前記受信者アドレスフィールドは、
受信端末のＥＵＩ－６４アドレス、１６ビット・ショートアドレス、または１６ビット・ショートアドレスと、前記端末が属したルータのプレフィックスとを含んだアドレスであることを特徴とする請求項１０に記載のＩＤ基盤暗号化を利用した通信方法。
【請求項１２】
前記受信者アドレスフィールドは、端末のＭＡＣアドレスやＥＵＩ－６４アドレスと、バージョン情報及びインデックスとを入力とする衝突回避ハッシュ関数の１６ビット出力値を前記受信者端末のアドレスとして含み、
前記暗号ヘッダフィールドは、前記インデックスをさらに含むことを特徴とする請求項１０に記載のＩＤ基盤暗号化を利用した通信方法。
【請求項１３】
端末のアドレスとバージョン情報とを含んだＩＤを公開キーとして使用するＩＤ基盤暗号化を利用した通信方法において、
送信端末は、受信端末のアドレス及びバージョン情報を含むＩＤを基に暗号化したデータを生成する段階と、
前記送信端末は、前記受信端末のアドレス及びバージョン情報と、前記暗号化したデータとを含んだパケットを生成する段階と、
前記送信端末は、前記パケットを受信端末に伝送する段階と、を含むことを特徴とするＩＤ基盤暗号化を利用した通信方法。
【請求項１４】
前記送信端末は、前記バージョン情報を前記受信端末または前記受信端末が位置したルータの周期的な広告メッセージを介して把握したり、あるいは日付形態のバージョン情報を自体生成することを特徴とする請求項１３に記載のＩＤ基盤暗号化を利用した通信方法。
【請求項１５】
受信端末は、前記送信端末から前記パケットを受信する段階と、
前記受信端末は、前記パケットに含まれた受信端末のアドレス及びバージョン情報を基に、既保存の対応する秘密キーを把握し、前記秘密キーを利用し、前記パケットの暗号化されたデータを復号化する段階と、を含むことを特徴とする請求項１３に記載のＩＤ基盤

暗号化を利用した通信方法。
【請求項１６】
端末のアドレスとバージョン情報とを含んだＩＤを公開キーとして使用するＩＤ基盤暗号化を利用した通信方法において、
ＩＤ基盤暗号化を利用して署名したパケットを生成する段階と、
前記パケットを受信端末に伝送する段階と、を含むが、
前記ＩＤ基盤暗号化を利用して署名したパケットは、
送信端末のアドレスを含む送信者アドレスフィールドと、
ＩＤ基盤暗号化を利用した署名の適用いかんを示すフラグ情報とバージョン情報とを含む暗号ヘッダフィールドと、
前記送信端末のアドレス並びに前記バージョン情報を含んだＩＤを利用して暗号化された署名をペイロードフィールドに追加する署名フィールドと、を含むことを特徴とするＩＤ基盤暗号化を利用した通信方法。
【請求項１７】
前記送信者アドレスフィールドは、
送信端末のＥＵＩ－６４アドレス、１６ビット・ショートアドレス、または１６ビット・ショートアドレスと、前記送信端末が属したルータのプレフィックスとを含んだアドレスであることを特徴とする請求項１６に記載のＩＤ基盤暗号化を利用した通信方法。
【請求項１８】
前記送信者アドレスフィールドは、送信端末のＭＡＣアドレスやＥＵＩ－６４アドレスと、バージョン情報及びインデックスとを入力とする衝突回避ハッシュ関数の１６ビット出力値を、前記送信者端末のアドレスとして含み、
前記暗号ヘッダフィールドは、前記インデックスをさらに含むことを特徴とする請求項１７に記載のＩＤ基盤暗号化を利用した通信方法。
【請求項１９】
端末のアドレスとバージョン情報とを含んだＩＤを公開キーとして使用するＩＤ基盤暗号化を利用した通信方法において、
送信端末は、前記送信端末のＩＤに対応する秘密キーを利用して署名を生成する段階と、
前記送信端末は、前記送信端末のアドレス及びバージョン情報と、前記署名とを含んだパケットを生成する段階と、
前記送信端末は、前記パケットを受信端末に伝送する段階と、を含むことを特徴とするＩＤ基盤暗号化を利用した通信方法。
【請求項２０】
前記受信端末は、前記送信端末から前記パケットを受信する段階と、
前記受信端末は、前記パケットに含まれた送信端末のアドレス及びバージョン情報を基に、前記パケットに保存された署名を検証する段階と、を含むことを特徴とする請求項１９に記載のＩＤ基盤暗号化を利用した通信方法。
【請求項２１】
請求項１ないし請求項２０のうち、いずれか１項に記載の方法を遂行するためのプログラムを記録したコンピュータで読み取り可能な記録媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ＩＤ基盤の暗号化方法及びその装置に係り、さらに詳細には、端末のアドレスをＩＤとする暗号化方法及びその装置と、その暗号化方法を利用した通信方法とに関する。
【背景技術】
【０００２】
事物通信（Ｍ２Ｍ：machine to machine）環境の到来によって、小型無線端末の数が幾

