

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第3861053号

(P3861053)

(45) 発行日 平成18年12月20日(2006.12.20)

(24) 登録日 平成18年9月29日(2006.9.29)

(51) Int. Cl.

H04L 12/28 (2006.01)

F I

H04L 12/28 300A

請求項の数 31 (全 13 頁)

(21) 出願番号	特願2002-544927 (P2002-544927)	(73) 特許権者	598036300
(86) (22) 出願日	平成13年11月21日(2001.11.21)		テレフオンアクチーボラゲット エル エ
(65) 公表番号	特表2004-515121 (P2004-515121A)		ム エリクソン (パブル)
(43) 公表日	平成16年5月20日(2004.5.20)		スウェーデン国 ストックホルム エスー
(86) 国際出願番号	PCT/EP2001/013435		1 6 4 8 3
(87) 国際公開番号	W02002/043325	(74) 代理人	100076428
(87) 国際公開日	平成14年5月30日(2002.5.30)		弁理士 大塚 康德
審査請求日	平成16年6月3日(2004.6.3)	(74) 代理人	100112508
(31) 優先権主張番号	60/252,828		弁理士 高柳 司郎
(32) 優先日	平成12年11月22日(2000.11.22)	(74) 代理人	100115071
(33) 優先権主張国	米国 (US)		弁理士 大塚 康弘
(31) 優先権主張番号	09/802,095	(74) 代理人	100116894
(32) 優先日	平成13年3月7日(2001.3.7)		弁理士 木村 秀二
(33) 優先権主張国	米国 (US)	(74) 代理人	100101063
			弁理士 松丸 秀和

最終頁に続く

(54) 【発明の名称】 匿名ブルートゥース装置のためのシステム及び方法

(57) 【特許請求の範囲】

【請求項 1】

第1の無線ネットワーク装置及び第2の無線ネットワーク装置間で匿名通信を可能にする方法であって、

前記第1の無線ネットワーク装置において暫定ID番号を取得するステップと、

前記暫定ID番号を無線ネットワークID番号として、前記第1の無線ネットワーク装置から送信されるメッセージに挿入するステップと、

前記メッセージを前記第1の無線ネットワーク装置から前記第2の無線ネットワーク装置へ送信するステップを有することを特徴とする方法。

【請求項 2】

前記第1の無線ネットワーク装置に関連づけられる新しい暫定ID番号を周期的に取得するステップを更に有することを特徴とする請求項1記載の方法。

【請求項 3】

前記暫定ID番号が有効な時間を前記メッセージに挿入するステップをさらに有することを特徴とする請求項2記載の方法。

【請求項 4】

前記第1の無線ネットワーク装置において前記暫定ID番号を生成するステップをさらに有することを特徴とする請求項1乃至請求項3のいずれか1項に記載の方法。

【請求項 5】

前記生成するステップが、

10

20

アルゴリズムを用いて前記暫定 I D 番号を生成するステップをさらに有することを特徴とする請求項 4 記載の方法。

【請求項 6】

前記無線ネットワーク装置がブルートゥースチップを有するブルートゥース装置であり、前記生成するステップが、
前記暫定 I D 番号を前記ブルートゥースチップで生成するステップをさらに有することを特徴とする請求項 4 又は請求項 5 記載の方法。

【請求項 7】

前記生成するステップが、
前記暫定 I D 番号を周期的な方法で生成するステップを更に有することを特徴とする請求項 4 乃至請求項 6 のいずれか 1 項に記載の方法。 10

【請求項 8】

前記生成するステップが、
前記暫定 I D 番号を無作為な間隔で生成するステップを更に有することを特徴とする請求項 4 乃至請求項 6 のいずれか 1 項に記載の方法。

【請求項 9】

前記生成するステップが、
前記暫定 I D 番号をトランザクションの初めに生成するステップを更に有することを特徴とする請求項 4 乃至請求項 6 のいずれか 1 項に記載の方法。

【請求項 10】

前記暫定 I D 番号のフォーマットを特定するアクセスコードを生成するステップを更に有することを特徴とする請求項 4 乃至請求項 9 のいずれか 1 項に記載の方法。 20

【請求項 11】

前記アクセスコードを前記第 1 の無線ネットワーク装置から前記第 2 の無線ネットワーク装置へ送信するステップをさらに有することを特徴とする請求項 10 記載の方法。

【請求項 12】

前記取得するステップが、
前記第 1 の装置と遠隔配置された情報源から暫定 I D 番号を受信するステップをさらに有することを特徴とする請求項 1 乃至請求項 3 のいずれか 1 項に記載の方法。

【請求項 13】

前記受信するステップが、
前記暫定 I D 番号を前記遠隔情報源に要求するステップと、
前記遠隔情報源から前記要求に対応する前記暫定 I D 番号を受信するステップとを更に有することを特徴とする請求項 12 記載の方法。 30

