

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第5259014号
(P5259014)

(45) 発行日 平成25年8月7日 (2013.8.7)

(24) 登録日 平成25年5月2日 (2013.5.2)

(51) Int.Cl. F I
H O 4 W 84/18 (2009.01) H O 4 W 84/18
H O 4 W 52/02 (2009.01) H O 4 W 52/02 1 1 1

請求項の数 38 (全 31 頁)

(21) 出願番号	特願2012-508406 (P2012-508406)	(73) 特許権者	503447036
(86) (22) 出願日	平成22年4月30日 (2010.4.30)		サムスン エレクトロニクス カンパニー リミテッド
(65) 公表番号	特表2012-525762 (P2012-525762A)		大韓民国・443-742・キョンギード ・スウォン・シ・ヨント・ン・ク・サムスン ーロ・129
(43) 公表日	平成24年10月22日 (2012.10.22)	(74) 代理人	100089037
(86) 国際出願番号	PCT/KR2010/002780		弁理士 渡邊 隆
(87) 国際公開番号	W02010/126342	(74) 代理人	100110364
(87) 国際公開日	平成22年11月4日 (2010.11.4)		弁理士 実広 信哉
審査請求日	平成23年10月31日 (2011.10.31)	(72) 発明者	ギリラジ・ゴヤール
(31) 優先権主張番号	1014/CHE/2009		インド・バンガロール・560034・コ ラマングラ・フォース・ブロック・フィフ ス・クロス・トウェルフス・メイン・ファ ースト・フロア・#636
(32) 優先日	平成21年4月30日 (2009.4.30)		最終頁に続く
(33) 優先権主張国	インド (IN)		
(31) 優先権主張番号	2605/CHE/2008		
(32) 優先日	平成21年10月26日 (2009.10.26)		
(33) 優先権主張国	インド (IN)		

(54) 【発明の名称】 コーディネータ装置を用いてボディエリアネットワークを管理するための方法及びシステム

(57) 【特許請求の範囲】

【請求項 1】

ボディエリアネットワークにおけるコーディネータ装置を用いて複数のインプラント装置を管理する方法であって、

M I C Sチャンネルを獲得するステップと、
非M I C Sチャンネルを用いてウェイクアップを指示するウェイクアップ信号を送信するステップと、

前記ウェイクアップ信号を受信したインプラント装置を前記M I C Sチャンネルで接続するステップと、

前記インプラント装置とデータを交換するステップと、
前記インプラント装置に分離命令メッセージを伝送して接続を解除するステップと、
を有し、

前記ウェイクアップ信号は、前記獲得されたM I C Sチャンネルに対する情報を含むことを特徴とする方法。

【請求項 2】

前記接続するステップは、
前記ウェイクアップ信号を受信したインプラント装置から第1の承認信号を前記M I C Sチャンネルで受信するステップと、

前記承認信号に基づいて、接続を指示する命令信号を前記M I C Sチャンネルで前記インプラント装置に送信するステップと、

前記命令信号に基づいた第2の承認信号を前記MICSチャンネルで前記インプラント装置から受信するステップと、

を有することを特徴とする請求項1に記載の方法。

【請求項3】

前記第2の承認信号は、セキュリティ制御フィールドを含み、

前記接続するステップは、

前記セキュリティ制御フィールドに基づいてセキュリティ手順を開始して前記インプラント装置を認証するステップと、

前記認証に基づいて暗号化及び復号化の中の一つを遂行するステップと、

再生保護を実行するステップと、

データフレームに対するインテグリティ保護を実行するステップと、

をさらに有することを特徴とする請求項2に記載の方法。

10

【請求項4】

前記接続するステップは、

接続を指示する命令信号を前記MICSチャンネルで前記インプラント装置に送信するステップと、

前記命令信号に基づいて承認信号を前記MICSチャンネルで前記インプラント装置から受信するステップと、

を有することを特徴とする請求項1に記載の方法。

【請求項5】

前記承認信号は、セキュリティ制御フィールドを含み、

前記接続するステップは、

前記セキュリティ制御フィールドに基づいてセキュリティ手順を開始して前記インプラント装置を認証するステップと、

前記認証に基づいて暗号化及び復号化の中の一つを遂行するステップと、

再生保護を実行するステップと、

データフレームに対するインテグリティ保護を実行するステップと、

をさらに有することを特徴とする請求項4に記載の方法。

20

【請求項6】

前記MICSチャンネルを獲得するステップは、非活性状態で前記コーディネータ装置と前記インプラント装置との間で前記MICSチャンネルを維持するステップを有することを特徴とする請求項1に記載の方法。

30

【請求項7】

前記ウェイクアップ信号を送信するステップは、

定義された周期内で前記承認信号が前記インプラント装置から受信されるまで前記非MICSチャンネルで前記信号を再送信するステップと、

定義された期間で前記承認信号が前記MICSで受信されないと、他の非MICSチャンネルで前記ウェイクアップ信号を再送信するステップのうちいずれか一つを有することを特徴とする請求項2に記載の方法。

【請求項8】

他のインプラント装置から送信された非常信号に対して前記コーディネータ装置で他のMICSチャンネルをスキッピングするステップと、

前記他のインプラント装置から前記非常信号が受信される場合に、前記インプラント装置との前記データ交換を中止し、前記他のインプラント装置とデータを交換するステップと、

をさらに含むことを特徴とする請求項1に記載の方法。

40

【請求項9】

前記コーディネータ装置は、装置識別子、マスターキー、及び該当マスターキー識別子、デバイスのタイプ、サービス、及びメディアアクセス制御アドレスを含むセキュリティテーブルで事前構成されることを特徴とする請求項1に記載の方法。

50

【請求項 1 0】

前記セキュリティ制御フィールドは、接続手順の間に交換されるセキュリティ制御、アプリケーションパラメータフィールドを用いて前記MACフレームでフレームレベルセキュリティを定義し、異なるセキュリティ特性は、アプリケーション及びBAN装置要求条件に従って各フレームに対して選択できることを特徴とする請求項3に記載の方法。

【請求項 1 1】

前記セキュリティ制御フィールドは、接続手順の間に交換されるセキュリティ制御、アプリケーションパラメータフィールドを用いて前記MACフレームでフレームレベルセキュリティを定義し、前記フレームレベルセキュリティは、接続手順の間に識別され、類似したフレームレベルセキュリティがセキュリティ保護を必要とする前記フレームに均一に使用されることを特徴とする請求項3に記載の方法。

10

【請求項 1 2】

オンボディ装置と通信を遂行するための通信チャンネルを獲得するステップと、
特定のオンボディ装置から前記コディネータ装置情報に対する要求を受信するステップと、
前記オンボディ装置からピコネットとの結合に対する接続要求を受信するステップと、
前記コディネータ装置のために定義される複数の許可制御パラメータに基づいて前記接続要求を確認するステップと、
前記接続要求を前記確認に基づいて承認するステップと、
前記接続要求に含まれるセキュリティ制御フィールドに基づいてセキュリティ手順を開始するステップと、
前記特定のオンボディ装置とデータを交換するステップと、
をさらに有することを特徴とする請求項 1 に記載の方法。

20

【請求項 1 3】

前記セキュリティ手順を開始するステップは、
前記特定のオンボディ装置を認証するステップ、前記認証に基づいて暗号化及び復号化の中の一つを遂行するステップ、再生保護を実行するステップ、及びデータフレームに対してインテグリティ保護を可能にするステップのうちいずれか一つを有することを特徴とする請求項1 2に記載の方法。

【請求項 1 4】

前記オンボディ装置と通信を遂行するための通信チャンネルを獲得するステップと、
前記コディネータ装置情報をブロードキャストリングするステップと、
前記ブロードキャストリングに基づいて前記特定のオンボディ装置から前記接続要求を受信するステップと、をさらに有することを特徴とする請求項 1 に記載の方法。

30

【請求項 1 5】

前記通信チャンネルの獲得は、ブロードキャストモードと非ブロードキャストモードの中の一つに基づくことを特徴とする請求項1 2に記載の方法。

【請求項 1 6】

前記通信チャンネルを獲得するステップは、
前記通信チャンネルの占有を指示する通知をブロードキャストリングするステップと、
前記通知に基づいて応答を決定するステップと、
を有することを特徴とする請求項1 2に記載の方法。

40

【請求項 1 7】

前記接続要求は、平均データレート、パケットサイズ、インターパケット到着時間、MAC層で送信したパケットのサイズ、遅延要求条件、及びセキュリティ制御フィールドのうち少なくとも一つを含むことを特徴とする請求項1 2に記載の方法。

【請求項 1 8】

前記コディネータ装置は、装置識別子、マスターキー識別子、デバイスのタイプ、サービス、及びメディアアクセス制御アドレスを含むセキュリティテーブルで事前構成されることを特徴とする請求項1 2に記載の方法。

50

【請求項 19】

前記複数のオンボディ装置を示す一つ又はそれ以上の代表ノードの中の各代表ノードから接続要求を受信するステップと、

前記一つ又はそれ以上の代表ノードの中で代表ノードから受諾される前記接続要求を受信することに基づいて前記接続要求を管理するステップと、

メッセージを前記複数のオンボディ装置にブロードキャストするステップと、を有し、

前記メッセージは、前記代表ノードに対応するグループ識別子、前記複数のオンボディ装置に対する装置識別子、及び1セットのセキュリティパラメータのうち少なくとも一つを含むことを特徴とする請求項12に記載の方法。

10

【請求項 20】

前記管理するステップは、前記複数の代表ノードのうち他の代表ノードに拒絶メッセージを送信するステップを有することを特徴とする請求項19に記載の方法。

【請求項 21】

前記一つ又はそれ以上の代表ノードは単一グループ識別子と関連されることを特徴とする請求項19に記載の方法。

【請求項 22】

前記一つ又はそれ以上の代表ノードは別途のグループ識別子と関連されることを特徴とする請求項19に記載の方法。

【請求項 23】

前記セキュリティパラメータのセットは、
前記コーディネータ装置と前記複数のオンボディ装置との間で共有されるマスターキー識別子と、

コーディネータノンスと、

クライアントノンスと、

固有個別キーと共通キーのうちいずれか一つを指示するフラグビットと、

を含むことを特徴とする請求項19に記載の方法。

20

【請求項 24】

前記マスターキー識別子、前記コーディネータノンス、前記クライアントノンス、及び各オンボディ装置の前記装置識別子を用いて前記コーディネータ装置と前記各オンボディ装置との間で固有ペアワイズキーを発生するステップと、

前記マスターキー識別子、前記コーディネータノンス、及び前記クライアントノンスを用いて前記コーディネータ装置と複数のオンボディ装置との間で共通ペアワイズキーを生成するステップのうちいずれか一つをさらに有することを特徴とする請求項23に記載の方法。

30

【請求項 25】

前記生成は、前記コーディネータ装置と前記各オンボディ装置によって別途に遂行されることを特徴とする請求項24に記載の方法。

【請求項 26】

ボディエリアネットワークを管理するコーディネータ装置であって、

通信インターフェースと、

前記通信インターフェースを通じて、MICSチャンネルを獲得し、非MICSチャンネルを用いてウェイクアップを指示するウェイクアップ信号を送信し、前記ウェイクアップ信号を受信したインプラント装置を前記MICSチャンネルで接続し、前記インプラント装置とデータを交換し、前記インプラント装置で分離命令メッセージを伝送して接続を解除するプロセッサと、