何級数的に増えており、これにより、人と人との通信、人と機器との通信、機器と機器との通信に対する保安問題も増加している。しかし、既存の公開キー暗号体系は、幾何級数的に増える端末の数に比例して増加するキー管理及び認証サーバ負荷の問題で、現実的に適用が不可能である。特に、事物通信の主な比重を占める機器間通信の場合、既存の秘密キー基盤暗号体系を適用するには、各小型端末のキー管理負担が増加し、公開キー暗号体系を使用する場合、機器の数に比例するキー管理及び機器間通信時のサーバ連結によって、現実的使用が不可能である。

【発明の概要】

【発明が解決しようとする課題】

【０００３】

本発明がなそうとする技術的課題は、幾何級数的に増える端末のキー管理問題を解決するＩＤ基盤の暗号化方法及びその装置を提供するところにある。

【課題を解決するための手段】

【０００４】

前記の技術的課題を達成するための本発明によるＩＤ基盤の暗号化方法の一例は、端末のアドレスを含むＩＤを生成する段階と、キーサーバから前記ＩＤを公開キーにする秘密キーを伝送される段階と、を含む。

【０００５】

前記の技術的課題を達成するための本発明によるＩＤ基盤の暗号化方法の他の一例は、端末のアドレスを含むＩＤを前記端末から受信する段階と、前記ＩＤを公開キーにする秘密キーを生成する段階と、前記秘密キーを前記端末に伝送する段階と、を含む。

【０００６】

前記の技術的課題を達成するための本発明によるＩＤ基盤暗号化のキー更新方法の一例は、端末のアドレスとバージョン情報とを含んだＩＤを公開キーとして使用するＩＤ基盤暗号化のキー更新方法において、前記端末のアドレスに新たなバージョン情報を含んだ新たなＩＤと、以前バージョン情報とをキーサーバに伝送する段階と、前記キーサーバから、前記新たなＩＤを公開キーにする新たな秘密キーを含んだデータを受信するが、前記データは、前記以前バージョン情報を含む以前ＩＤを利用して暗号化されたまま受信される段階と、以前ＩＤに係わる秘密キーで前記データを復号化し、前記新たな秘密キーを確保する段階と、を含む。

【０００７】

前記の技術的課題を達成するための本発明によるＩＤ基盤暗号化のキー更新方法の他の一例は、端末のアドレスとバージョン情報とを含んだＩＤを公開キーとして使用するＩＤ基盤暗号化のキー更新方法において、端末から前記端末のアドレスと、新たなバージョン情報とを含んだ新たなＩＤ、及び以前バージョン情報を受信する段階と、前記新たなＩＤを公開キーにする新たな秘密キーを生成する段階と、前記端末のアドレスと、前記以前バージョン情報とを含んだ以前ＩＤを利用し、前記新たな秘密キーを暗号化する段階と、前記暗号化された秘密キー情報を前記端末に伝送する段階と、を含む。

【０００８】

前記の技術的課題を達成するための本発明によるＩＤ基盤暗号化を利用した通信方法の一例は、端末のアドレスとバージョン情報とを含んだＩＤを公開キーとして使用するＩＤ基盤暗号化を利用した通信方法において、ＩＤ基盤暗号化が適用されたパケットを生成する段階と、前記パケットを受信端末に伝送する段階と、を含むが、前記ＩＤ基盤暗号化が適用されたパケットは、前記受信端末のアドレスを含む受信者アドレスフィールド；ＩＤ基盤暗号化の適用いかんを示すフラグ情報とバージョン情報とを含む暗号ヘッダフィールド；及び前記受信端末のアドレス並びに前記バージョン情報を含んだＩＤを利用して暗号化されたデータを含むペイロードフィールド；を含む。

