(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5536089号
(P5536089)
(45)発行日　平成26年7月2日(2014.7.2)　(24)登録日　平成26年5月9日(2014.5.9)

(51)Int.Cl.　　F I
H04W 12/04 (2009.01)　　H04W 12/04
H04W 84/18 (2009.01)　　H04W 84/18

請求項の数 14　(全 23 頁)

(21)出願番号　特願2011-537522 (P2011-537522)
(86)(22)出願日　平成21年11月13日 (2009.11.13)
(65)公表番号　特表2012-509646 (P2012-509646A)
(43)公表日　平成24年4月19日 (2012.4.19)
(86)国際出願番号　PCT/US2009/064405
(87)国際公開番号　WO2010/059522
(87)国際公開日　平成22年5月27日 (2010.5.27)
審査請求日　平成23年6月17日 (2011.6.17)
(31)優先権主張番号　12/272,988
(32)優先日　平成20年11月18日 (2008.11.18)
(33)優先権主張国　米国(US)

前置審査

(73)特許権者　595020643
クゥアルコム・インコーポレイテッド
ＱＵＡＬＣＯＭＭ　ＩＮＣＯＲＰＯＲＡＴＥＤ
アメリカ合衆国、カリフォルニア州　９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ　５７７５
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100109830
弁理士　福原　淑弘
(74)代理人　100103034
弁理士　野河　信久
(74)代理人　100075672
弁理士　峰　隆司

最終頁に続く

(54)【発明の名称】スペクトラム認可および関連通信の方法と装置

(57)【特許請求の範囲】
【請求項１】
第１のピア通信装置を動作させる方法であって、
認証および承認手順の一部として、スペクトラムアクセスキーソースに認証および認可情報を通信することと、
前記スペクトラムアクセスキーソースに認証および認可情報を通信することに応答して、前記スペクトラムアクセスキーソースから第１のスペクトラムアクセスキーを受け取ることと、
第２のピア通信装置から第１の信号を受け取ることと、
前記第１のスペクトラムアクセスキーに基づき、そして、前記第２のピア通信装置からの前記第１の信号に基づいて、第１の疑似ランダムビットシーケンスを発生することと、
第３のピア通信装置とエアリンク上で通信するために、前記発生された第１の疑似ランダムビットシーケンスを使用することと、
を備え、
前記第３のピア通信装置もまた、前記第１のスペクトラムアクセスキーを有し、そしてそれは前記第１の信号を受け取っており、
前記第１のスペクトラムアクセスキーは、暗号化された形式で受け取られ、
前記方法は、さらに、
前記第１の疑似ランダムビットシーケンスを発生するために、前記第１のスペクトラムアクセスキーを使用する前に、前記受け取られた第１のスペクトラムアクセスキーを解読

すること、
を備え、
前記第２のピア通信装置からの前記第１の信号はブロードキャストタイミング信号である方法。
【請求項２】
前記第２のピア通信装置はビーコン送信器である、請求項１に記載の方法。
【請求項３】
前記発生された第１の疑似ランダムビットシーケンスを使用することは、前記第１の疑似ランダムビットシーケンスに基づいて通信されるべきシンボル値を含む通信信号を発生すること、および前記第１の疑似ランダムビットシーケンスに基づいて受信された通信信号から通信されたシンボル値を再生すること、の少なくとも１つを含む、請求項１に記載の方法。
【請求項４】
前記発生された第１の疑似ランダムビットシーケンスを使用することは、通信信号を発生することの一部として前記発生された第１の疑似ランダムビットシーケンスに基づいてシンボルスクランブリング動作を実行することを含む、請求項３に記載の方法。
【請求項５】
前記発生された第１の疑似ランダムビットシーケンスを使用することは、受信された通信信号から通信されたシンボル値を再生することの一部として前記発生された第１の疑似ランダムビットシーケンスに基づいてシンボルデスクランブリング動作を実行することを含む、請求項３に記載の方法。
【請求項６】
第１のピア通信装置であって、
認証および認可手順の一部としてスペクトラムアクセスキーソースに認証および認可情報を通信し、
前記認証および認可手順の一部としてスペクトラムアクセスキーソースに認証および認可情報を通信することに応答して、前記スペクトラムアクセスキーソースから第１のスペクトラムアクセスキーを受信し、
第２のピア通信装置から第１の信号を受信し、
前記受信された第１のスペクトラムアクセスキーおよび前記第２のピア通信装置からの前記第１の信号に基づいて第１の疑似ランダムビットシーケンスを発生し、そして
エアリンク上で第３のピア通信装置と通信するために前記発生された第１の疑似ランダムビットシーケンスを使用する、
ように構成された少なくとも１つのプロセッサと；
前記少なくとも１つのプロセッサに結合されたメモリと；
を備え、
前記第３のピア通信装置もまた、前記第１のスペクトラムアクセスキーを有し、そしてそれは前記第１の信号を受け取っており、
前記第１のスペクトラムアクセスキーは、暗号化された形式で受け取られ、
前記少なくとも１つのプロセッサは、さらに、前記第１の疑似ランダムビットシーケンスを発生するために、前記第１のスペクトラムアクセスキーを使用する前に、前記受け取られた第１のスペクトラムアクセスキーを解読するように構成され、
前記第２のピア通信装置からの前記第１の信号はブロードキャストタイミング信号である第１のピア通信装置。
【請求項７】
前記第２のピア通信装置は１ビーコン送信器である、請求項６に記載の第１のピア通信装置。
【請求項８】
前記少なくとも１つのプロセッサはさらに、
前記第１の疑似ランダムビットシーケンスに基づいて通信されるべきシンボル値を含ん