【請求項 14】

前記要求するステップが、
前記第 1 の無線ネットワーク装置でランダム I D 番号を生成するステップと、
前記暫定 I D 番号の要求の内部に前記ランダム I D 番号を用いるステップとを更に有することを特徴とする請求項 13 記載の方法。

【請求項 15】

前記ランダム I D 番号を生成するステップが、
ブルートゥースアドレスのビットの所定の部分をランダムに生成するステップを更に有することを特徴とする請求項 14 記載の方法。 40

【請求項 16】

前記ブルートゥースアドレスのビットの前記部分を周期的に再生成するステップをさらに有することを特徴とする請求項 15 記載の方法。

【請求項 17】

前記ビットの所定の部分が、ブルートゥースアドレスの L A P 及び U A P フィールドを構成することを特徴とする請求項 15 又は請求項 16 記載の方法。

【請求項 18】

前記暫定 I D 番号を受信するステップが、
前記遠隔情報源からブロードキャストされる前記暫定 I D 番号として用いるための I D トークンを受信するステップをさらに有することを特徴とする請求項 1 2 乃至請求項 1 7 のいずれか 1 項に記載の方法。

【請求項 1 9】

前記遠隔情報源が前記第 2 の無線ネットワーク装置であることを特徴とする請求項 1 2 乃至請求項 1 8 のいずれか 1 項に記載の方法。

【請求項 2 0】

前記取得するステップが、
複数の暫定 I D 番号を前記第 1 の無線ネットワーク装置内に格納するステップと、
前記暫定 I D 番号として、前記複数の暫定 I D 番号の 1 つを無作為に選択するステップとをさらに有することを特徴とする請求項 1 乃至請求項 3 のいずれか 1 項に記載の方法。

10

【請求項 2 1】

前記取得するステップが、
前記第 1 の無線ネットワーク装置及び第 2 の無線ネットワーク装置間の第 1 の接続を確立するステップと、
前記第 1 の接続を介して前記第 1 の無線ネットワーク装置及び第 2 の無線ネットワーク装置間でデータを交換するステップと、
前記交換したデータを用いて前記暫定 I D 番号を生成するステップをさらに有することを特徴とする請求項 1 乃至請求項 3 のいずれか 1 項に記載の方法。

20

【請求項 2 2】

前記データが暫定的でない I D 番号及びインデックス値を含むことを特徴とする請求項 2 1 記載の方法。

【請求項 2 3】

前記生成された I D 番号をブルートゥース I D 番号として用い、前記第 1 の無線ネットワーク装置及び前記第 2 の無線ネットワーク装置間で第 2 の接続を確立するステップをさらに有することを特徴とする請求項 2 1 又は請求項 2 2 記載の方法。

【請求項 2 4】

前記第 1 及び前記第 2 の無線ネットワーク装置がブルートゥース装置であることを特徴とする請求項 1 乃至請求項 2 3 のいずれか 1 項に記載の方法。

30

【請求項 2 5】

前記匿名通信がブルートゥース通信プロトコルを用いることを特徴とする請求項 1 乃至請求項 2 4 のいずれか 1 項に記載の方法。

【請求項 2 6】

前記無線ネットワーク I D 番号がブルートゥース I D 番号であることを特徴とする請求項 1 乃至請求項 2 5 のいずれか 1 項に記載の方法。

【請求項 2 7】

他の無線ネットワーク装置との間で匿名通信を可能とする無線ネットワーク装置であって、
暫定 I D 番号を取得する手段と、

40

前記暫定 I D 番号を無線ネットワーク I D 番号として、前記無線ネットワーク装置から送信されるメッセージに挿入する手段と、
前記メッセージを前記他の無線ネットワーク装置へ送信する手段を有することを特徴とする無線ネットワーク装置。

【請求項 2 8】

前記無線ネットワーク装置がブルートゥース装置であることを特徴とする請求項 2 7 記載の無線ネットワーク装置。

【請求項 2 9】

前記暫定 I D 番号を格納するための第 1 の記憶領域をさらに有することを特徴とする請求項 2 7 又は請求項 2 8 記載の無線ネットワーク装置。

50

【請求項 3 0】

前記無線ネットワーク装置に関連する固定 I D 番号を格納するための第 2 の記憶領域をさらに有することを特徴とする請求項 2 9 記載の無線ネットワーク装置。

【請求項 3 1】

前記無線ネットワーク装置が通信する他の無線ネットワーク装置に関連する暫定 I D 番号を格納するためのテーブルをさらに有することを特徴とする請求項 2 8 乃至請求項 3 0 のいずれか 1 項に記載の無線ネットワーク装置。

【発明の詳細な説明】**【0001】**

(先に出願した仮出願への参照)

10

本発明は 2 0 0 0 年 1 1 月 2 0 日に出願された米国仮出願第 60/252,828 号の利益を請求するものである。

【0002】

(技術分野)