【０００９】

前記の技術的課題を達成するための本発明によるＩＤ基盤暗号化を利用した通信方法の他の一例は、端末のアドレスとバージョン情報とを含んだＩＤを公開キーとして使用する

ＩＤ基盤暗号化を利用した通信方法において、送信端末は、受信端末のアドレス及びバージョン情報を含むＩＤを基に暗号化したデータを生成する段階と、前記送信端末は、前記受信端末のアドレス及びバージョン情報と、前記暗号化したデータとを含んだパケットを生成する段階と、前記送信端末は、前記パケットを受信端末に伝送する段階と、を含む。

【００１０】

前記の技術的課題を達成するための本発明によるＩＤ基盤暗号化を利用した署名方法の一例は、端末のアドレスとバージョン情報とを含んだＩＤを公開キーとして使用するＩＤ基盤暗号化を利用した通信方法において、ＩＤ基盤暗号化を利用して署名したパケットを生成する段階と、前記パケットを受信端末に伝送する段階と、を含むが、前記ＩＤ基盤暗号化を利用して署名したパケットは、送信端末のアドレスを含む送信者アドレスフィールド；ＩＤ基盤暗号化を利用した署名の適用いかんを示すフラグ情報とバージョン情報とを含む暗号ヘッダフィールド；及び前記送信端末のアドレス並びに前記バージョン情報を含んだＩＤを利用して暗号化された署名をペイロードフィールドに追加する署名フィールド；を含む。

【００１１】

前記の技術的課題を達成するための本発明によるＩＤ基盤暗号化を利用した署名方法の他の一例は、端末のアドレスとバージョン情報とを含んだＩＤを公開キーとして使用するＩＤ基盤暗号化を利用した通信方法において、送信端末は、前記送信端末のＩＤに対応する秘密キーを利用して署名を生成する段階と、前記送信端末は、前記送信端末のアドレス及びバージョン情報と、前記署名とを含んだパケットを生成する段階と、前記送信端末は、前記パケットを受信端末に伝送する段階と、を含む。

【発明の効果】

【００１２】

本発明によれば、既存の暗号体系が有しているキー管理の問題点を根本的に解決する。また、事物通信環境の基本的な特性である移動性（mobility）を支援し、既存のＩＤ基盤暗号方法の問題点を解決する。また本発明は、６ＬｏＷＰＡＮに適用する場合、既存暗号体系で、暗号化／復号化と署名／認証とのために、パケットに付加的に搭載していた公開キー情報などを付ける必要がなく、標準による６ＬｏＷＰＡＮパケットにすでに含まれているＩＰアドレスを利用して公開キー情報を得ることができ、帯域幅制約が深刻な６ＬｏＷＰＡＮで、効率的に暗号化された通信が可能である。

【図面の簡単な説明】

【００１３】

【図１】本発明によるＩＤ基盤の暗号化方法で、ＩＤとして使用する端末アドレスの一例を図示した図面である。

【図２】本発明によるＩＤ基盤の暗号化方法のキー設定方法の一例を図示した図面である。

【図３】本発明によるＩＤ基盤の暗号化方法のキー更新方法の一例を図示した図面である。

【図４】本発明によるＩＤ基盤の暗号化方法を適用したパケットの一例を図示した図面である。

【図５】本発明によるＩＤ基盤の暗号化方法を利用した通信方法の一例を図示した図面である。

【図６】本発明によるＩＤ基盤の暗号化方法を利用した署名方法の一例を図示し図面である。

【発明を実施するための形態】

【００１４】

以下、添付された図面を参照しつつ、本発明によるＩＤ基盤の暗号化方法及びその装置について詳細に説明する。

【００１５】

図１は、本発明によるＩＤ基盤の暗号化方法で、ＩＤとして使用する端末アドレスの一

例を図示した図面である。

【００１６】

一般的なＩＰｖ６アドレスは、１２８ビットから構成され、ルータのプレフィックス（prefix）である上位６４ビットと、インターフェース識別子（interface identifier）である下位６４ビットとから構成される。端末が移動してルータが変更されれば、上位６４ビットのルータであるプレフィックスが変更される。しかし、下位ＥＵＩ－６４ビットは、端末が移動してルータが変更される場合には、変更されないので、ＥＵＩ－６４を、本発明による暗号化方法のＩＤと利用する場合、移動性（mobility）を支援することができる。