でいる通信信号を発生し、そして、
前記第１の疑似ランダムビットシーケンスに基づいて受信された通信信号から通信されたシンボル値を再生する
ように構成されている、請求項６に記載の第１のピア通信装置。
【請求項９】
前記少なくとも１つのプロセッサはさらに、通信信号を発生することの一部として、前記発生された第１の疑似ランダムビットシーケンスに基づいてシンボルスクランブリング動作を実行するように構成されている、請求項８に記載の第１のピア通信装置。
【請求項１０】
前記少なくとも１つのプロセッサはさらに、受信された通信信号から通信されたシンボル値を再生することの一部として、前記発生された第１の疑似ランダムビットシーケンスに基づいてシンボルデスクランブリング動作を実行するように構成されている、請求項８に記載の第１のピア通信装置。
【請求項１１】
第１のピア通信装置であって、
認証および認可手順の一部として、スペクトラムアクセスキーソースに認証および認可情報を通信するための手段と、
前記認証および認可手順の一部として、スペクトラムアクセスキーソースに認証および認可情報を通信することに応答して、前記スペクトラムアクセスキーソースから第１のスペクトラムアクセスキーを受信するための手段と、
第２のピア通信装置から第１の信号を受信するための手段と、
前記受信された第１のスペクトラムアクセスキーに基づいて、そして前記第２のピア通信装置からの前記第１の信号に基づいて、第１の疑似ランダムビットシーケンスを発生するための手段と、
前記発生された第１の疑似ランダムビットシーケンスを使用して、第３のピア通信装置と、エアリンク上で通信するための手段と、
を備え、
前記第３のピア通信装置もまた、前記第１のスペクトラムアクセスキーを有し、そしてそれは前記第１の信号を受け取っており、
前記第１のスペクトラムアクセスキーは、暗号化された形式で受け取られ、
前記第１のピア通信装置は、さらに、
前記第１の疑似ランダムビットシーケンスを発生するために、前記第１のスペクトラムアクセスキーを使用する前に、前記受け取られた第１のスペクトラムアクセスキーを解読するための手段と、
を備え、
前記第２のピア通信装置からの前記第１の信号はブロードキャストタイミング信号である第１のピア通信装置。
【請求項１２】
前記第１の疑似ランダムビットシーケンスに基づいて通信されるべきシンボル値を含む通信信号を発生するための手段と、
前記第１の疑似ランダムビットシーケンスに基づいて受信された通信信号から通信されたシンボル値を再生するための手段と、
を更に備える、請求項１１に記載の第１のピア通信装置。
【請求項１３】
通信信号を発生することの一部として、前記発生された第１の疑似ランダムビットシーケンスに基づいてシンボルスクランブリング動作を実行するための手段、
を更に備える、請求項１２に記載の第１のピア通信装置。
【請求項１４】
第１のピア通信装置において使用するためのコンピュータ読み取り可能記録媒であって、

少なくとも１つのコンピュータに認証および認可手順の一部としてスペクトラムアクセスキーソースへの認証および認可情報を通信させるためのコードと、
前記少なくとも１つのコンピュータに認証および認可手順の一部としてスペクトラムアクセスキーソースへの認証および認可情報を通信することに応答して、前記スペクトラムアクセスキーソースからの第１のスペクトラムアクセスキーを受信させるためのコードと、
前記少なくとも１つのコンピュータに第２のピア通信装置から第１の信号を受信させるためのコードと、
前記少なくとも１つのコンピュータに前記受信された第１のスペクトラムアクセスキーに基づいて、そして、前記第２のピア通信装置からの前記第１の信号に基づいて、第１の疑似ランダムビットシーケンスを発生させるためのコードと、
前記第１のスペクトラムアクセスキーも有し、そして前記第２のピア通信装置から前記第１の信号を受信した第３のピア通信装置と、エアリンク上で通信するために、前記少なくとも１つのコンピュータに、前記発生された第１の疑似ランダムビットシーケンスを使用させるためのコードと、
を備え、
前記第３のピア通信装置もまた、前記第１のスペクトラムアクセスキーを有し、そしてそれは前記第１の信号を受け取っており、
前記第１のスペクトラムアクセスキーは、暗号化された形式で受け取られ、
前記コンピュータ読み取り可能記録媒体はさらに、
前記少なくとも１つのコンピュータに、前記第１の疑似ランダムビットシーケンスを発生するために、前記第１のスペクトラムアクセスキーを使用する前に、前記受け取られた第１のスペクトラムアクセスキーを解読させるためのコード、
を備え、
前記第２のピア通信装置からの前記第１の信号はブロードキャストタイミング信号であるコンピュータ読み取り可能記録媒体。