本発明はブルートゥース装置に関し、特にブルートゥース通信プロトコルを用いて匿名装置間での通信を可能にすることに関する。

【0003】

(発明の背景)

ブルートゥース通信プロトコル (ブルートゥース (Bluetooth) はテレフオンアクチーボラ ゲット エル エム エリクソン (Telefonaktiebolaget LM Ericsson) の商標である) は、移動電話機、コンピュータ及び他の電子機器と言った装置を、互いに短距離の範囲で通信可能にする無線短距離通信プロトコルである。このプロトコルを用いて通信する際には、ブルートゥース無線ユニットが固有の I D 番号を無線リンク上に送信し、他の装置はこの I D 番号により当該ブルートゥース装置を識別及びアドレッシング可能である。ユニットがブルートゥース通信プロトコルを用いて動作するには固有 I D 番号の使用が必要である一方で、この要件はブルートゥース装置を携帯する人のセキュリティ及びプライバシーに対する脅威を意味する。

20

【0004】

これはブルートゥース装置の存在が、その固有 I D 番号の認証を通じて確立されることに帰因する。何者かが特定のブルートゥースユニットの存在を検出可能であり、かつこの装置を用いる特定の個人を識別することが可能であるとすると、この者はそのブルートゥース装置の存在を通じてその特定の個人が特定の範囲内に存在を知ることができる。ある状況においては、この形式の認証手順は非常に望ましくないであろう。従って、ブルートゥース装置の I D を与える必要がない、すなわちその装置を用いる個人が簡単に割り出せないような、ブルートゥース装置間の相互動作方法が必要である。

30

【0005】

(発明の概要)

本発明は第 1 のブルートゥース通信装置及び第 2 のブルートゥース通信装置の間で行うための匿名通信を可能にするシステム及び方法により、上述した問題及び他の問題を解決する。第 1 の実施形態において、第 1 のブルートゥース通信装置は、第 1 のブルートゥース通信装置から第 2 のブルートゥース通信装置への送信内に挿入される暫定 I D 番号を生成する。他の実施形態は、無作為に生成された I D 番号を第 2 のブルートゥース通信装置と最初に通信を確立するために用い、その後第 2 のブルートゥース通信装置から通信をサポートするための暫定 I D 番号を受信する第 1 のブルートゥース通信装置を有する。

40

【0006】

本発明の方法及び装置は、以下の詳細な説明の欄を添付図面とともに参照することによってより完全に理解されるであろう。

【0007】

(詳細な説明)

図面、特に図 1 を参照する。図 1 には、ブルートゥース通信プロトコルで用いられている

50

現在のフォーマットによるブルートゥース装置アドレス(BD_addr)の例が示されている。ブルートゥース装置アドレスは48ビット長である。LAP(lower address part)2及びUAP(upper address part)4はBD_addrの重要な部分を形成し、NAP(non-significant address part)6によって完結する。LAPは24ビット、UAPは8ビット、NAPは16ビットからなり、48ビットのアドレスを規定する。

【0008】

ブルートゥースアクセスコードはブルートゥースプロトコル内で送信される各パケットの最初の部分を構成する。ブルートゥースで用いられるアクセスコードの一部はブルートゥース装置アドレス内のLAPによって一意に決定される。アクセスコードには4つのこととなる形式がある。チャンネルアクセスコード(CAC:Channel Access Code)はマスターのLAP2から得られる。呼び出しアクセスコード(DAC:Device Access Code)はスレーブのLAP2から得られる。問い合わせアクセスコード(IAC:Inquiry Access Code)は2つのこととなる形式を取りうるが、特定のBD_addrとは関係しない、特別に割り当てられたLAP値から得られる。

【0009】

従って、CAC及びDACは特定ユーザの位置追跡に利用可能である。さらに、全ブルートゥースアドレスは所定の機会に用いられる特別な周波数ホップ同期(FHS)パケット内で送信される。ブルートゥースにおける周波数ホッピング手法はホッピングシーケンスによって決定される。ホッピングシーケンス計算は異なる入力パラメータを用いる。通信接続状態(connection state)に対しては、マスタ装置のLAP及びUAPのMSBの少なくとも4ビットが用いられる。呼び出し状態(page state)に対しては呼び出されるユニットのLAP/UAPが用いられる。これにより、論理的には、観察されるホッピング手法に基づいてLAP及びUAPのMSB4ビット上の情報を得ることが可能になる。このように、接続においてマスタ装置アドレスの上位ビットは明らかになる。

【0010】

図2は、第1のブルートゥース装置10及び第2のブルートゥース装置15の間の匿名ブルートゥース通信を提供するシステムの機能ブロック図である。各ブルートゥース装置は、第1のブルートゥース装置10及び第2のブルートゥース装置15の間でブルートゥース通信を可能にするためのブルートゥースチップ20を含んでいる。本発明の匿名ブルートゥース接続機能を提供するため、多数の構成及び/又はアルゴリズムを各ブルートゥースチップ20内に実装しうる。しかし、図2~11に説明される様々な実施形態の実施にはこれらのアルゴリズム及び/又は構成の一部のみが必要であって、構成又はアルゴリズムのそれぞれが存在する必要はないことを理解すべきである。さらに、説明されるアルゴリズム及び構成は、必要に応じてブルートゥースチップ20の外部で実施されうる。