【００１７】

図１を参照すれば、ＥＵＩ－６４形態の長いアドレスは、ユニークなアドレス値であり、ＩＥＥＥ ＥＵＩ－６４ １００から構成される場合と、ＩＥＥＥ ８０２の４８ビットＭＡＣ（media access control）アドレス１２０から構成される場合とがある。ＭＡＣアドレス１１０は、3バイトの機関区分値と、3バイトの装置区分値とから構成され、メーカーでＩＥＥＥに製造社ＩＤを申請し、これを割り当てられて生産する製品に、製造社ＩＤと装置ＩＤとを割り当てることによって製品を生成する。従って、あらゆる装置は、世界で唯一のＭＡＣアドレスを割り当てられる。また、ＥＵＩ－６４アドレス１００，１２０も同様に、3バイトから構成された製造社ＩＤと、5バイトから構成された装置ＩＤとを介して、全世界で唯一のＭＡＣアドレスを生成する。

【００１８】

ただし、ＩＥＥＥ ８０２の４８ビットＭＡＣアドレス１１０を有する場合、ＥＵＩ－６４表記法に合わせるために、ＩＥＥＥ標準によれば、４８ビットＭＡＣアドレスの上位3バイトと下位3バイトとの間に、１６ビットのダミービット（dummy bit）を挿入し、６４ビット（１２０）に拡張する。

【００１９】

また、６ＬｏＷＰＡＮ（wireless personal area network）の基底プロトコルであるＩＥＥＥ ８０２．１５．４では、ＥＵＩ－６４形態の長いアドレス形態と、パケットサイズの制限問題により、１６ビット・ショートアドレス（short address）形態とをいずれも支援する。６ＬｏＷＰＡＮ標準では、１６ビット・ショートアドレスを利用して通信する方法についても定義している。通信方法について簡略に説明すれば、各端末は、neighbor discovery段階で、自身のＭＡＣアドレスを自身が属したルータに登録し、１６ビット・ショートアドレスをランダムに選択し、自身が属したルータに、同一ＰＡＮ（personal area network）内の重複いかんを質疑する。衝突が発生した場合、端末は、新たなランダムな１６ビット・ショートアドレスを選択し、重複いかんを質疑する過程を反復し、衝突が発生しなければ、そのショートアドレスを登録する。同一ＰＡＮ内部で衝突が発生していないショートアドレスの場合、それから設定した６４ビットのＩＩＤ（interface identifier）と境界ルータのプレフィックスとが結合された１２８ビットＩＰｖ６アドレスを世界的に唯一のアドレスとして使用することができる。ただし、その場合、１６ビット・ショートアドレスの場合、プレフィックスと結合しなければ、唯一のアドレスにならないので、端末が新たなＰＡＮ領域に移動する場合、既存１６ビット・ショートアドレスが、新たなＰＡＮ内部で、他の端末と衝突を起こすことがあり、その場合、新たな１６ビット・ショートアドレスを選択せねばならない。

【００２０】

１６ビット・ショートアドレスの再使用性を高めるための方法として、端末のＭＡＣアドレスやＥＵＩ－６４アドレス、バージョン情報及びインデックスを入力とする衝突回避ハッシュ関数（collision free pseudo random hash function）の１６ビット出力値を、ショートアドレスとして使用することができる。バージョン情報については、追って説明するが、インデックスは、衝突回避ハッシュ関数の１６ビット出力値が、同一ＰＡＮ内部で衝突する場合、これを回避するために変更される値である。すなわち、衝突する場合、インデックスを１ずつ増加する方法を介して、新たな衝突回避ハッシュ関数の１６ビット

出力値を求める。

【００２１】

図２は、本発明によるＩＤ基盤の暗号化方法のキー設定方法の一例を図示した図面である。

【００２２】

図２を参照すれば、端末２００は、端末自身のアドレスを含むＩＤを設定する（Ｓ２５０）。ＩＤに含まれる端末のアドレスとしては、図１で説明したＥＵＩ－６４アドレス、１６ビット・ショートアドレス、端末が属したルータのプレフィックスとを合わせたアドレス、または衝突回避ハッシュ関数を介して得た１６ビット・ショートアドレスなどがある。