【発明の詳細な説明】
【分野】
【０００１】
いろいろな実施形態は無線通信に関し、そしてより詳しくは、スペクトラム（spectrum）の使用を認可する（authorizing）ためのおよび／またはスペクトラム、例えば、認可されたスペクトラム（licensed program）の認可されていない使用（unauthorized use）を防ぐあるいは止めさせるための方法および装置（method and apparatus）に関する。
【背景】
【０００２】
通信システム内のピアツーピア装置（peer to peer devices）はスペクトラム資源、例えば、スペクトラム所有者によって提供された、認可されたスペクトラム、を使用して通信する。例えば、タイムスロット対タイムスロット基準上で、送信のスケジューリングおよび通信資源の対応する割当を制御しているアクセスポイントのような集中コントローラがない時は、スペクトラム資源のアクセスおよび使用を制御することは困難である。例えば、個々の装置（individual devices）が通信資源を使用すべきか否かについて決定をすることができるピアツーピア通信システムでは、認可されない装置（unauthorized devices）によって通信資源の認可されていない使用を制御することは困難となりうる。ピアツーピア通信システム内で動作している装置は、サービスへのそのような認可を持たず、したがってこのスペクトラムを使用することを認可されない他の装置と同様に、ピアツーピア通信システム内のサービスについて申し込んだ加入したおよび正当な通信装置（both the subscribed and legitimate communications devices）の両方を含むことができる。ピアツーピア通信システム内で動作している正当な通信装置がスペクトラムのアクセスおよび使用を認められることが重要である一方で、サービス加入無しの認可されない通信装置によって認可されたスペクトラムの使用を防ぐか止めさせることができる機構について

の要求もある。

【０００３】

上記の検討に基づいて、スペクトラムの使用を認可する、および／またはスペクトラムの認可されていない使用を防ぐか止めさせるための方法および装置の要求があることは認識されねばならない。

【発明の概要】

【０００４】

いろいろな実施形態は無線通信に関し、そしてより詳しくは、スペクトラムの使用を認可するための、および／またはスペクトラム、例えば、認可されたスペクトラムの認可されていない使用を防ぐかあるいは止めさせるための方法および装置に関する。いくつかの実施形態では、スペクトラムアクセスキーの発行によって、スペクトラムを使用するために認可が与えられる。いくつかの実施形態では、認可された通信装置、例えば、認可されたスペクトラムを使用するように認可されたピアツーピア無線通信が安全な手法内のスペクトラムアクセスキーとともに提供される。この認可された通信装置はスペクトラムアクセスキーに基づいて疑似ランダムシーケンス（pseudo-random sequence）を発生し（generate）、そして通信するためにこの発生された疑似ランダムシーケンスを使用する。いくつかの実施形態では、疑似ランダムアクセスキーの使用はエアリンク上で認可された装置間で通信されているスクランブリング／デスクランブリング情報を含むことができる。したがって、いくつかのしかし必ずしも全部ではない実施形態では、認可されたスペクトラムの認可された装置間の通信は、スペクトラムアクセスキーから発生された疑似ランダムビットシーケンスに基づいた情報のスクランブリング／デスクランブリングを伴うことができる。

【０００５】

疑似ランダムビットシーケンスを発生している時に、ある程度の増加した安全性を提供するために、実施形態全体にわたって、疑似ランダムシーケンスは長期の時間に亘り定数を維持しており、いくつかの実施形態では、スペクトラムアクセスキーに加えて、第２の装置、例えば、ビーコンまたはＧＰＳ送信器、から受信されたエアインターフェイスタイミングおよび／または他の情報が、第２の入力として使用される。この手法では、疑似ランダムシーケンスは時間依存性（time varying）であってもよく、そして特定の領域内で通信するために探索している（seeking to communicate）いろいろな認可された装置によって受信されることができる第２の装置からの、受信された１つまたはそれ以上の信号に依存してもよい。

【０００６】

認可された装置は、スペクトラムアクセスキーおよび、オプションとしてもう１つの信号に基づいた通信を確保、例えば、スクランブル（scramble）または暗号化（encrypt）するので、認可された装置と通信し、従ってスペクトラムを使用するための、認可されない装置の能力（ability）は、認可されない装置が伝達された情報を確保し再生する、例えば、デスクランブル（descramble）または解読する（decrypt）ために使用されるスペクトラムアクセスキーを欠くであろう故に、スペクトラムを使用することは防止されるかあるいは止めさせられる。