前記交換されたデータを格納する格納装置と、

を含み、

前記ウェイクアップ信号は、前記獲得されたMICSチャンネルに対する情報を含むことを特徴とする装置。

40

50

【請求項 27】

前記プロセッサは、

前記インプラント装置を接続するために、前記ウェイクアップ信号を受信したインプラント装置から第1の承認信号を前記MICSチャンネルで受信し、前記承認信号に基づいて接続を指示する命令信号を前記MICSチャンネルで前記インプラント装置に送信し、前記命令信号に基づいた第2の承認信号を前記MICSチャンネルで前記インプラント装置から受信することを特徴とする請求項26に記載の装置。

【請求項 28】

前記第2の承認信号は、セキュリティ制御フィールドを含み、

前記プロセッサは、

前記セキュリティ制御フィールドに基づいてセキュリティ手順を開始して前記インプラント装置を認証し、前記認証に基づいて暗号化及び復号化の中の一つを遂行し、

再生保護を実行し、

データフレームに対するインテグリティ保護を実行することを特徴とする請求項27に記載の装置。

【請求項 29】

前記プロセッサは、

前記インプラント装置を接続するために、接続を指示する命令信号を前記MICSチャンネルで前記インプラント装置に送信し、

前記命令信号に基づいた承認信号を前記MICSチャンネルで前記インプラント装置から受信することを特徴とする請求項26に記載の装置。

【請求項 30】

前記承認信号は、セキュリティ制御フィールドを含み、

前記プロセッサは、

前記セキュリティ制御フィールドに基づいてセキュリティ手順を開始して前記インプラント装置を認証し、

前記認証に基づいて暗号化及び復号化の中の一つを遂行し、

前記再生保護を実行し、

データフレームに対するインテグリティ保護を実行することを特徴とする請求項29に記載の装置。

【請求項 31】

前記プロセッサは、前記MICSチャンネルの非活性状態で前記コーディネータ装置と前記インプラント装置との間で前記MICSチャンネルを維持することを特徴とする請求項26に記載の装置。

【請求項 32】

前記プロセッサは、定義された周期内で前記インプラント装置から前記承認信号が受信されるまで、前記非MICSチャンネル上に前記ウェイクアップ信号を再送信し、あるいは定義された周期で前記MICSチャンネルで承認信号が受信されないと、他の非MICSチャンネル上に前記ウェイクアップ信号を再送信することを特徴とする請求項27に記載の装置。

【請求項 33】

前記プロセッサは、

前記通信インターフェースを通じて、オンボディ装置と通信を遂行するための通信チャンネルを獲得し、特定のオンボディ装置から前記コーディネータ装置情報に対する要求を受信し、前記オンボディ装置からピコネットとの接続に対する接続要求を受信し、前記コーディネータ装置のために定義される複数の許可制御パラメータに基づいて前記接続要求を確認し、

前記確認に基づいて前記接続要求を承認し、前記接続要求に含まれたセキュリティ制御フィールドに基づいてセキュリティ手順を開始し、前記特定のオンボディ装置とデータを交換することを特徴とする請求項26に記載の装置。

【請求項 3 4】

前記プロセッサは、オンボディ装置と通信を遂行するための通信チャンネルを獲得し、前記コーディネータ装置情報をブロードキャストし、前記ブロードキャストに基づいて特定のオンボディ装置から接続要求を受信することを特徴とする請求項 2 6 に記載の装置。

【請求項 3 5】

前記プロセッサは、一つ又はそれ以上の代表ノードのうち各代表ノードから接続要求を受信し、前記一つ又はそれ以上の代表ノードは複数のオンボディ装置を表し、前記接続要求を受信することに基づいて前記接続要求を管理し、前記一つ又はそれ以上の代表ノードのうち代表ノードからの前記接続要求が受諾され、メッセージを前記複数のオンボディ装置にブロードキャストし、

10

前記メッセージは、前記代表ノードに対応するグループ識別子、前記複数のオンボディ装置に対する装置識別子、及びワンセットのセキュリティパラメータのうち少なくとも一つを含むことを特徴とする請求項 2 6 に記載の装置。

【請求項 3 6】

インプラント装置がボディエリアネットワークをサポートする方法であって、非 M I C S チャンネルを介してコーディネータ装置からウェイクアップ信号を受信するステップと、

前記ウェイクアップ信号の受信によって M I C S チャンネル機能を活性化するステップと、

20

前記ウェイクアップ信号に含まれた M I C S チャンネルの情報を用いてコーディネータ装置と前記 M I C S チャンネルで前記コーディネータ装置に接続するステップと、

前記コーディネータ装置とデータを交換するステップと、
を有することを特徴とする方法。

【請求項 3 7】

前記接続するステップは、

前記ウェイクアップ信号に基づいて第 1 の承認信号を前記コーディネータ装置に伝送するステップと、

前記承認信号に関連して、前記コーディネータ装置への接続を指示する命令信号を前記コーディネータ装置から受信するステップと、

30

前記命令信号に基づいて第 2 の承認信号を前記コーディネータ装置に伝送するステップと、

を有することを特徴とする請求項 3 6 に記載の方法。

【請求項 3 8】

前記接続するステップは、

前記ウェイクアップ信号の受信後に、前記コーディネータ装置への接続を指示する命令信号を前記コーディネータ装置から受信するステップと、

前記命令信号に基づいて承認信号を前記コーディネータ装置に伝送するステップと、
を有することを特徴とする請求項 3 6 に記載の方法。

【発明の詳細な説明】

40

【技術分野】

【0 0 0 1】

本発明は、一般的にインプラント医療用通信システムの分野に関するもので、より具体的には、コーディネータ装置を用いてインプラント装置とオンボディ装置を含むボディエリアネットワークを管理するための方法及びシステムに関する。

【背景技術】

【0 0 0 2】

現在、ボディエリアネットワーク(Body Area Network: BAN)は、デバイスの間で通信を行うために短距離無線媒体を利用する。コーディネータ装置と呼ばれる中央ノード(centralized node)は、ピコネット通信を制御する。コーディネータ装置に接続された

50

1 セットのBANデバイスは、ピコネットを形成する。このBANデバイスは、医療制御システム、患者モニタリング、健康及びフィットネス、ゲーム、及びマルチメディアアプリケーションに応じるように使われる。このBANデバイスの一部は、人体に植え込まれてインプラント装置(Implant Device: IMD)と称し、生体(人体)上に提供される他のBANデバイスはオンボディ装置(On-Body Device: OBD)と称する。

【0003】

BANデバイスは、一般的に小さく、一定の電力供給接続を具備しない。BANデバイスは、頻繁に再充電が不可能なバッテリーから電力の供給を受け、一部のIMDに対しては全く再充電が不可能である。

【0004】

電力が制限されるIMDは、非常事態を感知して目覚める非常(emergency)イベントの場合を除き、ほとんどの場合にディープスリープモード(deep sleep mode)にあり、通信の開始前にウェイクアップ過程を必要とする。しかしながら、このIMDに対するデータ通信段階は、僅か数秒のセッションの間に起きるので、IMDデバイスの寿命と比較すると、ほとんど無視してもよい。したがって、ウェイクアップ及び接続過程は、インプラント通信過程の主な部分である。さらに、IMDとの通信は、インプラント医療用通信システム(medical implant communication systems)に限定される一方で、OBDとの通信は、それに限定されず、超広帯域又は狭帯域信号を用いて遂行でき、それによってコーディネータ装置の動作の複雑性を増加させる。

【発明の概要】

【発明が解決しようとする課題】

【0005】

したがって、上述した従来技術の問題点に鑑みて、本発明の目的は、コーディネータ装置を用いてインプラント装置とオンボディ装置を含むボディエリアネットワークを管理するための方法及びシステムを提供することにある。

【課題を解決するための手段】

【0006】

上記のような目的を達成するために、本発明の一実施形態は、コーディネータ装置を用いてインプラント装置とオンボディ装置を含むボディエリアネットワークを管理するための方法及びシステムを提供する。

【0007】

コーディネータ装置を用いてボディエリアネットワークで複数のインプラント装置を管理する方法の一例は、コーディネータ装置においてインプラント医療用通信サービス(MICS)送受信器によってMICSチャンネルを獲得するステップを有する。また、この方法は、非MICS(non-MICS)チャンネル内でインプラント装置にウェイクアップ過程を指示する信号を送信するステップを有する。さらに、上記方法は、MICS送受信器によってインプラント装置にピコネットとの結合を指示する命令信号を送信するステップを有する。命令信号は、装置識別子を含む。また、上記方法は、インプラント装置への命令信号の送信に基づいてコーディネータ装置のMICS送受信器によって承認(acknowledgement)信号を受信するステップをさらに有する。承認信号は、セキュリティ制御フィールドを含む。また、上記方法は、セキュリティ制御フィールドに基づいてインプラント装置を認証するステップ、認証に基づいて暗号化及び復号化のうちの一つを遂行するステップ、再生保護を実行するステップ、及びデータフレームに対するインテグリティ保護を可能にするステップを含むセキュリティ手順を開始するステップを有する。また、上記方法は、開始に基づいてコーディネータ装置とインプラント装置との間でデータを交換するステップ、及び命令メッセージを送信してインプラント装置を分離するステップをさらに有し、命令メッセージは、ユニキャストメッセージ、マルチキャストメッセージ、及びブロードキャストメッセージのうちいずれか一つを含む。

【0008】

ボディエリアネットワークにおいてコーディネータ装置を用いて複数のオンボディ装置

10

20

30

40

50

を管理する方法の一例は、コーディネータ装置で送受信器によって通信チャンネルを獲得するステップを有する。上記方法は、オンボディ装置からコーディネータ装置情報に対する要求を受信するステップを有する。また、上記方法は、オンボディ装置からピコネットとの結合に対する接続要求(association request)を受信するステップを有する。接続要求は、一つ又はそれ以上のパラメータを含む。さらに、上記方法は、コーディネータ装置のために定義された複数の許可制御パラメータに基づいて接続要求を決定するステップを有する。また、上記方法は、この決定に基づいてメッセージ信号との接続要求を承認するステップを有し、メッセージ信号は、ピコネットでオンボディ装置に対する装置識別子を含む受諾メッセージ信号、及び接続要求を拒否するための理由を含む拒絶メッセージ信号のうちいずれか一つを含む。また、上記方法は、オンボディ装置を認証するステップ、認証に基づいて暗号化及び復号化のうちの一つを遂行するステップ、及びデータフレームに対してインテグリティ保護を可能にするステップのうちいずれか一つを含むセキュリティ制御フィールドに基づいてセキュリティ手順を開始するステップを有する。また、上記方法は、開始に基づいてコーディネータ装置とオンボディ装置との間でデータを交換するステップを有する。上記方法は、命令メッセージを送信してオンボディ装置を分離するステップを有し、命令メッセージは、ユニキャストメッセージ、マルチキャストメッセージ、及びブロードキャストメッセージのうちいずれか一つを含む。