【００２３】

端末２００は、ＩＤをキーサーバ２１０に伝送し（Ｓ２６０）、キーサーバ２１０は、ＩＤを公開キーにする秘密キーを生成する（Ｓ２７０）。キーサーバ２１０は、離散対数群から与えられた離散対数を計算する方法で、秘密キーを生成することができる。キーサーバ２１０は、生成した秘密キーを、秘密チャンネル（オンライン／オフライン）を介して、端末２００に提供する（Ｓ２８０）。

【００２４】

端末２００は、受信した秘密チャンネルをバージョン情報と共に保存する（Ｓ２９０）。バージョン情報は、年月の日付情報の形態であるか、あるいはユーザが定義した一定形態であって、更新可能な情報である。

【００２５】

本実施形態では、ＩＤに端末のアドレスが含まれる場合を仮定したが、端末のアドレスとバージョン情報とを合わせた値をＩＤとして使用できることは言うまでもない。このとき、バージョン情報について、端末とキーサーバとの間で、事前に約束された生成規則、例えば、バージョン情報として、日付情報を利用する場合であるならば、バージョン情報を必ずＩＤに含めて伝送しなくともよい。

【００２６】

図３は、本発明によるＩＤ基盤の暗号化方法のキー更新方法の一例を図示した図面である。

【００２７】

図３の場合、端末が、端末のアドレスとバージョン情報とをＩＤとする公開キーに対する秘密キーを事前に保存していると仮定する。これは、前述の図２のキー設定過程を介して達成される。

【００２８】

図３を参照すれば、端末３００は、端末自身のアドレスと、新たなバージョン情報とを含んだ新たなＩＤを設定する（Ｓ３５０）。端末３００は、新たなＩＤと、以前バージョン情報とをキーサーバ３１０に伝送し（Ｓ３６０）、キーサーバ３１０は、新たなＩＤを公開キーにする新たな秘密キーを生成する（Ｓ３７０）。そして、キーサーバ３１０は、新たな秘密キーを秘密チャンネルを介して端末３００に伝送する（Ｓ３８０）。端末３００は、受信した新たな秘密キーで既存秘密キーを更新し、バージョン情報また新たなバージョン情報に更新する（Ｓ３８０）。

【００２９】

ここで、秘密キーを伝送する秘密チャンネルの方法として、キーサーバ３１０は、以前ＩＤ（すなわち、以前公開キー）でもって、新たな秘密キーを暗号化したデータを、端末３００に伝送することができ、端末３００は、以前ＩＤでもって暗号化されたデータを受信すれば、以前ＩＤに対応する秘密キーで暗号化されたデータを復号化し、新たな秘密キーを確保することができる。