【０００７】

いくつかの例示的な実施形態はピアツーピアシステムのコンテキストの中で記述されるがしかしこの中に記述された方法は種々様々な無線通信システム、例えば、その中では１つの装置がもう１つの装置によって送信された信号を検出できるシステムを用いた使用によく適している。したがって、この記述された方法はピアツーピアシステムに限定されないことは認識されるべきである。

【０００８】

１つの例示的な実施態様に従って、第１の通信装置を動作させる（operating a first communication device）例示的な方法は第１のスペクトラムアクセスキーを受信すること、第２の通信装置から第１の信号を受信すること、第１のスペクトラムアクセスキーに基

づいておよび第２の通信装置からの第１の信号に基づいて第１の疑似ランダムビットシーケンスを発生すること、およびエアリンク上で第３の通信装置と通信するために発生された第１の疑似ランダムビットシーケンスを使用することを含む。

【０００９】

必ずしも全部ではないいくつかの実施形態では、スペクトラムアクセスキーは暗号化形式で（in an encrypted form）第１の通信装置によって受信される。いくつかのそのような実施形態ではこの方法は前記疑似ランダムビットシーケンスを発生するためにスペクトラムアクセスキーを使用するより前に受信されたスペクトラムアクセスキーを解読することをさらに含む。

【００１０】

１つのしかし必ずしも全部ではない実施態様によれば、第１の通信装置は、第１のスペクトラムアクセスキーを受信し、第２の通信装置から第１の信号を受信し、この受信された第１のスペクトラムアクセスキーおよび第２の通信装置からのこの第１の信号に基づいて第１の疑似ランダムビットシーケンスを発生し、そして、エアリンク上で第３の通信装置と通信するためにこの発生された第１の疑似ランダムビットシーケンスを使用する、ように構成された少なくとも１つのプロセッサを含んでいる。第１の通信装置は、前記少なくとも１つのプロセッサに結合されたメモリを含むことができ、そしていくつかの実施形態では、それを含まなくともよい。

【００１１】

いろいろな実施形態が上記発明の概要（summary）で説明されているが、必ずしも全部でない実施形態では、同じ特徴を含み、そしていくつかの実施形態では、上述された特徴は必要ではないが、望まれ得るということ認識されるべきである。いろいろな実施形態の多数の付加的な特徴、実施形態および恩恵は次に続く詳細な説明において説明される。

【図面の簡単な説明】

【００１２】

【図１】１つの例示的な実施形態に従って、ピアツーピア通信ネットワーク、広域ネットワークおよびセキュリティ認証オーソリティ、例えば、サーバを含む１つの例示的なシステム示す図。

【図２】第１および第２の通信装置、およびいろいろなエレメントおよび装置間のシグナリング交換をより詳細に示している図１のシステム内のセキュリティ認証オーソリティを示すより詳細な図。

【図３】１つの例示的な実施形態に従って、通信装置、例えば、他のピア装置と通信するためにスペクトラムアクセスキーおよびタイミング情報を受信し、処理し、そして使用する通信装置を動作させるための１つの例示的な方法のステップを示すフローチャート。

【図４】図１のシステム内で使用されることができる１つの例示的な通信装置を示す図。

【図５】図４の例示的な通信装置内で使用されることができるモジュールのアセンブリを示す図。

【詳細な説明】

【００１３】

図１は、１つの例示的な実施形態に従って、ピアツーピア通信（Ｐ２Ｐ）ネットワーク１０１、Ｐ２Ｐスペクトラム所有者／管理者システム１２０、広域ネットワーク１３０、およびセキュリティ認証オーソリティサーバ１４０、例えば、認証および認可サーバを含んでいる１つの例示的なシステム１００を図示する。図示された実施形態ではセキュリティ認証オーソリティサーバ１４０はＰ２Ｐネットワーク１０１の部分である。Ｐ２Ｐネットワーク１０１の外部として示された一方で、所有者／管理者システム１２０はまたＰ２Ｐネットワーク１０１の部分であってもよい。例示的なピアツーピア通信ネットワーク１０１は複数の通信装置、例えば、第２の装置１１２のような他の通信装置のほかにあるピアツーピア通信装置を含む。複数のピアツーピア通信装置は、それぞれ、第１、第３、第Ｉ、第Ｋおよび第Ｎのピアツーピア通信装置１０２、１０４、１０６、１０８および１１０を含む。第２の装置１１２は、例えば、ピアツーピア通信装置によって検出されること