【0009】

システムの一例は、ボディエリアネットワークを含むシステムである。ボディエリアネットワークは、複数のインプラント装置、複数のオンボディ装置、及び複数のインプラント装置と通信するコーディネータ装置を含む。コーディネータ装置は、コーディネータ装置と複数のインプラント装置との間で信号とデータを交換するための通信インターフェースを含む。コーディネータ装置は、コーディネータ装置でインプラント医療用通信サービス(MICS)送受信器によってMICSチャンネルを獲得するために通信インターフェースと電子通信するプロセッサを含む。プロセッサは、非MICSチャンネルでウェイクアップ過程(process)を指示する信号をインプラント装置に送信する。また、プロセッサは、MICS送受信器によってピコネットとの結合を指示する命令信号をインプラント装置に送信する。命令信号は、装置識別子を含む。また、プロセッサは、命令信号をインプラント装置に送信することに基づいてコーディネータ装置のMICS送受信器によって承認信号を受信する。承認信号は、セキュリティ制御フィールドを含む。また、プロセッサは、セキュリティ制御フィールドに基づいて、インプラント装置を認証し、認証に基づいて暗号化及び復号化の中の一つを遂行し、再生保護を遂行し、データフレームに対するインテグリティ保護を可能にするセキュリティ手順を開始する。プロセッサは、開始に基づいてコーディネータ装置とインプラント装置との間でデータを交換する。また、プロセッサは、命令メッセージを送信してインプラント装置を分離する。この命令メッセージは、ユニキャストメッセージ、マルチキャストメッセージ、及びブロードキャストメッセージのうちいずれか一つを含む。複数のオンボディ装置と通信するコーディネータ装置は、コーディネータ装置と複数のオンボディ装置との間で信号とデータを交換するための通信インターフェースを含む。コーディネータ装置は、コーディネータ装置内の送受信器によって通信チャンネルを獲得するために通信インターフェースと電子通信をする前記プロセッサを含む。プロセッサは、オンボディ装置からコーディネータ装置情報に対する要求を受信する。また、プロセッサは、オンボディ装置からピコネットとの結合に対する接続要求を受信する。接続要求は、一つ又はそれ以上のパラメータを含む。また、プロセッサは、コーディネータ装置に対して定義された複数の許可制御パラメータに基づいて接続要求を決定する。また、プロセッサは、決定に基づいてメッセージ信号で接続要求を承認する。メッセージ信号は、ピコネットでオンボディ装置に対する装置識別子を含む受諾メッセージ信号、及び前記接続要求を拒絶するための理由を含む拒絶メッセージ信号を含む。また、プロセッサは、セキュリティ制御フィールドに基づいて、オンボディ装置を認証し、認証に基づいて暗号化及び復号化中の一つを遂行し、再生保護を実行し、データフレームに対するインテグリティ保護を可能にするセキュリティ手順を開始する。プロセッサは、また

10

20

30

40

50

開始に基づいてコーディネータ装置とオンボディ装置との間でデータを交換する。また、プロセッサは、命令メッセージを送信してオンボディ装置を分離し、この命令メッセージは、ユニキャストメッセージ、マルチキャストメッセージ、及びブロードキャストメッセージのうちいずれか一つを含む。

【発明の効果】

【0010】

本発明は、コーディネータ装置を用いてインプラント装置とオンボディ装置を含むボディエリアネットワークを管理するための方法及びシステムを提供できる。

【図面の簡単な説明】

【0011】

10

【図1】多様な実施形態が実行できる環境のブロック構成図である。

【図2】一実施形態によるコーディネータ装置のブロック構成図である。

【図3】一実施形態によるコーディネータ装置を用いて、ボディエリアネットワークで複数のインプラント装置を管理する方法を示すフローチャートである。

【図4】一実施形態によるコーディネータ装置を用いて、ボディエリアネットワークで複数のインプラント装置を管理する方法を示すフローチャートである。

【図5】一実施形態によるボディエリアネットワークにおいて、コーディネータ装置によってチャンネルを獲得する方法を示すフローチャートである。

【図6】一実施形態によるウェイクアップ過程のフローを示す図である。

【図7】一実施形態によるコーディネータ装置でのウェイクアップ過程を示すフローチャートである。

20

【図8】一実施形態によるコーディネータ装置での他のウェイクアップ過程を示すフローチャートである。

【図9】他の実施形態によるウェイクアップ過程のフローを示す図である。

【図10】他の実施形態によるコーディネータ装置でのウェイクアップ過程を示すフローチャートである。

【図11】一実施形態によるコーディネータ装置を用いて、ボディエリアネットワークで複数のオンボディ装置を管理する方法を示すフローチャートである。

【図12】一実施形態によるコーディネータ装置を用いて、ボディエリアネットワークで複数のオンボディ装置を管理する方法を示すフローチャートである。

30

【図13】一実施形態によるオンボディ装置によってコーディネータ装置を発見する方法を示すフローチャートである。

【図14】一実施形態によるコーディネータ装置と一つのグループのオンボディ装置との間の認証及びセキュリティキー生成のための方法に対するフローを示す図である。

【図15】一実施形態によるコーディネータ装置によって複数のIMDと通信する方法を示すフローチャートである。

【図16】一実施形態によるグループ接続を可能にするために必要なグループ情報要素(IE)を示す図である。

【図17】一実施形態によるグループ接続を可能にするために必要なグループ情報要素(IE)を示す図である。

40

【図18】一実施形態によるグループ接続を可能にするために必要なグループ情報要素(IE)を示す図である。

【図19】一実施形態によるグループ接続を可能にするために必要なグループ情報要素(IE)を示す図である。

【図20】一実施形態によるグループ接続を可能にするために必要なグループ情報要素(IE)を示す図である。

【図21】一実施形態によるグループ接続を可能にするために必要なグループ情報要素(IE)を示す図である。

【図22】一実施形態によるグループ接続を可能にするために必要なグループ情報要素(IE)を示す図である。

50

【発明を実施するための形態】

【0012】

以下、本発明の望ましい実施形態を添付の図面を参照して詳細に説明する。

【0013】

方法段階とシステム構成要素は、但し本発明の理解に関連した特定の詳細を示す図で従来のシンボルによって表示されることに注目すべきである。また、当該技術分野で通常の知識を持つ者に公知されている詳細は開示しない。本発明において、第1及び第2のような関連用語は、エンティティ間の実際的な関係又は順序を必ずしも暗示するとはいえず、一つのエンティティを他のエンティティと区別するために使われる。

【0014】

本明細書に記載される実施形態は、コーディネータ装置を用いてインプラント装置とオンボディ装置とを含むボディエリアネットワークを管理するための方法及びシステムを提供する。

【0015】

図1は、多様な実施形態が実行できる環境100のブロック構成図である。この環境は、ボディエリアネットワーク(BAN)であり得る。

【0016】

環境100は、コーディネータ装置105と複数のインプラント装置(IMD)、例えばインプラント装置110a及びインプラント装置110bを含む。環境100は、また複数のオンボディ装置(OBD)、例えばオンボディ装置115a及びオンボディ装置115bを含む。コーディネータ装置105は、IMD及びOBDと電子通信を遂行する。コーディネータ装置105は、例としてコンピュータ、ラップトップコンピュータ、モバイルデバイス、携帯用デバイス、個人用携帯情報端末(PDA)、及び医療用アプリケーションに使用される電子装置を含み、これらに限定されるものではない。IMDは、生物体内に移植される電子デバイスである。OBDは、生物体上に又は生物体に近く位置するデバイスである。コーディネータ装置105は、生物体上に又は生物体に近接するように位置してチャンネルを制御し、一つ又はそれ以上のIMD及びOBDにネットワークアクセスを提供するデバイスである。

【0017】

IMD及びOBDは、コーディネータ装置とのデータ通信のために使われる。例えば、ボディエリアネットワーク(BAN)は、コーディネータ装置105と通信する電子デバイスを含む。

【0018】

コーディネータ装置105とIMD及びOBDの間には多重通信チャンネルが存在し、データの通信は、通信チャンネルのうちいずれか一つを利用して行われる。一実施形態において、IMD110aは、スリープ(sleep)状態にあり、コーディネータ装置105は、データ通信のためにIMD110aにウェイクアップ信号を送信する。他の実施形態において、コーディネータ装置105は、データ通信のためにOBD115aから要求を受信する。

【0019】

コーディネータ装置105は、非常信号を識別するための一つ又はそれ以上の要素を含む。要素を含むコーディネータ装置105は、図2で詳細に説明される。

【0020】

図2は、一実施形態によるコーディネータ装置105を示すブロック構成図である。コーディネータ装置105は、情報を通信するためのバス205と、情報を処理するためにバス205に結合されるプロセッサ210とを含む。また、コーディネータ装置105は、メモリ215、例えばプロセッサ210により要求される情報を格納するためにバス205に結合されるRAM(Random Access Memory)を含む。メモリ215は、プロセッサ210により要求される臨時情報を格納するために使用できる。コーディネータ装置105は、プロセッサ210により要求される静的情報を格納するためにバス205に結合さ

10

20

30

40

50

れるROM(Read Only Memory) 220をさらに含む。格納部225、例えば磁気ディスク、ハードディスク、又は光ディスクは、情報を格納するためにバス205に提供及び結合することができる。

【0021】

コーディネータ装置105は、バス205を介して情報をディスプレイするためのディスプレイ230、例えばCRT(Cathode Ray Tube)又はLCD(Liquid Crystal Display)に接続される。多様なキーを含む入力装置235は、情報をプロセッサ210に通信するためにバス205に接続される。プロセッサ210に情報を通信するために使用されるカーソル制御器240、例えばマウス、トラックボール、ジョイスティック、又はカーソル方向キーは、コーディネータ装置105に結合することができる。

10

【0022】

一部の実施形態において、本発明の段階は、プロセッサ210を用いてコーディネータ装置105により遂行される。この情報は、機械読み取り可能な媒体(machine-readable medium)、例えば格納部225からメモリ215に読み取り可能である。他の実施形態において、ハードワイヤード回路(hard-wired circuitry)は、多様な実施形態を実行するためにソフトウェア命令を代替し、あるいは組み合わせて使われることができる。

【0023】

機械読み取り可能な媒体は、機械が特定機能を遂行するように機械にデータを提供する媒体として定義される。この機械読み取り可能な媒体は、格納媒体であり得る。格納媒体は、不揮発性媒体と揮発性媒体を含むことができる。この格納部225は、不揮発性媒体であり得る。メモリ215は、揮発性媒体であり得る。このようなすべての媒体は、媒体に格納されている命令を機械内に読み取る物理的メカニズムにより感知されるように実在するものでなければならない。

20

【0024】

機械読み取り可能な媒体の例としては、フロッピー（登録商標）ディスク、フレキシブルディスク、ハードディスク、磁気テープ、CD-ROM、光ディスク、パンチカード、ペーパーテープ、RAM、PROM、EPROM、及びFLASH-EPROMを含み、これらに限定されない。

【0025】

コーディネータ装置105は、信号及びデータ通信を可能にするために、バス205に接続された通信インターフェース245を含む。通信インターフェース245は、例としてジグビーポート、又はIEEE(Institute of Electrical and Electronic Engineers) 802.15.6タスクグループによって規定された無線ポートを含み、これに限定されるものではない。通信インターフェース245は、IMD及びOBDと電子通信を遂行する。多重通信チャンネルが通信インターフェース245と接続することができる。

30

【0026】

一部の実施形態において、プロセッサ210は、自身の一つ又はそれ以上の機能を遂行するための一つ又はそれ以上の処理装置を含むことができる。この処理装置は、特定機能を遂行するハードウェア回路である。