【００３０】

図３のキー更新過程は、一定周期、またはキーの使用回数が既設定の一定回数に達すれば、端末またはキーサーバがキー更新を要請して遂行することができる。

【００３１】
図４は、本発明によるＩＤ基盤の暗号化方法を適用したパケットの一例を図示した図面である。
【００３２】
図４を参照すれば、本発明によるＩＤ基盤の暗号化方法が適用されたパケット４００は、送信者アドレスフィールド４０２、受信者アドレスフィールド４０４、暗号ヘッダフィールド４０６、ペイロード４０８などを含む。送信者アドレスフィールド４０２及び受信者アドレスフィールド４０４は、送信者と受信者とのアドレスを保存し、暗号ヘッダフィールド４０６は、パケットが、本発明によるＩＤ基盤の暗号化方法が適用されたことを示すフラグ情報、ＩＤ（すなわち、公開キー）に含まれたバージョン情報、図１で衝突回避ハッシュ関数を介した１６ビット・ショートアドレスの生成時に使用したインデックス情報などを含む。ペイロード４０８は、暗号化されたデータや署名などを含む。
【００３３】
さらに具体的には、暗号化データを伝送するパケット４２０の場合、該パケット４２０は、公開キーとして使われる受信者アドレスを含む受信者アドレスフィールド４２２、暗号化を示すフラグ情報や、ＩＤに含まれるバージョン情報などを含む暗号ヘッダフィールド４２４、及び暗号化されたデータを含むペイロード４２６などを含む。受信者アドレスとしては、図１で説明したＥＵＩ－６４アドレス、１６ビット・ショートアドレス、または１６ビット・ショートアドレスと、端末が属したルータのプレフィックスとを加えたアドレスが使われる。
【００３４】
署名時に、パケット４４０は、公開キーとして使われる送信者アドレスを含む送信者アドレスフィールド４４２、署名されたということを示すフラグ情報や、ＩＤに含まれるバージョン情報などを含む暗号ヘッダフィールド４４４、及び送信者側のＩＤに対応する秘密キーで暗号化された署名４４８などを含んだペイロード４４６などを含む。
【００３５】
このように、ＩＤ基盤の暗号化方法が適用されたパケットは、パケットに含まれた送信者アドレスや受信者アドレスを公開キーとして利用するので、別途の公開キー情報をパケットに付加する必要がない。
【００３６】
図５は、本発明によるＩＤ基盤の暗号化方法を利用した通信方法の一例を図示した図面である。
【００３７】
図５を参照すれば、送信端末５００は、まず受信端末５１０のＩＤを把握する（Ｓ５５０）。あらゆる端末は、neighbor discovery段階で、自身が属した境界（border）ルータに、自身のＥＵＩ－６４アドレスを登録するので、送信端末５００は、自身のルータに、受信端末５１０が属したルータから、受信端末のＥＵＩ－６４アドレスを得られるように要請することができる。受信端末５１０のバージョン情報の場合、受信端末５１０、または受信端末５１０が属したルータの周期的な広告メッセージを介して獲得したり、あるいはバージョン情報が、年月などの日付情報であるか、あるいは時間情報などである場合、送信端末５００で自体生成可能である。
【００３８】
送信端末５００は、獲得した受信端末５１０のアドレスとバージョン情報とを利用してデータを暗号化した後（Ｓ５６０）、この暗号化されたデータをペイロードに搭載し、受信端末５１０のアドレスやバージョン情報などが含まれた、図４に図示されたようなパケットを生成する（Ｓ５７０）。そして、送信端末５００は、パケットを受信端末５１０に伝送する（Ｓ５８０）。
【００３９】
受信端末５１０は、パケットを受信すれば、パケットから、受信端末５１０のアドレスやバージョン情報などを介して、ＩＤ、すなわち、公開キーを把握し、これに対応する秘

密キーで暗号化されたデータを復号化する（Ｓ５９０）。もし受信したパケットのバージョン情報が、自身が有しているバージョン情報と異なる場合、受信端末５１０は、送信端末５００に新たなバージョン情報を有したパケットの伝送を要請することができる。

【００４０】

図６は、本発明によるＩＤ基盤の暗号化方法を利用した署名方法の一例を図示した図面である。

【００４１】

図６を参照すれば、送信端末６００は、自身のＩＤに対応する秘密キーを利用してデータを署名し（Ｓ６５０）、署名されたパケットを受信端末６１０に伝送する（Ｓ６６０）。受信端末６１０は、パケットに含まれた送信端末６００のアドレスやバージョン情報などを利用し、送信字のＩＤ（すなわち、公開キー）を獲得し、これを利用して該当パケットの署名の正当性を検証する（Ｓ６７０）。

【００４２】

図１で説明した衝突回避ハッシュ関数を利用し、１６ビット・ショートアドレスを生成する場合、一般的に１つのＰＡＮ領域に該当する端末が、通信品質などの理由で、2^{16}個より顕著に少なく、かつ使用したハッシュ関数が、pseudo randomである性質を有するので、再使用の確率が相対的に高い。このように生成したショートアドレスにバージョン情報を追加してＩＤを生成し、これに対応する秘密キーを、再帰代理署名技法（self proxy signature）を適用し、ＥＵＩ－６４から生成されたＩＤに対応する秘密キーから自体生成したり、あるいはキーサーバから該当する秘密キーを発給されるのである。

【００４３】

ルータは、衝突が発生したアドレスに対する秘密キー生成のためのパケットを伝送しないことによって、全数調査（complete enumeration）を介した悪意的なユーザの秘密キー保存を防止することができる。また、バージョン情報をショートアドレス生成の入力として使用することにより、暗号学的安全性を保証する。

【００４４】

ルータは、自身のＰＡＮ領域外に伝送されるパケットに対する署名のために、自身のプレフィックスに対応する秘密キーをキーサーバから発給される。このとき、送信端末が１６ビット・ショートアドレスを使用し、これから派生したＩＤを利用してＩＤ基盤署名を行う場合、パケットの暗号ヘッダには、１６ビット・ショートアドレスの生成時に使用したインデックス情報が追加される。パケットの送信者アドレスフィールドには、１６ビット・ショートアドレスが含まれるが、１－hop間には、ＭＡＣ階層で、ＭＡＣアドレスを互いに知ってこそ通信するので、１－hop隣接者は、送信端末のＥＵＩ－６４アドレスを知っている。従って、送信端末の１－hop隣接者は、送信端末のＥＵＩ－６４アドレス、バージョン情報及びインデックスを利用し、ショートアドレスが正当であるか否かをチェックすることが可能であり、正当なショートアドレスであるならば、それを他の端末に伝送することができる。