ができる信号を送信するピアツーピア装置または非ピアツーピア通信装置であってもよい。例えば、第２の装置はビーコン送信器、時間同期送信器またはＧＰＳ（グローバルポジショニングシステム）送信器であってもよい。第２の装置１１２はエアインターフェイスタイミング信号および／または矢印１１３によって示されたような他の同期信号のような信号をブロードキャストし、それはＰ２Ｐネットワーク１０１内の通信装置によって検出されることができる。続くセクション内で検討されるであろうように、ネットワーク１０１内の通信装置は、ネットワーク１０１内の他の認証装置との通信において使用されることができる疑似ランダムビットシーケンスを発生するために、第２の装置１１２からの信号１１３を使用することができる。下文で検討されるであろうように、第１および第３のピアツーピア通信装置１０２、１０４は信号を送信する、例えば、ブロードキャストすることができる、接続を確立し、そしてピアツーピア通信ネットワーク内で使用可能なスペクトラムを使用して通信することができる。図１に示されたもののようないくつかの実施形態では、ピアツーピア通信ネットワーク１０１は集中コントローラ、例えば、基地局が個々の無線端末による伝送のスケジューリングを制御するために使用される場合であるかもしれないような信号の伝送のための装置への資源の割当を制御するコントローラ、の使用無しに実施される。中央制御装置が使用されない間、認可された装置からおよび／またはこの装置に通信する信号を解釈することを困難にする一方で、セキュリティ認証オーソリティサーバ１４０は正当な装置およびそれらの関連ユーザに、互いに通信させる認証を発生して分配する。

【００１４】

いくつかの実施形態では、Ｐ２Ｐスペクトラム所有者／管理者システム１２０は使用可能なエアリンク通信資源の所有者および／またはプロバイダ、例えば、無線スペクトラム所有者に相当する。広域ネットワーク１３０は、例えば、通信ネットワーク１０１を含むローカル域を取り扱っている、インターネットサービスのローカルアクセスプロバイダであってもよい。セキュリティ認証オーソリティサーバ１４０は、例えば、Ｐ２Ｐ通信資源、例えば、スペクトラムをアクセスして使用するためにタイトルされる通信ネットワーク１０１内で動作している正当な通信装置を認証および認可するサーバであってもよい。そのような認証に続いて、セキュリティ認証オーソリティサーバ１４０は通信のための通信装置にスペクトラムのアクセスをさせることができる。いくつかの実施形態では、セキュリティ認証オーソリティサーバ１４０およびＰ２Ｐスペクトラム所有者／管理者システム１２０はシングルエンティティとして実施されることができる。

【００１５】

１つの例示的な実施形態に従って、Ｐ２Ｐスペクトラムを使用して互いに通信することを求める通信装置（communications devices）、例えば、ネットワーク１０１内の第１の通信装置１０２および第３の通信装置１０４（1st communications device 102 and the 3rd communications device 104）は、２装置間の通信セッションの確立より前に認証され、そして認可される必要があるかもしれない。通信資源へのアクセスがサービスプロバイダおよび／またはスペクトラム所有者と提携される正当な加入者装置に限定されることは望ましいので、これは重要でありうる。認証および認可はいくつかの方法でＰ２Ｐ通信およびセキュリティ認証オーソリティサーバ１４０をサポートするためにセキュリティ認証オーソリティサーバ１４０から認証、例えば、スペクトラムアクセスキーを求めている装置間で実行されることができる。例えば、Ｐ２Ｐ信号および／またはＷＡＮ１３０による通信は認証および認可目的のために使用されることができる。１つの例示的な実施形態に従って、加入者装置、例えば、第１の通信装置１０２間の、例えば、認証および認可手順のための、シグナリング交換は、ＷＡＮ１３０を通して運ばれる。したがって、加入者装置およびセキュリティ認証オーソリティサーバ１４０は、例えば、コネクタ１３２および１３４によって示されたような、もう１つのネットワーク、例えば、インターネットを介してシグナリングを交換することができる。ＷＡＮは他のＰ２Ｐ装置によって容易にモニタされない帯域外シグナリングパスとして働くのでこれはＰ２Ｐシグナリングを使用することに対して安全度を加えることができる。