【0027】

40

一つ又はそれ以上の機能は、コーディネータ装置105でインプラント医療用通信サービス(medical implant communication service: MICS)送受信器によってMICSチャンネルを獲得するステップを含む。この機能は、非MICSチャンネルでインプラント装置、例えばIMD110aにウェイクアップ過程を指示する信号を送信するステップを有する。また、この方法は、MICS送受信器によってインプラント装置にピコネットとの接続を指示する命令信号を送信するステップを有する。命令信号は、装置識別子を含む。また、この機能は、命令信号をインプラント装置に送ることに基づいてコーディネータ装置105のMICS送受信器によって承認信号を受信するステップをさらに有する。承認信号は、セキュリティ制御フィールドを含む。また、この機能は、セキュリティ制御フィールドに基づいてIMD110aを認証するステップ、この認証に基づいて暗号化及

50

び復号化のうちの一つを遂行するステップ、再生保護を実行するステップ、及びデータフレームに対するインテグリティ(integrity)保護を可能にするステップを含むセキュリティ手順を開始するステップを有する。また、この機能は、開始に基づいてコーディネータ装置105とIMD110aとの間でデータを交換するステップ及び命令メッセージを送信してIMD110aを分離(disassociating)するステップを有する。命令メッセージは、ユニキャストメッセージ、マルチキャストメッセージ、及びブロードキャストメッセージのうちいずれか一つを含む。

【0028】

OBDとの通信のために、プロセッサ210の機能は、コーディネータ装置105で受信器によって通信チャンネルを獲得するステップを有する。この機能は、オンボディ装置、例えばOBD115aからコーディネータ装置情報のための要求を受信するステップを有する。また、この機能は、オンボディ装置からピコネットとの接続のための接続要求を受信するステップを有する。また、接続要求は、一つ又はそれ以上のパラメータを含む。また、この機能はコーディネータ装置105に対して定義された複数の許可制御パラメータに基づいて接続要求を決定するステップを有する。この機能は、決定に基づいてメッセージ信号で接続要求を承認するステップを有する。メッセージ信号は、ピコネットでOBD115aに対する装置識別子を含む受諾メッセージ信号と接続要求を拒絶する理由を含む拒絶メッセージ信号のうちいずれか一つを含む。上記機能は、セキュリティ制御フィールドに基づいてOBD115aを認証するステップ、認証に基づいて暗号化及び復号化のうちの一つを遂行するステップ、及びデータフレームに対するインテグリティ保護を可能にするステップのうちいずれか一つを含むセキュリティ手順を開始するステップを有する。また、この機能は、開始に基づいてコーディネータ装置105とOBD115aとの間でデータを交換するステップを有する。また、この機能は、命令メッセージを送信してOBD115aを分離するステップを有する。命令メッセージは、ユニキャストメッセージ、マルチキャストメッセージ、及びブロードキャストメッセージのうちいずれか一つを含む。

【0029】

各IMD、例えば、IMD110a、及び各OBD、例えば、OBD115aは、構造的にコーディネータ装置105に類似することができ、コーディネータ装置115のために示すような多様な要素を備えることに注意すべきである。図2のコーディネータ装置105の各要素の機能性は、プロセッサ210を除いてはIMD110a及びOBD115aと同様であり得る。

【0030】

図3乃至図4は、コーディネータ装置、例えばコーディネータ装置105を用いてボディエリアネットワーク内の複数のインプラント装置(IMD)を管理するための方法を示すフローチャートである。

【0031】

一実施形態において、IMD、例えばIMD110aは、ディープスリープモードである。ディープスリープモードは、IMDが電源は供給されるが非動作状態にあるとして定義され得る。ディープスリープモードでは、非MICS受信器のエネルギー検出器がデュエティサイクリングモードで活性化される。IMDは、非常状態で又はウェイクアップ過程がコーディネータ装置によって開始されるときに動作する。

【0032】

上記方法は、ステップ305で開始する。

【0033】

ステップ310で、MICSチャンネルは、コーディネータ装置でMICS送受信器によって獲得される。MICSチャンネルは、最初に所定の期間でMICSチャンネルを感知する。MICSチャンネルが、如何なる干渉もないと決定されると、MICSチャンネルが通信のためにコーディネータ装置によって獲得される。

【0034】

また、M I C Sチャンネルを獲得した後に、獲得されたM I C Sチャンネル上の非活性期間が予め定義された期間と同一であり、あるいは超えると、コーディネータ装置は、パケット、例えばヌルパケット(null packet)を送信してM I C Sチャンネルを維持できる。

【0035】

ステップ315で、ウェイクアップ過程を指示する信号が非M I C SチャンネルでIMDに送信される。この信号は、IMDでウェイクアップ過程を開始するためにコーディネータ装置によって送信されることができる。この信号は、非M I C S送信器、例えば2.4GHzを用いてコーディネータ装置によって送信される。この信号は、M I C Sチャンネルと関連した情報を含む。

10

【0036】

一実施形態において、非M I C S帯域は、同一に位置した同一の帯域幅のN個のチャンネルに分割される。IMDとコーディネータ装置両方は、干渉が大きいチャンネルを避ける。しかしながら、干渉レベルは、IMDとコーディネータ装置の両方に対して相互に異なることができる。例えば、コーディネータ装置に対して管理可能な干渉レベルがIMDからより低く設定することができる。

【0037】

非M I C S帯域のチャンネルで干渉が検出されないと、コーディネータ装置は、信号を搬送波感知多重アクセス及び衝突回避技術を用いてウェイクアップ過程の開始を指示するIMDに上記信号を送信する。この信号は、管理可能な干渉レベル内で非M I C Sチャンネルで送信される。一部の実施形態において、上記信号が信頼性を増大させるために管理可能な干渉レベル内で各非M I C Sチャンネルでまた送られることができる。一部の実施形態では、承認がコーディネータ装置によって受信されるまでランダムな順序で管理可能な干渉レベル内で非M I C Sチャンネルで送信される。

20

【0038】

ディープスリープモードで、より少ない干渉を有する非M I C SチャンネルでIMDデュティは、エネルギー検出器上でサイクリングされる。この信号を受信すると、IMDは、承認信号を送ることができる。

【0039】

一部の実施形態において、承認信号は、IMDへの上記信号の送信に基づいてコーディネータ装置のM I C S送受信器によって受信される。

30

【0040】

一部の実施形態において、定義された期間内にインプラント装置から承認信号が受信されるまで、上記信号は、非M I C Sチャンネル上に再送信される。一部の実施形態で、信号が定義された期間内に、承認信号がM I C Sチャンネルで受信されないと、この信号は、他の非M I C Sチャンネル上に再送信される。

【0041】

ステップ320で、ピコネットとの結合を指示する命令信号がM I C S送受信器によってインプラント装置に送信される。命令信号は、コーディネータ装置によって指定されたIMD用の装置識別子を含む。

40

【0042】

一実施形態で、命令信号は、インプラント装置への信号送信に応答して送信される承認信号を受信した後に送信される。

【0043】

ステップ325で、承認信号は、インプラント装置に送られた命令信号に基づいてコーディネータ装置のM I C S送受信器によって受信される。承認信号は、IMDでセキュリティ要件を定義するセキュリティ制御フィールドを含む。

【0044】

一部の実施形態において、IMDは、セキュリティ制御フィールドを有する承認信号が送信される前にこの信号と命令信号が受信されるまで待機する。

50

【0045】

ステップ330で、セキュリティ手順は、セキュリティ制御フィールドに基づいて開始される。

【0046】

セキュリティレベルは、一つのバイトビットマップを用いてセキュリティ制御フィールドに表示される。各ビットは、次のようにセキュリティ特性のサポートを指示するために使用される。

ビット0－認証

ビット1－インテグリティ保護

ビット2－暗号化及び復号化

ビット3－フレームカウンタを用いる再生保護

ビット4－一つのセッションですべてのフレームに対する同一のセキュリティ

ビット5－キーサイズ192ビット

ビット6－キーサイズ256ビット

ビット7－将来の使用のために予備(RFU)

10

【0047】

セキュリティが必要でない場合、セキュリティ制御フィールドのビットは、0に設定される。使用されるデフォルトキーサイズは、128ビットキーとして設定される。セキュリティの異なるレベルは、一つのバイトビットマップを用いて多様なデバイスに対して実行することができる。IMDにより指示されるセキュリティレベルが許容されないと、コーディネータ装置は、接続に失敗する可能性がある。セキュリティ制御フィールドは、セキュリティ制御、アプリケーションによって相互に異なるセキュリティ特性が各フレームに対して選択される接続手順の間に交換されるアプリケーションパラメータフィールド、及びBAN装置要件を用いてMACフレームにフレームレベルセキュリティを定義する。一部の実施形態において、フレームレベルセキュリティは、類似したフレームレベルセキュリティがセキュリティ保護を必要とするフレームに対して均一に使用される接続手順の間に識別される。

20

【0048】

一部の機能(capabilities)は、セキュリティレベルの実行のためにコーディネータ装置とIMDで遂行される。

30

【0049】

コーディネータ装置は、次のような詳細を有するように事前構成することができる。

IMDがサポートするとコーディネータ装置が期待する最小セキュリティモード。

【0050】

セキュリティテーブルは、次のフィールドを含むコーディネータ装置の不揮発性メモリに格納される。

各クライアントデバイス用共有キー(マスターキーID(MKID))と呼ばれる識別子によって識別される複数のキー)。この場合にクライアントデバイスは、IMDであり得る。

40

デバイスID、MACアドレス、デバイスのタイプ、クライアントにより提供されるサービス。このような情報は、接続手順によって予め格納され、あるいは収集できることである。この情報は、クライアントデバイスがコーディネータ装置から分離された後にクライアントデバイス内に保持される。

【0051】

また、BAN装置は、コーディネータ装置のようにセキュリティキーと該当MKIDで事前構成することができる。デバイスID、MACアドレス、デバイスのタイプ、クライアントデバイスによって提供されるサービスがクライアントデバイスで事前構成することができる。

【0052】

IMDとコーディネータ装置は、キーが以後セッションで再交渉されるまで臨時キーと

50

フレームカウンタを格納する機能を有する。

【0053】

ステップ335で、IMDは、マスターキーがコーディネータ装置とIMDとの間で共有されることを認める4方式のハンドシェイク(handshake)手順を用いて認証される。

【0054】

ステップ340で、暗号化と復号化を可能にするペアワイズキー生成が認証に基づいて遂行される。例えば、AES-128カウンタモードがデータ暗号化のために使われることができる。

【0055】

ステップ345で、再生保護が実行される。

10

【0056】

フレームカウンタは再生保護のために使用される。2バイトフレームカウンタが使われることができる。以前セッションからのフレームカウンタの値はコーディネータ装置とIMDに格納する必要がある。以後セッションは、以前セッションから格納されたフレームカウンタから続けてカウンティングし、あるいは新たなランダムフレームカウンタで再び開始することを選択できる。

【0057】

ステップ350で、データフレームに対するインテグリティ保護が可能である。

【0058】

AES-128暗号ブロック連鎖メッセージ認証コード(Cipher Block Chaining-Message Authentication Code: CBC-MAC)は、インテグリティチェック計算のために使用できる。インテグリティチェックは、データフレームに含まれることができる。