【００４５】

ＰＡＮ領域外部に伝送されるパケットであり、ショートアドレスを拡張したＩＩＤに、プレフィックスを付けたアドレスを使用する場合、ルータは、ＰＡＮ領域のプレフィックスに該当する、あらかじめ発給された秘密キーを利用してパケットに再署名した後、これを伝送する。それにより、受信端末は、伝送されたパケットのプレフィックスを利用して追加された署名の正当性を検証し、ショートアドレスやバージョン情報などを利用し、送信端末の署名を検証する。

【００４６】

本発明はまた、コンピュータで読み取り可能な記録媒体に、コンピュータで読み取り可能なコードとして具現することが可能である。コンピュータで読み取り可能な記録媒体は、コンピュータシステムによって読み取り可能なデータが保存されるあらゆる種類の記録装置を含む。コンピュータで読み取り可能な記録媒体の例としては、ＲＯＭ（read-only memory）、ＲＡＭ（random-access memory）、ＣＤ－ＲＯＭ、磁気テープ、フロッピーデ

ィスク、光データ保存装置などがある。また、コンピュータで読み取り可能な記録媒体は、ネットワークに連結されたコンピュータシステムに分散され、分散方式でコンピュータで読み取り可能なコードが保存されて実行される。

【００４７】

以上、本発明についてその望ましい実施形態を中心に説明した。本発明が属する技術分野で当業者であるならば、本発明が本発明の本質的な特性から外れない範囲で変形された形態で具現可能であるということを理解することができるであろう。従って、開示された実施形態は、限定的な観点ではなく、説明的な観点から考慮されねばならない。本発明の範囲は、前述の説明でなく、特許請求の範囲に示されており、それと同等な範囲内にあるあらゆる差異点は、本発明に含まれたものであると解釈されねばならない。

【産業上の利用可能性】

【００４８】

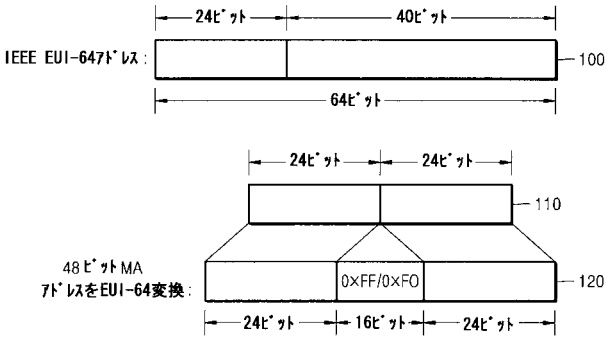
本発明のＩＤ基盤の暗号化方法及びその装置は、例えば、移動通関連の技術分野に効果的に適用可能である。

【符号の説明】

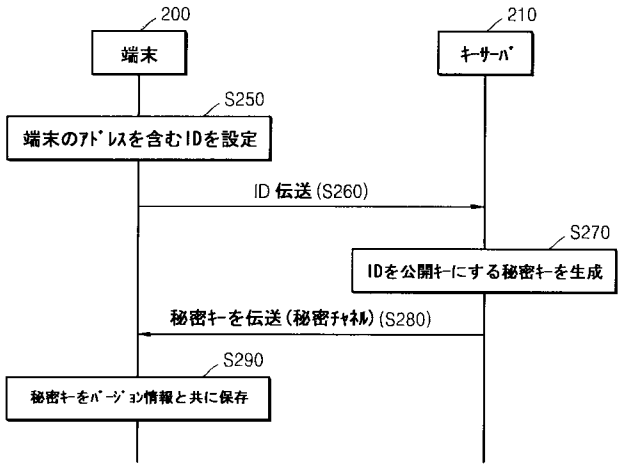
【００４９】

１００　ＩＥＥＥ ＥＵＩ－６４
１１０，１２０　ＭＡＣアドレス
２００，３００　端末
２１０，３１０　キーサーバ
４００，４２０，４４０　パケット
４０２　送信者アドレス
４０４　受信者アドレス
４０６　暗号ヘッダ
４０８　ペイロード
４２２　受信者アドレスフィールド
４２４，４４４　暗号ヘッダフィールド
４２６，４４６　ペイロード
４４２　送信者アドレスフィールド
４４８　署名