【００１６】
既知のテクニック、例えば、チャレンジおよびレスポンス法を使用して実施されることができる、認証および認可手順に続いて、成功した認証および認可を想定している認証オーソリティは認証された加入者装置へのスペクトラムアクセスキーを認可するであろう。いくつかの実施形態では、スペクトラムアクセスキーは暗号化された形式で通信されることができ、そして加入者装置、例えば、第１の通信装置１０２は使用するより前にこのキーを解読する。いくつかの実施形態では加入者装置は他の装置と通信するために使用可能なスペクトラムをアクセスするためにスペクトラムアクセスキーを使用する前にさらなる処理を実行する必要があるかもしれない。例示的な実施形態に従って、１つまたはそれ以上の認証された加入者装置はスペクトラムアクセスキーを使用して互いに通信することができる。例えば、スペクトラムアクセスキーは通信をスクランブルするために使用されることができる。非正当な装置、例えば、妥当なスペクトラムアクセスキーを欠いている装置は正当なスペクトラムアクセスキーを使用し、それによってスペクトラムを利用して、正当な、例えば、認可されそして認証された装置との相互作用を拒んでいる装置を判断してそれと通信することはできないであろう。
【００１７】
図２はいろいろなエレメントおよび装置間のシグナリング交換をさらに詳しく示している図１のシステム内で特徴づけられたセキュリティ認証オーソリティサーバ１４０と同様に第１および第２の通信装置１０２、１１２の図２００である。いくつかの実施形態では、ネットワーク１０１内のピアツーピア通信装置のいずれか（例えば、１０４、１０６、１０８および１１０）は第１の通信装置１０２として実施されることができ、従って図２内に示され、そして下文で検討されたと同一のまたは類似のエレメントおよび／またはモジュールを含んでもよいことは認識されるべきである。第１の装置１０２のエレメント／モジュールによって実行された機能は他の通信装置１０４、１０６、１０８および１１０のいずれかの中の類似のまたは同一のエレメント／モジュールによって実行されることができる。図２に示されたように、ピアツーピア通信装置１０２は認証クライアントモジュール２１８および点線ボックス内に囲まれて示されたような複数のタンパーレジスタントモジュールを含む。タンパーレジスタントモジュールは解読モジュール２２０、はめこまれた認証モジュール２２２、疑似ランダムシーケンス発生器２２４、コントローラ２２６、回復モジュール２２８および送信処理モジュール２３０を含む。タンパーレジスタントモジュールはいかなる処理および／またはタンパリングも検出されること無しにこれらのモジュールになされないようにすることができ、それによって追加レベルのセキュリティを供給し、そして時にはそのように設計されることは認識されるべきである。タンパーレジスタントモジュールはエポキシまたは他の材料でコートされてもよい。従って、タンパーレジスタントモジュールをタンパする試みは可能であり、そして一般に通信装置１０２を無効にし、そして無機能にするであろう。
【００１８】
セキュリティ認証オーソリティサーバ１４０は図１の例の中で初期に検討されたいろいろな機能を実行し、そして認証オーソリティモジュール２０４、セキュリティモジュール２０６および認可エージェントモジュール２０８を含む。第２の通信装置１１２、例えば、ビーコン送信器は、タイミング情報モジュール２１４および送信器／受信器モジュール２１６を含む。いくつかの実施形態では、第２の通信装置１１２はまた疑似ランダム（ＰＲ）ビットシケンス発生器２１２も含む。
【００１９】
１例示的な実施形態に従って、ピアツーピア通信装置１０２は、ネットワーク１０１内の他のピア装置と通信するためにスペクトラムのアクセスを得るより前に、認証手順の部分としてセキュリティ認証オーソリティサーバ１４０とシグナリングを交換する。このシグナリング交換は矢印２０１および２０３を使用して示される。認可クライアントモジュール２１８は、スペクトラムアクセスキーの発行または分布に先立つことができる認証および／または認可手順の間中セキュリティ認証オーソリティサーバ１４０内の認可エージ

ェントモジュール２０８との相互作用について責任がある相互作用モジュールである。いくつかの実施形態では、認可クライアントモジュール２１８はセキュリティ認証オーソリティサーバ１４０との通信の認証ステージの間中チャレンジレスポンス手順内に参加する。例えば、いくつかの実施形態では、セキュリティ認証オーソリティサーバ１４０内の認可エージェントモジュール２０８は第１の通信装置１０２のアイデンティティを確かめるために使用されているチャレンジへの答えとともに装置１０２を要求する。チャレンジに応じて、認可クライアントモジュール２１８は応答を発生し、そしてオプションとして、第１の装置１０２に対応する識別情報を含んでいる応答をセキュリティ認証オーソリティサーバ１４０に送る。認証オーソリティモジュール２０４はアイデンティティを確かめ、そして受信された応答が第１の装置１０２からの期待された応答とマッチすることを仮定して第１の装置１０２を認証するであろう。いくつかの実施形態では、認証オーソリティモジュール２０４は受信された応答情報を第１の装置１０２およびセキュリティ認証オーソリティサーバ１４０に知られた共有の秘密から発生された期待された応答と比較することによって第１の装置１０２を認証することができる。共有の秘密および対応する識別情報のデータベースはセキュリティ認証オーソリティサーバ１４０の部分であってもまたはなくてもよい。そのうえ、他の実施形態では、認証手順は共有の秘密よりはむしろ公開／私有のキーペアを含む。このために、例えば、いくつかのしかし全部ではない実施形態では、セキュリティ認証オーソリティサーバ１４０内の認可エージェントモジュール２０８はそれのはめ込まれた認証２２２を表示し、そしてこの分野で既知の公開／私有キープロトコルおよびアルゴリズムを使用している前記認証内の公開キーと関連する私有キーの所有を改善する。