【0011】

各ブルートゥースチップ20は、ブルートゥース装置10、15がブルートゥース装置のID番号を含むメッセージ又は応答を送信する毎に暫定ID番号を生成することを可能にするためのアルゴリズム25を含む。暫定ID番号を生成するためのアルゴリズム25は、ブルートゥース装置10、15のブルートゥースチップ20に内蔵されても、ブルートゥース装置10、15にダウンロードされても、あるいはユーザが選択しても良い。この特定のアルゴリズム25は、それによって提供されるセキュリティ及びプライバシーの程度という点を除き、重要でない。アルゴリズム25は、既存の及び/又は将来的な番号フォーマットに準拠したブルートゥースID番号を生成せねばならない。

【0012】

ブルートゥースチップ20はさらに、アルゴリズム25が生成した暫定ID番号を一時的に格納するための記憶領域30を含んでも良い。加えて、ブルートゥース装置10が現在通信している他のブルートゥース装置15についての暫定IDが格納されるであろうIDテーブル55を用いても良い。最後に、通常の固定ID番号40が、固定ID番号を必要とする処理に利用するためにブルートゥースチップ20のどこかに格納もしくは関連づけられる。

10

20

30

40

50

【 0 0 1 3 】

図 2 のアルゴリズム 2 5 に関して上述したように、第 1 のブルートゥース装置 1 0 及び第 2 のブルートゥース装置 1 5 の間で匿名ブルートゥース通信を提供するための様々な方法を、多数のアルゴリズムが実施しうる。これら方法の数々を図 3 ~ 1 5 に関して説明する。

【 0 0 1 4 】

図 3 は、ある実施形態を示しており、ステップ 5 0 においてブルートゥース装置が暫定 I D 番号を生成する。ステップ 5 0 における暫定 I D 番号の生成は、周期的に循環するような方法で、無作為な時間間隔で、又は第 1 のブルートゥース装置 1 0 及び第 2 のブルートゥース装置 1 5 の間の各トランザクションに回答して行うことができる。ステップ 5 5 で、ブルートゥース装置 1 0 は、第 2 のブルートゥース装置 1 5 から受信した問い合わせ要求に回答し、暫定 I D 番号を用いて送信する。暫定 I D 番号は、図 2 に関して以前説明した一時記憶領域 3 0 に格納しておくことができる。暫定 I D 番号はトランザクション期間中に変更されても良い。この場合、ブルートゥース装置は新しい I D 番号又は、現行の I D 番号の知見に基づいてどのように暫定 I D 番号を生成するかの指示を交換するであろう。

【 0 0 1 5 】

図 4 は、第 1 のブルートゥース装置 1 0 及び第 2 のブルートゥース装置 1 5 間での要求に回答して、アクセスコードを暫定 I D 番号とともに供給する代替実施形態を説明する図である。前の実施形態と同様、ステップ 6 0 で第 1 のブルートゥース装置 1 0 が自装置についての暫定 I D 番号を生成する。第 1 のブルートゥース装置 1 0 は、さらにステップ 6 5 で、暫定 I D 番号のフォーマット及びカテゴリに関する情報を含むアクセスコードを生成する。ブルートゥース仕様書において現在規定されるアクセスコードを用いることが可能である。アクセスコードは、他のノードが別の I D フォーマットを取り扱い可能な可能性を与える。そのノードはアクセスコードを用いて、標準仕様に完全には準拠しない別の I D フォーマットを生成することが可能である。問い合わせ又は要求に回答して、第 1 のブルートゥース装置 1 0 はステップ 7 0 で暫定 I D 番号及びアクセスコードを第 2 のブルートゥース装置 1 5 へ送信する。この方法の利点は、第 2 のブルートゥース装置 1 0 が標準仕様に完全には準拠しないであろう別の I D フォーマットを取り扱う可能性に備えていることである。この能力は、ユニット間の全体的な動作互換性を低下させるため望ましくないであろうが、一方では高いプライバシーが必要とされる所定のアプリケーションにとっては望ましいかもしれない。ブルートゥース仕様書（ブルートゥース S I G , 「ブルートゥースシステム仕様書バージョン 1 . 0 B、第 1 巻及び第 2 巻。参照により本明細書に統合される）に現在規定されるアクセスコードをこの目的に使用可能である。