20

【0059】

MACプロトコルは、IMDとコーディネータ装置から送信されたデータフレームに使用されるプライバシーとインテグリティ保護を選択的に使用することができる。セキュリティヘッダーフィールドは、このような選択を指示するために使われる。コーディネータ装置から送られた標準フレーム、例えばポール(poll)又は他の制御フレームは、暗号化され、あるいはインテグリティ保護される必要がない。

【0060】

ステップ355で、データは、ステップ330での開始に基づいてコーディネータ装置とIMDとの間で交換される。データ交換は、ステップ330で定義されたセキュリティ手順に基づいて遂行できる。

30

【0061】

コーディネータ装置が複数のIMDと通信する場合に、データは、コーディネータ装置によってブロードキャストイングされ、あるいは各IMDに個別的に送信することができる。データを受信すると、各IMDは、コーディネータ装置に応答を送る。このようなデータの例としては、命令信号、データフレーム、ポールメッセージ、データ要求、制御信号、及び動作信号を含み、これらに限定されるものではない。例えば、IMDがコーディネータ装置からデータフレームを受信する場合、IMDは、データ承認信号をコーディネータ装置に送信する。一部の実施形態において、コーディネータ装置からデータを受信すると、応答がIMDにより送信されない。

40

【0062】

ステップ360で、インプラント装置は、命令メッセージを送信して分離される。命令メッセージは、ユニキャストメッセージ、マルチキャストメッセージ、及びブロードキャストメッセージのうちいずれか一つを含む。分離は、IMDに命令メッセージを送信して装置識別子を解除して遂行できる。

【0063】

一実施形態において、コーディネータ装置は、エンドセッションメッセージをIMDにブロードキャストイング又はマルチキャストイングして複数のIMDを分離できる。

【0064】

50

一部の実施形態では、IMDは、コーディネータ装置から分離できる。

【0065】

上記方法は、ステップ365で終了する。

【0066】

一部の実施形態において、コーディネータ装置は、非常イベントを有するIMDから非常信号を受信するための他のMICS送受信器又はMICS受信器を含むことができる。他のMICS送受信器又はMICS受信器は、非常信号を聞くためにより少ない干渉を有するMICSチャンネルでデューティサイクリングできる。受信された複数の信号が非ボディアエリアネットワーク信号であると、非MICSチャンネルの受信器周波数は、受信器周波数に比べてより少ない干渉を有する他の周波数にシフトされる。非常信号は、受信された非常信号でペイロードヘッダーを用いて識別できる。

10

【0067】

一実施形態において、他のMICS送受信器で非常信号を受信すると、コーディネータ装置はIMDと進行中である通信を中断させ、MICS送受信器は非常状況に対処するために他のインプラント装置と通信を始める。

【0068】

他の実施形態において、他のMICS送受信器で非常信号を受信すると、コーディネータ装置は、正常な通信を中断することなく非常事態を処理する。

【0069】

一実施形態において、コーディネータ装置は、第1のIMDと通信する。このコーディネータ装置は、第2のIMDに接続するように要求される。この場合、コーディネータ装置は、第1のIMDに保持命令を受信すると、第1のIMDは、スリープモードに進み、あるいはスイッチオフされる。第1のIMDは、所定の時間以後に、又は所定の期間にわたって周期的に動作するように開始される。その後、コーディネータ装置は、図3及び図4に示された方法に基づいて第2のIMDとの接続を開始する。第2のIMDとの接続を達成すると、コーディネータ装置は、第1のIMDに非保持(unhold)命令を送信する。一実施形態において、第1のIMDは、所定時間の完了後に動作される。

20

【0070】

第2の実施形態において、コーディネータ装置は、MICSチャンネルで第1のIMDと通信する。コーディネータ装置は、第2のIMDに接続するように要求される。コーディネータ装置は、非MICSチャンネルで第2のIMDにウェイクアップ信号を送信する。ウェイクアップ信号を受信すると、第2のIMDは、搬送波感知多重アクセス及び衝突回避技術を用いてMICSチャンネルで承認信号を送信する。コーディネータ装置が承認信号を受信する場合に、コーディネータ装置は、図3及び図4で説明した方法に基づいて第2のIMDとの接続を開始する。

30

【0071】

図5は、一実施形態によるボディアエリアネットワークにおけるコーディネータ装置によってチャンネルを獲得する方法を示すフローチャートである。

【0072】

上記方法は、ステップ405で開始する。

40

【0073】

ステップ410で、複数のチャンネルでエネルギー検出スキャンが遂行される。各チャンネルは、エネルギーを検出するために所定の期間で感知される。

【0074】

ステップ415で、フリーチャンネルのリストが決定される。フリーチャンネルリストは、低い干渉でチャンネルを識別して決定することができる。

【0075】

一実施形態において、フリーチャンネルが決定されないと、チャンネル獲得のための上記方法は終了する。

【0076】

50

ステップ420で、少なくとも干渉を有するチャンネルがフリーチャンネルリストから選択される。

【0077】

ステップ425で、チャンネル獲得メッセージは、チャンネルがBANの他のコーディネータ装置によって活用されるか否かを決定するためにブロードキャストされる。

【0078】

ステップ430で、ブロードキャストされたメッセージに対して応答が受信されたか否かが決定される。応答が受信されない場合には、ステップ435が遂行される。

【0079】

選択されたチャンネルが他のコーディネータ装置によって活用されていることを示す応答が受信されると、ステップ415が遂行される。

10

【0080】

上記方法は、ステップ435で終了する。

【0081】

図6は、一実施形態によるウェイクアップ過程のフローを示す。

【0082】

このフロー図は、コーディネータ装置、例えばコーディネータ装置105及び現在ディープスリープモードであるIMD、例えばIMD110a間の通信のためのMICSチャンネルでポーリング(polling)が使用されない場合のウェイクアップ過程を示す。

【0083】

20

最初に、MICS送受信器は、MICSチャンネル獲得を遂行するためにコーディネータ装置105によってスイッチオンされる。また、IMD110aで、非MICS受信器は、ウェイクアップ信号を聞くためにスイッチオンされる。

【0084】

MICSチャンネルを獲得すると、非MICS送信器がコーディネータ装置105によりスイッチオンされ、MICSチャンネル情報を含むウェイクアップ信号はIMDに送信される。IMD110aでの非MICS受信器は、ウェイクアップ信号を受信し、IMDに指示する。IMD110aは、ウェイクアップ過程が完了したことを指示するコーディネータ装置105に承認信号を送信するためにIMDのMICS送受信器をスイッチオンする。コーディネータ装置は、承認信号を受信すると、非MICS送信器をスイッチオフする。

30

【0085】

図7は、一実施形態によるコーディネータ装置、例えばコーディネータ装置105でのウェイクアップ過程を示すフローチャートである。

【0086】

上記方法は、ステップ605で開始する。

【0087】

ステップ610で、ウェイクアップ信号は、コーディネータ装置によってIMDに送信される。コーディネータ装置は、承認信号を受信するために所定時間を待機する。

【0088】

40

ステップ615で、承認信号が受信されたか否かを決定する。

【0089】

承認信号が受信されない場合には、ステップ620が遂行され、そうでない場合には、ステップ625が遂行される。

【0090】

ステップ620で、ウェイクアップ信号を送信する最大再試行が遂行されるか否かが決定される。

【0091】

最大再試行が遂行される場合には、ステップ625が遂行され、そうでないと、ステップ610が遂行される。

50

【0092】

一実施形態において、最大再試行が遂行されると、図7の方法は他のMICSチャンネルを用いて遂行される。

【0093】

上記方法は、ステップ625で終了する。

【0094】

図8は、一実施形態によるコーディネータ装置、例えばコーディネータ装置105での他のウェイクアップ過程を示すフローチャートである。

【0095】

上記方法は、ステップ705で開始する。

10

【0096】

ステップ710で、ウェイクアップ信号は、所定の期間でコーディネータ装置によってIMDに送信される。所定の期間中に、ウェイクアップ信号は、非MICSチャンネルでIMDに連続してN回送信される。

【0097】

ステップ715で、ウェイクアップ信号は、すべての非MICSチャンネルで送信されるか否かが決定される。

【0098】

すべての非MICSチャンネルが活用されると、ステップ720が遂行され、そうでない場合には、ステップ710が他のMICSチャンネルに対して遂行される。

20

【0099】

上記方法は、ステップ720で終了する。

【0100】

図9は、他の実施形態によるウェイクアップ過程のフローを示す。

【0101】

フロー図は、コーディネータ装置105とディープスリープモードであるIMD110aとの間の通信のためにポーリングが使用される場合のウェイクアップ過程を示す。

【0102】

最初に、MICS送受信器は、MICSチャンネルの獲得を遂行するためにコーディネータ装置105によってスイッチオンされる。また、IMD110aで、非MICS受信器は、ウェイクアップ信号を聞くためにスイッチオンされる。

30

【0103】

MICSチャンネルを獲得すると、非MICS送信器は、コーディネータ装置105によりスイッチオンされ、ウェイクアップ信号はIMDに送信される。IMD110aでの非MICS受信器は、ウェイクアップ信号を受信し、IMDに指示する。IMD110aは、非MICS受信器をスイッチオフし、ピコネットとの結合を指示する命令信号を待機する。命令信号を受信すると、IMD110aは、承認信号をコーディネータ装置105に送信ためにIMDのMICS送受信器をスイッチオンする。コーディネータ装置105は、承認信号を受信すると、非MICS送信器をスイッチオフし、ウェイクアップ過程は終了する。

40

【0104】

図10は、他の実施形態によるコーディネータ装置、例えばコーディネータ装置105でのウェイクアップ過程を示すフローチャートである。

【0105】

上記方法は、ステップ905で始まる。

【0106】

ステップ910で、ウェイクアップ信号は、コーディネータ装置によってIMDに送信される。

【0107】

ステップ915で、ピコネット結合を指示する命令信号は、ウェイクアップ信号を送信

50

する所定の期間以後に I M D に送られる。コーディネータ装置は、承認信号を受信するために他の期間の間に待機する。

【0108】

ステップ 920 で、承認信号が受信されたか否かが決定される。

【0109】

承認信号が受信されない場合、ステップ 925 が遂行され、そうでない場合には、ステップ 930 が遂行される。

【0110】

ステップ 925 で、ウェイクアップ信号を送信する最大再試行が遂行されるか否かが決定される。

10

【0111】

最大再試行が遂行されると、ステップ 930 が遂行され、そうでないと、ステップ 910 が遂行される。

【0112】

上記方法は、ステップ 930 で終了する。

【0113】

図 11 乃至図 12 は、コーディネータ装置、例えばコーディネータ装置 105 を用いてボディエリアネットワークで複数のオンボディ装置を管理する方法を示すフローチャートである。

【0114】

20

オンボディ装置、例えばオンボディ装置(OBD)115a は、オンボディ装置を扱う機能を有するコーディネータ装置の発見を遂行する。

【0115】

一実施形態において、コーディネータ装置は、ボディエリアネットワークで機能をブロードキャストできる。他の実施形態においては、オンボディ装置は、情報要求をコーディネータ装置に送ることができる。

【0116】

上記方法は、ステップ 1005 で開始する。

【0117】

ステップ 1010 で、通信チャンネルの周波数は、コーディネータ装置の送受信器により獲得される。

30

【0118】

周波数は、所定の期間で通信チャンネルの周波数を初期に感知することによって得られる。通信チャンネルでの周波数がいかなる干渉もないと決定される場合、コーディネータ装置は、通信チャンネルを獲得するためにチャンネル通知(announcement)を遂行する。チャンネル通知に対して応答が受信されない場合には、通信チャンネルが獲得される。