【００２０】

認証手順に続いて、認証オーソリティモジュール２０４は、例えば、セキュア形式で、セキュアスペクトラムアクセスキーを認証および認可装置に供給する。いくつかの実施形態では、スペクトラムアクセスキーが発生され、そしてその後セキュリティモジュール２０６によって行われた暗号化動作に従う。いくつかの実施形態では、セキュリティモジュール２０６は私有キーに対応する公開キーを使用しているスペクトラムアクセスキー、例えば、第１の通信装置１０２には既知だが他にはそうでない秘密、を暗号化する。他の実施形態では、スペクトラムアクセスキーはセキュリティ認証オーソリティサーバ１４０および第１の通信装置１０２の両者に既知の共有の秘密に基づいて暗号化される。暗号は装置１０２に特有であるので、安全にされた、例えば、暗号化されたスペクトラムアクセスキーは正当なレベルの安全性を維持している一方で、公共ネットワーク上にあることができる。暗号化されたスペクトラムアクセスキーは第１の通信装置１０２に通信される。スペクトラムアクセスキーが１つまたはそれ以上の申し込まれた装置について同一物か類似物であってもよいことに注意されたい。スペクトラムアクセスキーを安全にするために暗号化を使用することよりも、メモリチップあるいはケースセキュリティが伝送機構によって供給されるセキュア通信チャネルのような、セキュア通信法の使用によってスペクトラムアクセスキーは安全にされることができる。いくつかの実施形態では、暗号化されたスペクトラムアクセスキーは、矢印２１１によって示されたように、第２の装置１１２に通信されることができる。いくつかのそのような実施形態では、第２の装置１１２は疑似ランダムビットシーケンスを発生するためにモジュール２１４によって発生されたタイミング情報と組み合わせて受信されたスペクトラムアクセスキーを使用することができる。疑似ランダムビットシーケンスは疑似ランダムビットシーケンス発生器２１２によって発生される。

【００２１】

初期に検討されたように、第２の装置１１２は、送信器／受信器モジュール２１６を使用しているエアインターフェイスタイミング信号および／または他の同期信号のような信号２１７を、装置１０２を含んでいる通信ネットワーク１０１内の１つまたはそれ以上の装置にブロードキャストする。信号２１７は回復モジュール２２８によって処理され、そして再生される。例えば、受信されたタイミング情報である回復モジュール２２８からの

出力は、疑似ランダムシーケンス発生器２２４への入力として供給される。復号モジュール２２０は受信された暗号化スペクトラムアクセスキーを処理して復号する責任がある。いくつかの実施形態では、復号モジュール２２０は、例えば、私有キーまたは共有秘密でありうるはめ込まれた認証２２２を使用している受信されたスペクトラムアクセスキーを復号する。受信されたスペクトラムアクセスキーを復号する後で、復号モジュール２２０は疑似ランダムシーケンス発生器２２４への第２の入力としてスペクトラムアクセスキーを供給する。疑似ランダムシーケンス発生器２２４は、回復モジュール２２８からの入力として受信したタイミング情報および、例えば、復号モジュール２２０からのスペクトラムアクセスキーを使用して、疑似ランダムビットシーケンスを発生する。そのような疑似ランダムビットシーケンスが、認証されたそして正当な加入者装置、例えば、他の装置ではない正当なスペクトラムアクセスキーを有している装置によって発生されるであろうことは認識されるべきである。スペクトラムアクセスキーが暗号化よりも伝送機構によって安全にされる場合には、暗号化および対応する復号手順は省かれることができる。

【００２２】

疑似ランダムビットシーケンスの発生に続いて、コントローラ２２６は発生された疑似ランダムビットシーケンスを回復モジュール２２８および／または送信処理モジュール２３０に選択的に供給する。いくつかの実施形態では、送信処理モジュールは発生された疑似ランダムビットシーケンスに基づいてシンボル値（symbol values）を含む通信信号を発生する。疑似ランダムビットシーケンスを使用して発生された通信信号はその後、もう１つの装置、例えば、どの通信装置１０２と通信すべきかを探索する（seeks to communicate）第３の通信装置１０４への送信のため、矢印２３１を使用して示されたような送信器に供給される。