【 0 0 1 6 】

図 5 は、本発明の方法の別の代替実施形態を示す図である。本実施形態において、第 1 のブルートゥース装置 1 0 はステップ 7 5 で最初にランダム I D 番号を生成する。装置の特定のサービス又はクラスへの問い合わせはステップ 8 0 において第 1 のブルートゥース装置 1 0 から送信される。ステップ 8 5 で、第 1 のブルートゥース装置 1 0 は、その問い合わせに対して複数の応答を受信する。ステップ 9 0 で、第 1 のブルートゥース装置 1 0 は、受信した問い合わせに対応する所望のサービス又はデバイスを選択し、生成したランダム I D 番号をブルートゥース I D 番号として用いて、選択されたユニットとの接続を確立する。サービス又はデバイスを選択すると、ステップ 9 5 で、第 1 のブルートゥース装置 1 0 は、サービス又はデバイスの要求先である第 2 のブルートゥース装置 1 5 へ暫定 I D 番号要求を送信する。この要求は依然としてランダム I D 番号をブルートゥース I D 番号として用いる。ステップ 1 0 0 で、第 1 のブルートゥース装置 1 0 は、暫定 I D 番号を受信し、その I D 番号を第 1 のブルートゥース装置 1 0 及び第 2 のブルートゥース装置 1 5 間のトランザクション期間に渡って用いる。トランザクション中又は後のどこかの時点で、第 1 のブルートゥース装置 1 0 は暫定 I D 番号の仕様を終了しても良い（ステップ 1 0 5 ）。これは、第 1 のブルートゥース装置 1 0 がその領域を離れるか、所定時間経過後に

10

20

30

40

50

暫定ID番号が失効した場合に応答して起こりうる。暫定ID番号がトランザクション中に失効した場合、ステップ75から100を繰り返すことにより新しい暫定ID番号を得ることができる。

【0017】

図6は、第1のブルートゥース装置10がまずステップ110で無作為に選択されたID番号をブルートゥースID番号として用いて接続を確立する別の実施形態を示す図である。ランダムID番号の使用は、ステップ115における接続の確立において、図5に対応して上述したような、ブルートゥースID番号としての暫定ID番号の使用を可能にする。問い合わせステップ120は、ステップ115で確立された暫定ID番号の失効を監視し、暫定ID番号が失効すると、暫定ID番号がステップ125で置き換えられる。図7 10
に示すように、暫定ID番号が有効であろう期間は、第1のブルートゥース装置10からの要求に応答して第2のブルートゥース装置15から第1のブルートゥース装置10へ送信されるメッセージ130内で規定することができる。メッセージ130内には、暫定ID番号135及び、暫定ID番号135が有効な期間を示すメッセージ時間140が含まれるであろう。

【0018】

図8及び9は、図5及び6において言及されたランダムブルートゥースアドレスの生成方法の一実施形態を示す図である。この方法は、無作為に選択される、有効期間の短い(short-lived)ブルートゥースアドレス(BD_addr_active)を用いるが、全てのユニットは有効期間の長いブルートゥースアドレス(BD_addr)もまた含んでいる。有効アドレス(active address)であるBD_addr_activeは、BD_addrと同じNAPフィールド136を有する。BD_addr_activeアドレスは、ブルートゥースモジュールが起動された際、ステップ137で32のランダムビットを生成することによって得られる。この32のランダムビットは任意の方法によって生成することができる。これら32のランダムビットはBD_addr_activeアドレスのLAP138及びUAP139フィールドを決定する。LAP138及びUAP139フィールドはまた、ステップ141で32のランダムビットを再選択して周期的に更新される。 20

【0019】

ランダムなBD_addr_activeアドレスが生成されると、ステップ142において、FHS(周波数ホッピングシーケンス)パケット内で用いられるアドレスがDB_addr_activeアドレスとなるであろうことを除き、現在ブルートゥース仕様書で策定されているのと同じ様式で問い合わせ処理が進行する。最初のFHSパケットはマスターのBD_addr_activeアドレスを含むであろう。引き続くFHSパケットは平文形式で送信されるマスターのBD_addrを含むか、スレーブに属する匿名ユニットキーとともに、暗号化形式でマスターのBD_addrを送信するであろう。ブルートゥース通信プロトコル内の呼び出し手順は、ステップ143において、アクセスコード(CACおよびDAC)及び周波数ホッピング手法がBD_addr_activeアドレスに基づくことを除き、現在規定されるブルートゥース仕様に従って進行する。 30

【0020】

BD_addr_activeアドレスを用いてマスター及びスレーブユニット間での問い合わせ及び呼び出しが行われた後、マスターユニットはスレーブのBD_addrを知らないし、スレーブもまた同様にマスターユニットのBD_addrを知らない。接続が確立すると、マスター及びスレーブユニットは、各ユニットのBD_addrアドレスを交換できるよう、2ユニット間で暗号化された接続を確立可能とするセキュリティペアリング手順を実行することができる。 40