【0119】

ステップ 1015 で、コーディネータ装置情報に対する要求は、OBD から受信される。この要求は、コーディネータ装置の機能とコーディネータ装置用識別子を含む。

【0120】

40

コーディネータ装置は、その機能と識別子を送信できる。

【0121】

一実施形態において、コーディネータ装置情報は、コーディネータ装置によってブロードキャストできる。

【0122】

ステップ 1020 で、ピコネットとの結合のための接続要求が OBD から受信される。接続要求は、一つ又はそれ以上のパラメータ、例えばオンボディ装置情報、平均データレート、パケットサイズ、内部パケット到着時間、MAC 層で送信したパケットのサイズ、遅延要件、及びセキュリティ制御フィールドを含む。

【0123】

50

ステップ1025で、接続要求は、コーディネータ装置に対して定義された複数の許可制御パラメータに基づいて決定される。許可制御パラメータの例としては、保証されたタイムスロットの可用性(availability)を含み、これに限定されるものではない。

【0124】

ステップ1030で、接続要求は、決定に基づいてメッセージ信号で承認される。このメッセージは、ピコネットでOBDに対する装置識別子を含む受諾メッセージ信号、及び接続要求を拒絶する理由を含む拒絶メッセージ信号のうちいずれか一つであり得る。

【0125】

ステップ1035で、セキュリティ手順は、セキュリティ制御フィールドに基づいて開始できる。

【0126】

セキュリティ制御フィールド内のセキュリティレベルは、一つのバイトビットマップを用いて表示される。各ビットは、次のようにセキュリティ特性サポートを表すために使われる。

ビット0－認証

ビット1－インテグリティ保護

ビット2－暗号化及び復号化

ビット3－フレームカウンタを用いる再生保護

ビット4－一つのセッションですべてのフレームに対する同一のセキュリティ

ビット5－キーサイズ192ビット

ビット6－キーサイズ256ビット

ビット7－RFU

【0127】

セキュリティが必要でない場合、セキュリティ制御フィールド内のビットは0に設定される。デフォルトキーサイズは128ビットキーに設定できる。異なるレベルのセキュリティは、一つのバイトビットマップを用いて多様なデバイスに対して遂行できる。オンボディ装置によって指示されるセキュリティレベルが許容できないと、コーディネータ装置は、接続に失敗する。

【0128】

一部の機能は、セキュリティレベルの実行のためのコーディネータ装置とオンボディ装置で遂行される。

【0129】

コーディネータ装置は、次のような詳細を有するように予め構成される。

コーディネータ装置はオンボディ装置がサポートすると期待する最小セキュリティモード。

【0130】

セキュリティテーブルは、次のフィールドを含むコーディネータ装置の不揮発性メモリに格納される。

各クライアントデバイス用の共有キー(マスターキーID(MKID))と呼ばれる識別子により識別される複数のキー)。この場合にクライアントデバイスは、OBDであり得る。

デバイスID、MACアドレス、デバイスのタイプ、クライアントにより提供されるサービス。このような情報は、接続手順によって予め格納され、あるいは収集できることである。この情報は、クライアントデバイスがコーディネータ装置から分離された後にクライアントデバイス内に保持される。

【0131】

また、オンボディ装置は、コーディネータ装置のようにセキュリティキーと該当MKIDで事前構成することができる。デバイスID、MACアドレス、デバイスのタイプ、クライアントデバイスによって提供されるサービスがクライアントデバイスで事前構成することができる。

10

20

30

40

50

【0132】

オンボディ装置とコーディネータ装置は、キーが以後セッションで再交渉されるまで臨時キーとフレームカウンタを格納する機能を有する。

【0133】

フレームカウンタは、再生保護のために使われる。2バイトフレームカウンタが使用できる。以前セッションからのフレームカウンタの値は、コーディネータ装置とオンボディ装置に格納する必要がある。以後セッションは、以前セッションから格納されたフレームカウンタから続けてカウンティングし、あるいは新たなランダムフレームカウンタで再開することを選択できる。

【0134】

ステップ1040で、OBDは、マスターキーがコーディネータ装置とOBDとの間で共有されることを認める4方式のハンドシェイク手順を用いて認証される。

【0135】

ステップ1045で、暗号化と復号化を可能にするペアワイズキー生成は、認証に基づいて遂行される。AES-128カウンタモードは、データ暗号化のために使用することができる。

【0136】

ステップ1050で、再生保護が実行される。

【0137】

ステップ1055で、データフレームに対するインテグリティ保護が可能である。

【0138】

AES-128暗号ブロック連鎖メッセージ認証コード(CBC_MAC)は、インテグリティチェック計算のために使われることができる。インテグリティチェックは、データフレームに含まれることができる。

【0139】

MACプロトコルは、OBDとコーディネータ装置から送信されたデータフレームに使用されるプライバシーとインテグリティ保護を選択的に使用することができる。セキュリティヘッダーフィールドは、このような選択を指示するために使われる。コーディネータ装置から送信される標準フレーム、例えばポール又は他の制御フレームは、暗号化にされ、あるいはインテグリティ保護される必要がない。

【0140】

ステップ1060で、データは、開始に基づいてコーディネータ装置とオンボディ装置との間で交換される。

【0141】

ステップ1065で、オンボディ装置に指定された装置識別子は、コーディネータ装置によって分離される。分離は、分離命令信号をOBDに送信して装置識別子を解除して遂行できる。

【0142】

上記方法は、ステップ1070で終了する。

【0143】

図13は、一実施形態によるオンボディ装置、例えばオンボディ装置115aによってコーディネータ装置を発見する方法を示すフローチャートである。

【0144】

上記方法は、ステップ1105で開始する。

【0145】

ステップ1110で、コーディネータ装置からブロードキャストメッセージに対する受動スキャンが遂行される。

【0146】

ボディエリアネットワーク内のコーディネータ装置のリストは、通信チャンネルでコーディネータ装置からのブロードキャストされたメッセージに基づいて生成される。

10

20

30

40

50

ブロードキャストメッセージは、コーディネータ装置の機能と識別子を含むことができる。

【0147】

ステップ1115で、オンボディ装置の機能と識別子のマッチングが決定される。

【0148】

機能と識別子のマッチングが成功的であると、ステップ1130が遂行され、そうでない場合には、ステップ1120が遂行される。

【0149】

ステップ1120では、通信チャンネルのすべての周波数が受動スキャンングを遂行するために活用されるか否かが決定される。

10

【0150】

すべての周波数が活用される場合、ステップ1135が遂行され、そうでない場合には、ステップ1125が遂行される。

【0151】

ステップ1125で、通信チャンネルの周波数は、他の周波数にシフトされる。

【0152】

ステップ1130で、ステップ1115又はステップ1125で決定された機能及び識別子マッチングに基づいて、接続手順がコーディネータ装置で始まる。

【0153】

上記方法は、ステップ1135で終了する。

20

【0154】

図14は、一実施形態によるコーディネータ装置と複数のオンボディ装置との間での認証及びセキュリティキー生成方法のフローを示す。

【0155】

コーディネータ装置は、複数のオンボディ装置を示す代表デバイスから接続要求を受信する。複数のデバイスは、アプリケーションに基づいてグループ化でき、代表デバイスによって表示される。コーディネータ装置は、以後認証のための4方式のハンドシェイク手順を開始する。マスターキーは、代表デバイスとコーディネータ装置両方ともを認証するために使用される共有キーである。

【0156】

30

4方式のハンドシェイク手順が完了すると、コーディネータ装置は、代表ノードに該当するグループ識別子、複数のオンボディ装置に対する装置識別子、及びワンセットのセキュリティパラメータのうちいずれか一つを含むメッセージをブロードキャストする。セキュリティパラメータのセットは、コーディネータ装置と複数のオンボディ装置との間で共有されるマスターキーID(MKID)、クライアントノンス、コーディネータノンス、及び固有個別キーと共通キーがコーディネータ装置と複数のオンボディ装置との間での通信のために活用されるか否かを示すフラグビットを含む。コーディネータの認証中に交換されるノンス情報、代表ノード、デバイスグループのためにコーディネータによって割り当てられる装置識別子は、通信を確保するために使用される共通ペアワイズキー又は固有ペアワイズキーを生成するために各オンボディ装置によって使われる。装置識別子は、複数のオンボディ装置に対する個別装置識別子を含む。

40

【0157】

MKIDを用いて、コーディネータノンス、クライアントノンス、ここでグループキーとして知られている共通ペアワイズ臨時キー(PTK)は、コーディネータ装置と複数のオンボディ装置の各オンボディ装置により生成する。データ通信は、共通グループキーを用いてコーディネータ装置とデバイスグループの任意のデバイスとの間で確保される。

【0158】

また、コーディネータ装置は、コーディネータノンス及びクライアントノンスとともに各オンボディ装置の装置識別子を用いてデバイスグループの各オンボディ装置に対するペアワイズ固有キーを生成することができる。同様に、デバイスグループの各デバイスは、

50

オンボディ装置 I D、コーディネータノンス、及びクライアントノンスを用いてペアワイズ固有キーを生成させる。データ通信は、固有デバイスキーを用いてコーディネータ装置と任意のグループデバイスとの間で確保される。

【0159】

図15は、一実施形態によるコーディネータ装置、例えばコーディネータ装置105によって複数のIMDと通信する方法を示すフローチャートである。

【0160】

一部の場合に、一瞬間に複数のIMDと通信することが要求される。したがって、ウェイクアップ過程は、各IMDに対して同時に開始される必要がある。

【0161】

上記方法は、ステップ1305で開始する。

【0162】

ステップ1310で、ウェイクアップ過程は、IMDに対して開始される。ウェイクアップ過程は、IMDでプログラム化され、あるいはアプリケーションプログラムによって遂行することができる。

【0163】

IMDは、ステップ1315で、アイドルモード(idle mode)にある。

【0164】

ステップ1320で、MICSチャンネルが獲得される。MICSチャンネルの成功的な獲得は、ステップ1325でチェックされる。

【0165】

MICSチャンネルが成功的に獲得される場合には、ステップ1335が遂行され、そうでないと、最大再試行に対するチェックがステップ1330で遂行される。

【0166】

ステップ1335で、接続過程は、IMDの各々に対して順々(sequence)に又はバッチ(batch)処理して開始される。MICSチャンネルは、パケット、例えばヌルパケットを送信してさらに獲得できる。

【0167】

ステップ1340で、IMDの各々との成功的な接続がチェックされる。すべてのIMDと接続が成功でない場合、ステップ1355が遂行され、そうでない場合には、ステップ1345が遂行される。

【0168】

ステップ1345で、コーディネータ装置とIMDとの間でデータが交換され、ステップ1350が遂行される。

【0169】

ステップ1350で、IMDは、コーディネータ装置によって分離され、装置識別子は解除される。この分離はIMDに分離命令信号を送信して装置識別子を解除して遂行することができる。ステップ1380は、ステップ1350以後に遂行される。

【0170】

一部の実施形態において、IMDは、コーディネータ装置から分離される。

【0171】

ステップ1355で、各IMDとの接続要求条件がチェックされる。

【0172】

一部IMDのみが接続される必要である場合に、ステップ1360が遂行され、そうでないと、ステップ1365が遂行される。

【0173】

ステップ1360で、接続に失敗したIMDに対する最大再試行がチェックされる。最大再試行が完了すると、ステップ1370が遂行され、そうでないと、ステップ1335が遂行される。