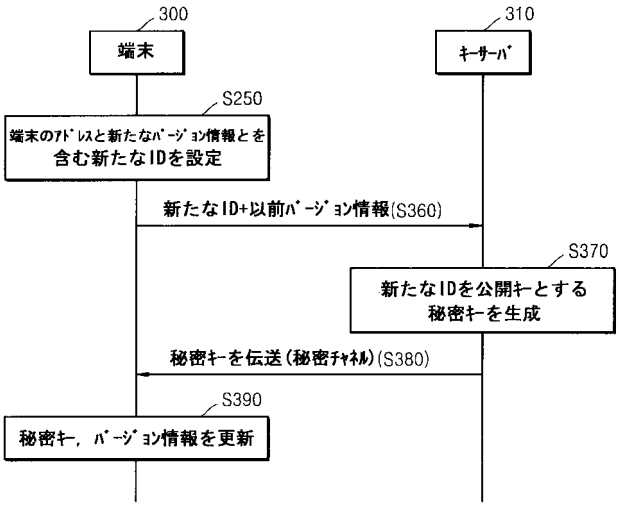
【図１】



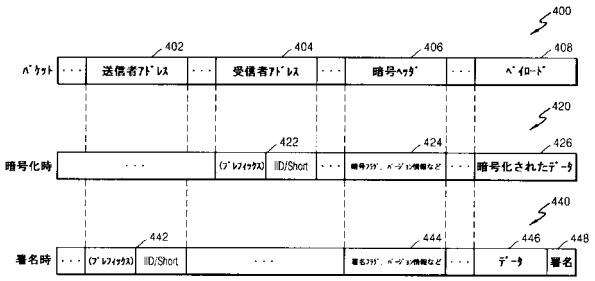
【図２】



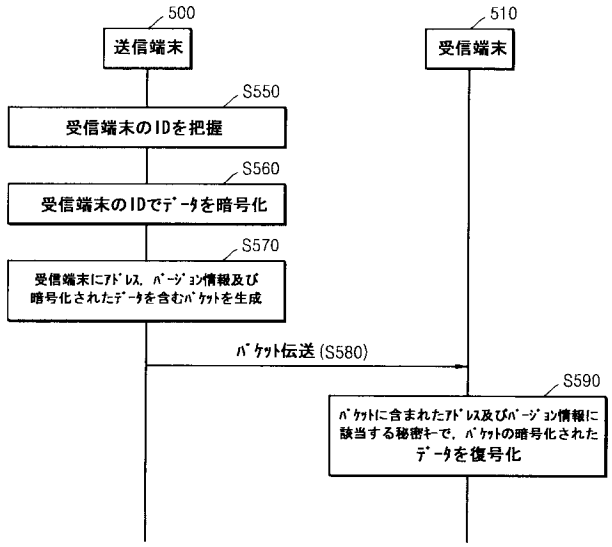
【図３】



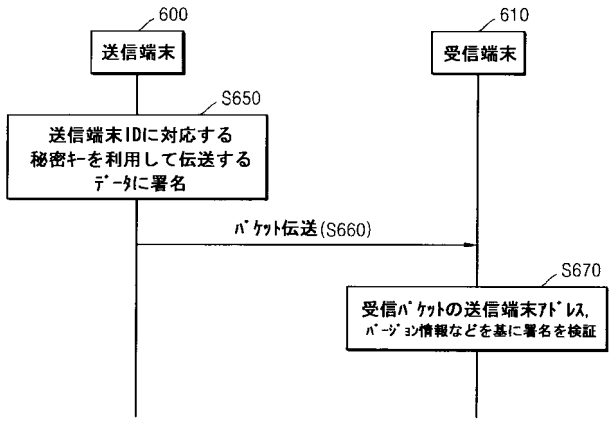
【図４】



【図５】



【図６】



フロントページの続き

(72)発明者　ヨーン、ヒョ、ジン
大韓民国キョンギ‐ド、ヨンイン‐シ、スジ‐グ、ジュクジョン、１‐ドン、ヒュンダイ、ホームタウン、３‐チャ、１‐ダンジ、７０７－７０３

Ｆターム(参考) 5J104 AA16 EA04 EA15 EA26 JA21 MA05 NA02