【0021】

図10A及び10Bに、ステップ145において第1のブルートゥース装置10からのランダムID番号を用いて接続が確立される、更に別の実施形態を示す。ランダムID番号を用いて第1のブルートゥース装置10及び第2のブルートゥース装置15の間で接続が確立すると、ステップ150において、セキュリティペアリングが2つの装置間で実行されうる。セキュリティペアリングの結果、ブルートゥース装置は、ステップ155におい 50

て、暗号化された、暫定的でないブルートゥースID番号及びインデックス値を交換する。各ブルートゥース装置は、個別かつ独自のインデックス値を有する。

【0022】

その後、第1及び第2のブルートゥース装置が互いにコンタクトを希望する際には、ステップ160において、コンタクトするブルートゥース装置により、暫定的でないID番号及びインデックス値を用いて疑似ランダムID番号を生成する。コンタクトするブルートゥース装置はステップ165において、生成した疑似ランダムID番号を用いてもう一方のブルートゥース装置を呼び出す。コンタクトするブルートゥース装置はステップ170において応答を監視する。呼び出しに対する応答を受信すると、ステップ180でブルートゥース装置間の接続が確立する。応答が受信されない場合、ステップ175において、例えば図5で説明したような別の方法を用いて接続を確立する。

10

【0023】

図11に、第1のブルートゥース装置10が第2のブルートゥース装置15との通信に入る際に、第1のブルートゥース装置10がステップ185で第2のブルートゥース装置15に暫定ID番号を要求する代替実施形態を示す。第2のブルートゥース装置15から暫定ID番号を受信すると、第1のブルートゥース装置10はステップ190でこの暫定ID番号を用いて第2のブルートゥース装置15と接続を確立する。

【0024】

図12に示す実施形態においては、システム内の少なくとも1つのブルートゥース装置が、ステップ195でIDトークンをブロードキャストする。あるブルートゥース装置が他のブルートゥース装置との通信を確立したい際には、そのブルートゥース装置はIDトークンをステップ200で受理し、受理したIDトークンを用いてステップ205で通信を確立する。

20

【0025】

図13は、ステップ210で、ブルートゥース装置10が例えば図1に記載した記憶領域20内に、複数の暫定ID番号を格納するさらに別の実施形態を示す。別個のブルートゥース装置15と接続を確立する必要があると、ステップ215で複数のID番号の1つが無作為に選択される。そして、無作為に選択されたID番号を用い、ステップ220で接続を確立する。

【0026】

図14は、さらに別の実施形態を示す。この実施形態では、ステップ225でブルートゥース装置が、独立した情報源に暫定ID番号を要求する。要求したブルートゥース装置はステップ230において、例えば公衆無線網又はブルートゥース接続を介して、独立した情報源から暫定ID番号を受信する。そして、ブルートゥース装置10は、与えられた暫定ID番号を用い、ステップ235において接続を確立することができる。ブルートゥース装置が暫定ID番号を受信する独立情報源には、例えばネットワークサーバ、無線ネットワークサーバ、インターネットサーバ等が含まれる。

30

【0027】

図15は、さらに別の実施形態を示す。この実施形態では、第1のブルートゥース装置10から第2のブルートゥース装置240へ送信される問い合わせ及び通信が、問い合わせ又は通信とともに暫定ID番号を含んでいる。ステップ245で、コンタクトされるブルートゥース装置15は、問い合わせに対し、別の暫定ID番号を生成又は取得する処理を行わずに、供給された暫定ID番号を用いて応答する。

40

【0028】

上述した実施形態を用いて、ブルートゥース装置は、通信装置又はブルートゥース装置を用いるユーザのIDを容易に与えることなく他のブルートゥース装置と通信可能な、匿名エンティティとして振る舞うことが可能になる。ブルートゥースIDとは別個のアプリケーションレベルにおいて、セキュアな方法で任意のユーザ認証を行うことが可能である。従って、権限のない個人は、特定のブルートゥース装置を誰が使用しているかを不正に調べることができなくなるであろう。

50

【 0 0 2 9 】

上の説明は本発明の実施のための好ましい実施形態の説明であり、本発明の範囲は必ずしもこの説明に限定されるべきものではない。代わりに、本発明の範囲は、以下の請求範囲によって規定される。