【0174】

10

20

30

40

50

ステップ1365で、接続に失敗したIMDに対する最大再試行がチェックされる。最大再試行が完了すると、ステップ1375が遂行され、そうでないと、ステップ1335が遂行される。

【0175】

ステップ1370で、通信モードが接続されたIMDで開始され、ステップ1380が遂行される。

【0176】

ステップ1375で、コーディネータ装置が接続されたIMDから接続解除され、ステップ1380が遂行される。

【0177】

上記方法は、ステップ1380で終了する。

【0178】

図16乃至図21は、一実施形態によるグループ接続を可能にするために要求されるグループ情報要素(Information Element: IE)を示す。

【0179】

グループIEは、グループ接続要求、グループ接続応答、TDMA基盤のチャンネルアクセスメカニズムのためのブロードキャストメッセージでのグループ情報に対するグループIEを可能にする情報要素である。図16に示すように、上記情報用IEは、要素タイプフィールドを用いて識別される。長さフィールドは、グループIEの長さを提供する。

【0180】

グループ接続IEは、多くのノードカウンフィールドとグループ識別子を有する。一部の実施形態において、一つのフラグは、固有セキュリティキーとグループセキュリティキーのうちの一つであるセキュリティキー識別子を指示するために導入される。

【0181】

グループ接続要求に対する応答と共にコーディネータ装置からのブロードキャストメッセージとともに送信されるグループ応答IEは、要素タイプ、長さ、及び装置識別子を含むことができる。コーディネータ装置によってブロードキャストされたグループIEに対して、グループIEは、要素タイプ、長さ、グループ識別子、装置識別子、及びスロットプール(slot pool)情報を含む。グループIEに対する一部の実施形態において、装置識別子は、グループデバイスビットマップによって代替できる。グループIEに対する他の実施形態で、装置識別子は存在せず、デバイススロット割り当ては明示的スロット割り当てビットマップによって指示できる。

【0182】

図17で、スロット割り当ての範囲はデバイスに対して定義される。一実施形態において、スロット割り当ては、TDMAに基づいて連続的であり得る。他の実施形態において、スロット割り当ては、TDMAに基づいて非連続的であり得る。

【0183】

図18で、グループの識別子は、連続的なセットの装置識別子として定義される。

【0184】

図19で、コーディネータ装置により割り当てられたグループの識別子は非連続的である。

【0185】

図20で、デバイスがコーディネータ装置によってスロットが提供されるかを指示するデバイスビットマップが提供される。例えば、デバイスビットマップフィールドでのビット0が可能であると、デバイスグループの第1のデバイスは上記スロットが提供される。ビット1は、コーディネータ装置によってデバイスグループにスロットが提供されることを示すためにリセットされる。

【0186】

デバイスグループのうち一つのデバイスは異なる数のスロットが割り当てられる場合、デバイスは、図21に示すようにスロット割り当てビットマップを用いて定義されること

10

20

30

40

50

がある。スロット割り当てビットマップは、コーディネータ装置にスロットが提供されるデバイスに対する情報を含む。例えば、100は、4個のスロットが第1のデバイスに対して提供されることを示す。同様に、スロットは、コーディネータ装置によってスロットが割り当てられたデバイスに対して定義される。

【0187】

一部の実施形態において、デバイスビットマップとスロット割り当てビットマップは、図22に示すように、単一フィールド‘明示的スロット割り当てビットマップ’として表示可能である。図22で、第1のデバイスは、100により定義される4個のスロットを有する。第2のデバイスは、000により定義される0スロットを有することができる。

【0188】

以上、本発明の詳細な説明においては具体的な実施形態に関して説明したが、特許請求の範囲を外れない限り、様々な変更が可能であることは、当該技術分野における通常の知識を持つ者には明らかである。したがって、本発明の範囲は、前述の実施形態に限定されるものではなく、特許請求の範囲の記載及びこれと均等なものに基づいて定められるべきである。

【符号の説明】

【0189】

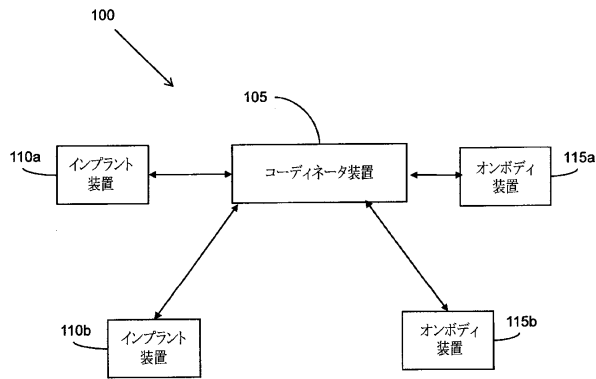
- 100 環境
- 105 コーディネータ装置
- 110a, 110b インプラント装置(IMD)
- 115a, 115b オンボディ装置(OBD)
- 205 バス
- 210 プロセッサ
- 215 メモリ
- 220 ROM(Read Only Memory)
- 225 格納部
- 230 ディスプレイ
- 235 入力装置
- 240 カーソル制御器
- 245 通信インターフェース

10

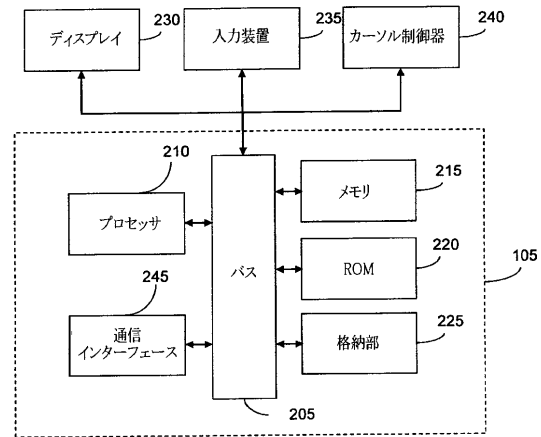
20

30

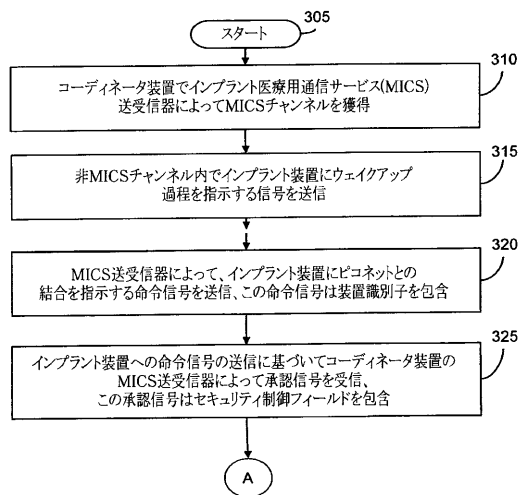
【図 1】



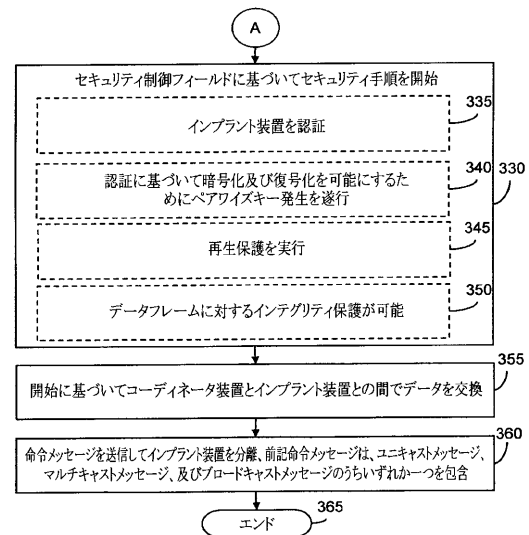
【図 2】



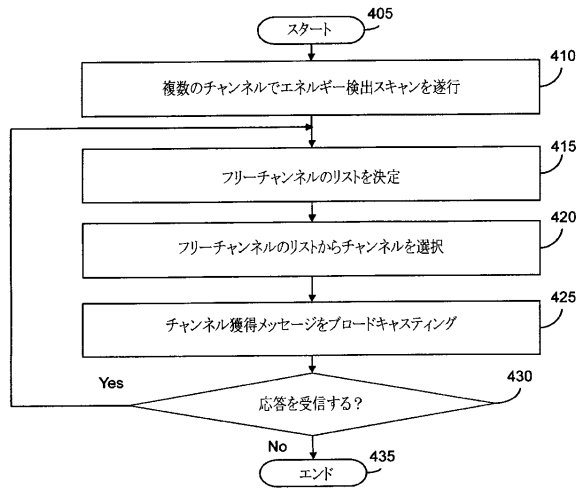
【図 3】



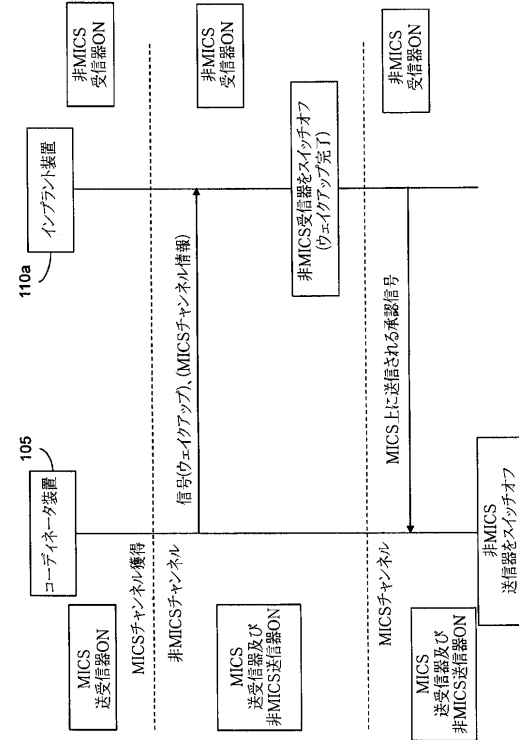
【図 4】



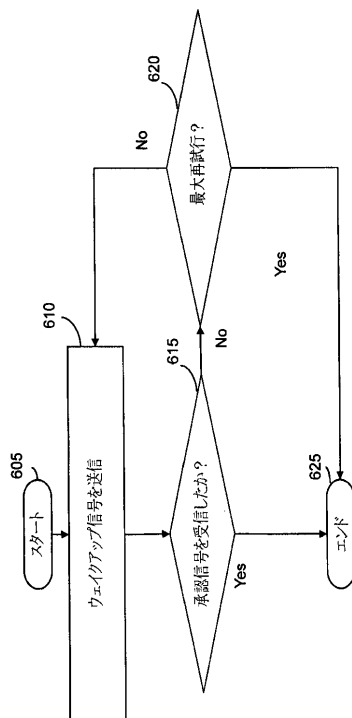
【図 5】



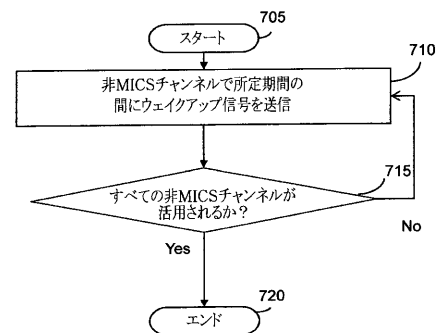
【図 6】



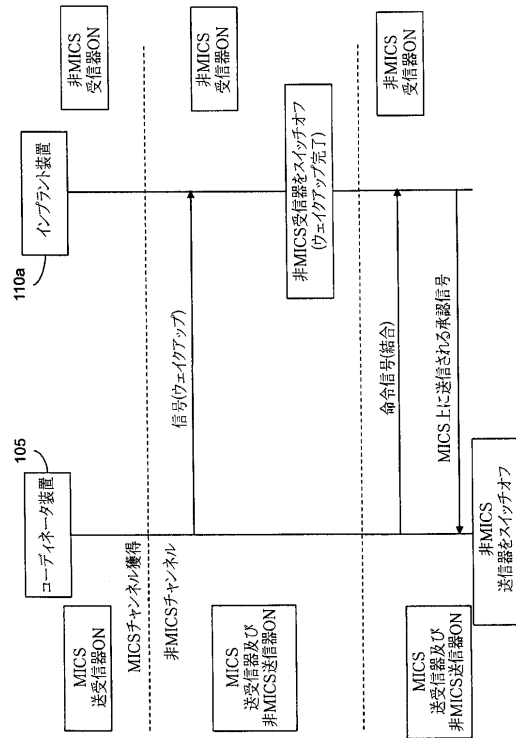
【図 7】



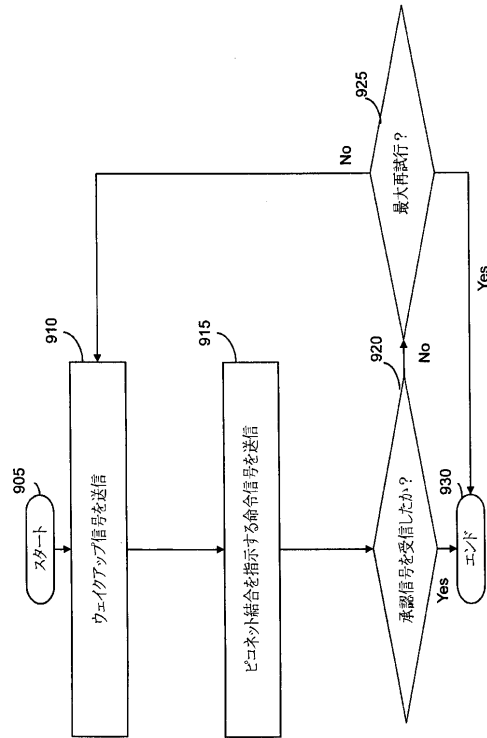
【図 8】



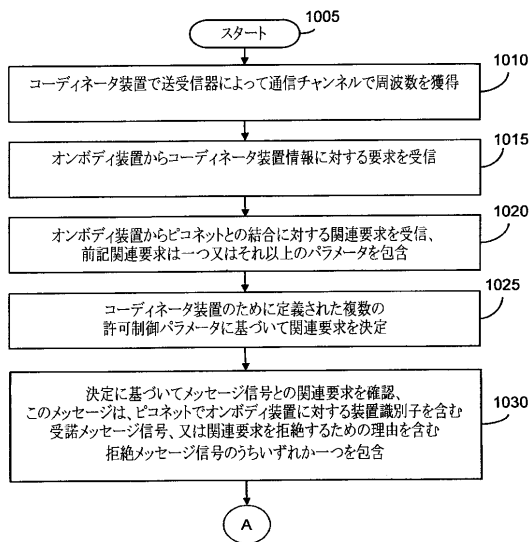
【図 9】



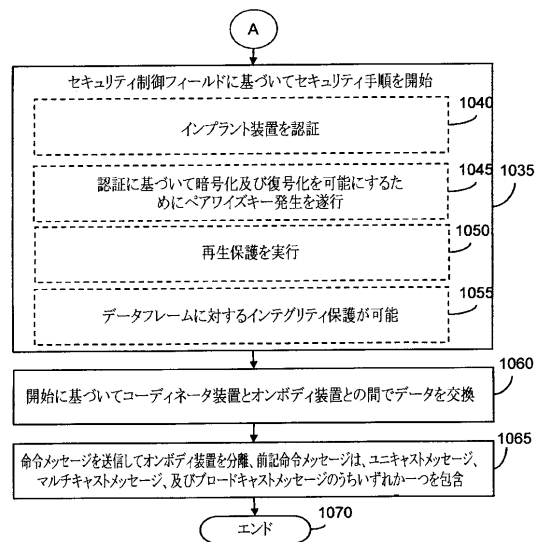
【図 10】



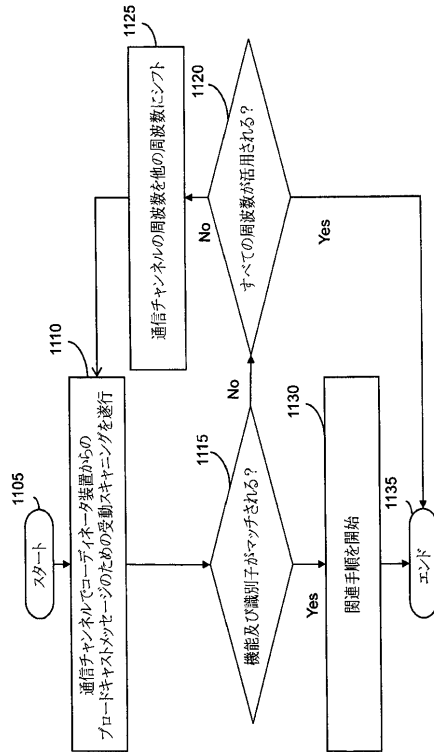
【図 11】



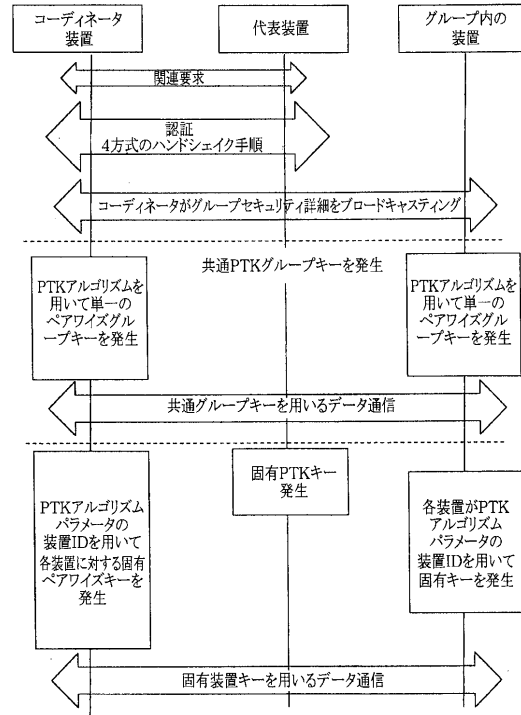
【図 12】



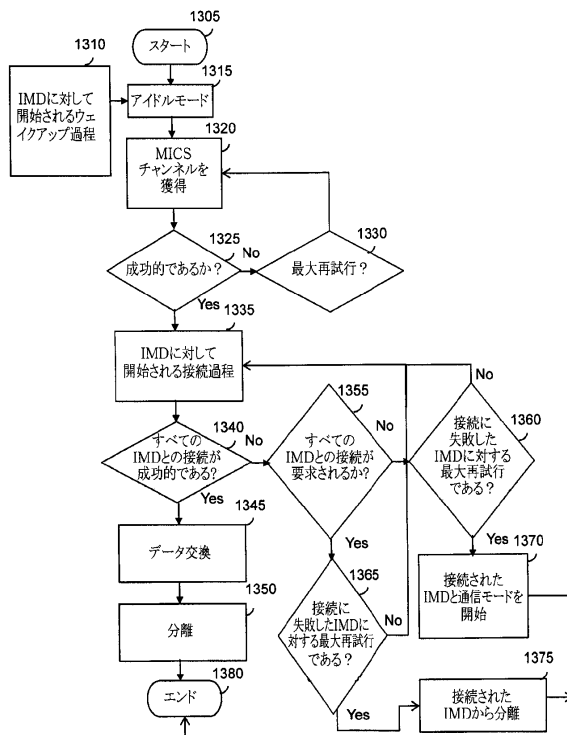
【図 13】



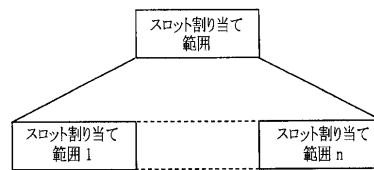
【図 14】



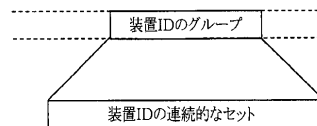
【図 15】



【図 17】



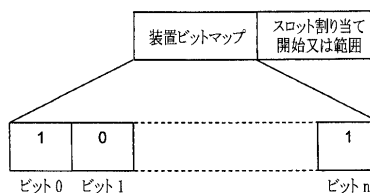
【図 18】



【図 19】



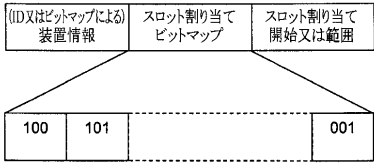
【図 20】



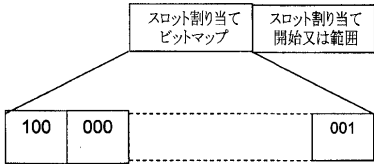
【図 16】

要素タイプ	長さ
-------	----

【図 2 1】



【図 2 2】



フロントページの続き

- (72)発明者 キラン・バイナム
インド・バンガロール・560024・ガンガナガル・エクステンション・アールビーアイ・コロ
ニー・ファースト・メイン・クリエイティブ・ヴィッラ・#44
- (72)発明者 テンモジ・アルナン
インド・バンガロール・560012・インディアン・インスティテュート・オブ・サイエンス・
オールド・イー・クォーターズ・イー-31
- (72)発明者 ユンテ・ウォン
大韓民国・ソウル・157-015・ガンソグ・ウージャンサンドン・1159・ウージャン
-サン・ヒュンデ・アイパーク・アパート・#115-2202

審査官 松野 吉宏

- (56)参考文献 Maulin Patel, Are MICS and MedRadio bands suitable for IEEE 802.15.6?, IEEE 802.15-08-0132-00-0006, 米国, IEEE mentor, 2008年 3月17日, slide 6,9,10,15,17,23, URL, <https://mentor.ieee.org/802.15/dcn/08/15-08-0132-00-0006-are-mics-and-medradio-bands-suitable-for-ieee-802-15-6.ppt>
- Kyungsup Kwak, Sana Ullah, Xizhi An, M.A.Ameen, Seokho Kim, Bumjung Kim, Youjin Kim, Youngwoo Choi, Hyungsoo Lee, Jaeyoung Kim, A Pattern-Based WBAN System with Bridging Mechanism, IEEE 802.15-09-0145-00-0006, 米国, IEEE mentor, 2009年 3月10日, slide 23-27,29,33,35, URL, <https://mentor.ieee.org/802.15/dcn/09/15-09-0145-00-0006-pattern-based-wban-system-with-bridging-mechanism.pdf>

(58)調査した分野(Int.Cl., DB名)

H04B	7/24	—	7/26
H04W	4/00	—	99/00