【図面の簡単な説明】

【図 1】 ブルートゥースアドレスのフォーマットを示す図である。

【図 2】 相互に匿名通信可能なブルートゥース装置を示すブロック図である。

【図 3】 ブルートゥース装置間の匿名通信のための方法の第 1 の実施形態を示す図である。

【図 4】 ブルートゥース装置間の匿名通信のための方法の別の実施形態を示す図である 10

【図 5】 ブルートゥース装置間の匿名通信のための方法のさらに別の実施形態を示す図である。

【図 6】 ブルートゥース装置間の匿名通信のための方法のさらに別の実施形態を示す図である。

【図 7】 図 5 に示す方法を用いてブルートゥース装置間で送信されるメッセージを示す図である。

【図 8】 無作為に生成されるブルートゥースアドレスを示す図である。

【図 9】 図 8 のランダムブルートゥースアドレスの生成方法を示すフローチャートである。 20

【図 10 A】

【図 10 B】

【図 11】

【図 12】

【図 13】

【図 14】

【図 15】 ブルートゥース装置間の匿名通信のための方法のさらに別の実施形態を示す図である。

【図 1】

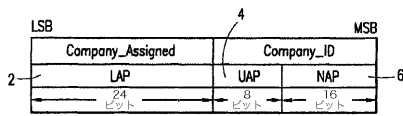


FIG. 1

【図 2】

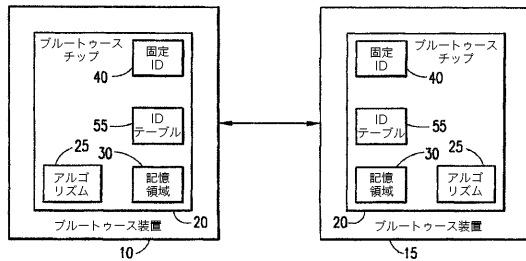


FIG. 2

【図 3】

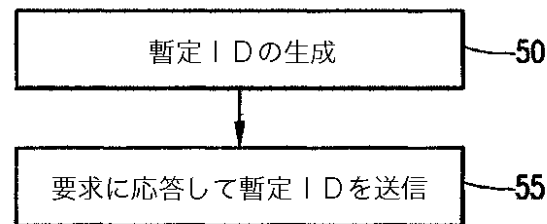


FIG. 3

【図 5】

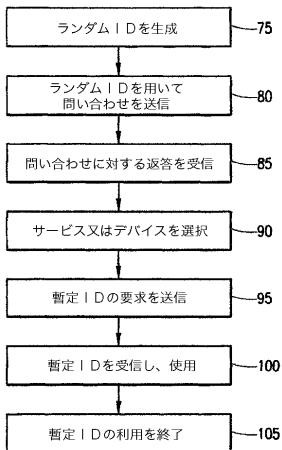


FIG. 5

【図 6】

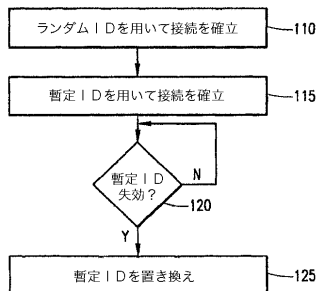


FIG. 6

【図 4】

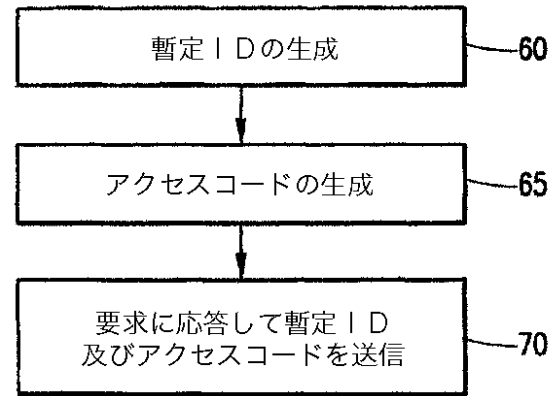


FIG. 4

【図 7】

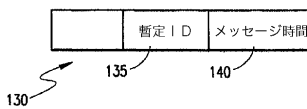


FIG. 7

【図 8】

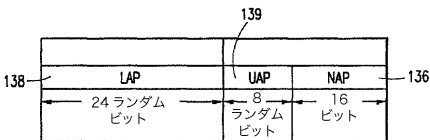
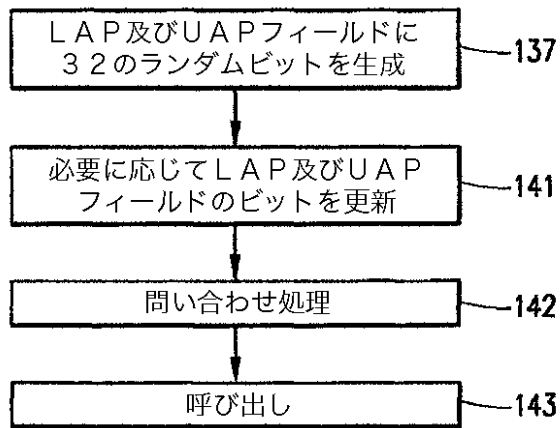
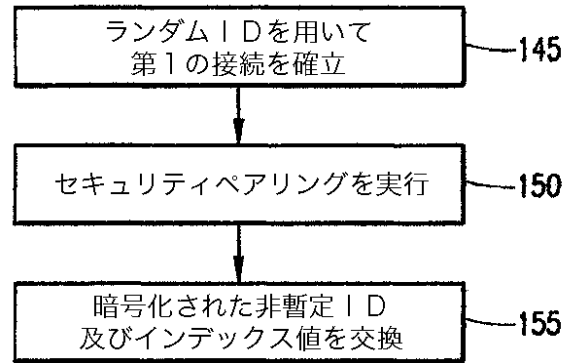


FIG. 8

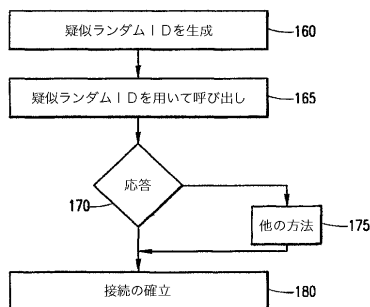
【図 9】

**FIG. 9**

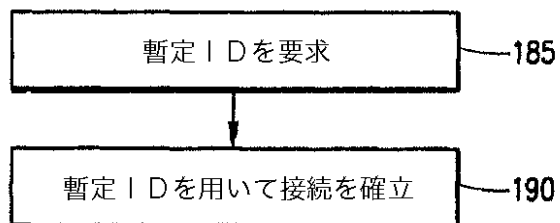
【図 10 A】

**FIG. 10a**

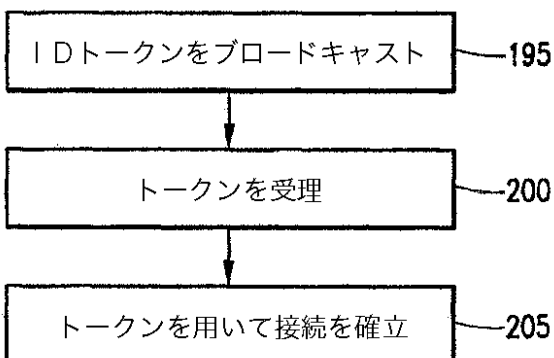
【図 10 B】

**FIG. 10b**

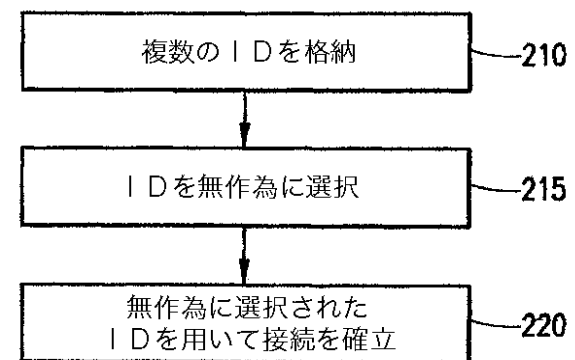
【図 11】

**FIG. 11**

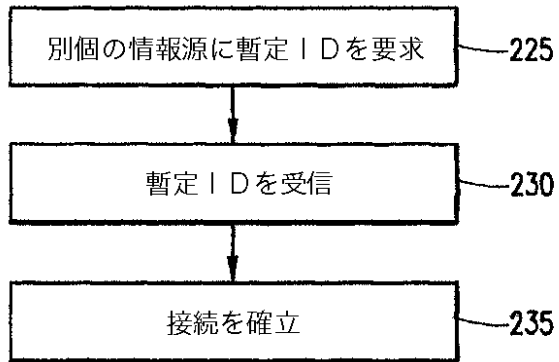
【図 12】

**FIG. 12**

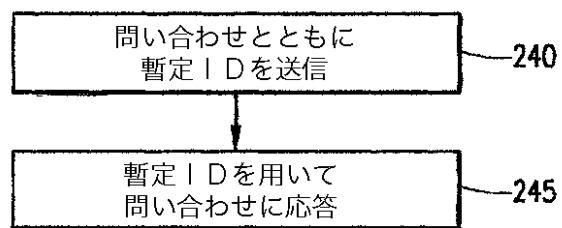
【図 13】

**FIG. 13**

【図 1 4】

**FIG. 14**

【図 1 5】

**FIG. 15**

フロントページの続き

(74)代理人 100130409

弁理士 下山 治

(72)発明者 リュドベック, ニルス

アメリカ合衆国 ノースカロライナ州 27511, キャリー, ルセルグラン ロード 202

(72)発明者 スクビク, ヤネス

スウェーデン国 ヘッセルビュ エス - 165 73, レディスヴェーゲン 46

(72)発明者 デント, ポール

アメリカ合衆国 ノースカロライナ州 27312, ピッツボロ, イーグルポイント ロード 637

(72)発明者 ゲールマン, クリスティアン

スウェーデン国 ルント エス - 222 29, サンクト モンスガタン 17エー

審査官 矢頭 尚之

(56)参考文献 特開平8 - 214369 (JP, A)

特開平6 - 112944 (JP, A)

特開平4 - 225642 (JP, A)

特開平8 - 242245 (JP, A)

(58)調査した分野(Int.Cl., DB名)

H04L 12/28

H04L 12/40

H04L 12/42

H04L 12/44

H04L 12/46