【００２３】

いくつかの実施形態において通信装置１０２は、例えば、この通信信号を送っている第３の装置１０４によって発生された疑似ランダムビットシーケンス、例えば、それを使用してスクランブルされた、通信信号に基づいて第３の装置１０４によって発生された通信信号を受信する。そのような事象では、例えば、矢印２２９を使用して示されたような、受信された通信信号は回復モジュール２２８によって処理される。いくつかの実施形態では、回復モジュールは疑似ランダムビットシーケンスに基づいて受信された通信信号から通信されたシンボル値を再生するように構成される。もう１度、初期に検討されたように、不認可装置はスクランブリングの結果として受信された通信信号から意味のある情報を再生することができないであろう、したがって申込み無しの不認可装置による認可されたスペクトラムの使用を止めさせる一方で、認可されたそしてスペクトラムアクセスキーを供給された正当な通信装置は通信された信号の意味をなさなくし、そして通信されたシンボル値を再生することができるべきである。スクランブリングがスペクトラムアクセスキーおよび位置上使用可能な時間変化信号の両者に基礎を置くことによって、こわされている（例えば、スペクトラムキーへのアクセス無しの第３者によって再生された）スクランブリングの可能性は、スクランブリングが時間とともに変化するであろうので、１つのキーのみが使用されたかどうかと似ているとみなされた時に、減らされる。

【００２４】

例示的な実施形態がいろいろな特徴を記述するために使用された一方で、いくつかの実施形態内で使用された方法は図３および４内に示されたフローチャートの視野内で考慮された時にいっそう明確になるであろう。

【００２５】

図３は、例示的な実施形態に従って、第１の通信装置、例えば、ネットワーク１０１内において、もう１つのピア装置と通信するために、例えば、スペクトラムアクセスキーおよびタイミング情報を受信し、処理しそして使用している装置を動作させることの例示的な方法のステップを示すフローチャート３００である。第１の通信装置は、例えば、図１および２内に示された第１のピアツーピア通信装置１０２であることができる。

【００２６】

動作は第１の通信装置１０２がパワーオンされて初期化されるステップ３０２で始まる。動作はスタートステップ３０２から、並列に実行されてもよいが、しかしその必要がない、ステップ３０４および３０６に進む。いくつかの他の実施形態では、ステップ３０４および３０６は交互に行われる。

【００２７】

ステップ３０４で第１の通信装置１０２は第１の信号、例えば、信号１１３を、第２の装置、例えば、図２の第２の装置１１２から受信する。初期に検討されたように受信された信号１１３は、例えば、エアインターフェイスタイミング信号および／または他の同期信号であってもよい。いくつかの実施形態では、第２の（２ｎｄ）通信装置１１２はビーコン送信器である。いくつかの実施形態では、第２の装置から受信された第１の信号はブロードキャストタイミング信号である。動作はステップ３０４からステップ３１１に進む。ステップ３０６に戻って、ステップ３０６では第１の通信装置１０２は、認証および認可手順の部分として、認証および認可情報をスペクトラムアクセスキーソース、例えば、図２のセキュリティ認証オーソリティサーバ１４０に通信する。セキュリティ認証オーソリティサーバ１４０はピアツーピアネットワーク１０１の外部に存在してもよく、そして第１の通信装置１０２およびセキュリティ認証オーソリティサーバ１４０の間のシグナリング交換はＰ２Ｐネットワークの外部、例えば、ＷＡＮローカルアクセスプロバイダのようなもう１つのネットワーク上にあってもよいことは認識されるべきである。これは第１の通信装置１０２が認証手順の間中セキュリティ認証オーソリティサーバ１４０とシグナリングを交換する図２の例において詳細に検討された。認証および認可手順に続いて、動作は第１の通信装置１０２が第１のスペクトラムアクセスキーを受信するステップ３０８に進む。いくつかの実施形態では、第１のスペクトラムアクセスキーは暗号化形式で受信される。いくつかの実施形態では、通信より前に、他の装置ではないがこの通信装置１０２に既知の私有キーに対応する公開キーを使用して、第１のスペクトラムアクセスキーはスペクトラムキーソース、例えば、セキュリティ認証オーソリティサーバ１４０によって暗号化される。他の実施形態では、セキュリティ認証オーソリティサーバ１４０および第１の装置１０２に既知の秘密がスペクトラムアクセスキーを暗号化するために使用される。

【００２８】

動作は通信装置１０２がスペクトラムアクセスキーを再生するために受信された暗号化された第１のスペクトラムアクセスキー上で解読動作を行うステップ３０８からステップ３１０に進む。再び、例えば、はめ込まれた認証２２２、例えば、私有キーまたは共有の秘密を使用している復号モジュール２２０によって実行されることができる第１の通信装置１０２内の受信された第１のスペクトラムアクセスキーを解読する手順は、初期に検討された。動作はステップ３１０からステップ３１１に進む。ステップ３１１では、第１のスペクトラムアクセスキーおよび第２の装置１１２からの第１の信号が第１の通信装置１０２に伝えられた時刻までのある次の時刻に起こることは、受信された第１のスペクトラムアクセスキーに基づいて、そして第２の装置１１２からの受信された第１のタイミング信号に基づいて第１の通信装置１０２は第１の疑似ランダムビットシーケンスを発生する。これはスペクトラムアクセスキーおよび疑似ランダムビットシーケンスを発生することにおいて使用される入力として第１の信号の両方を受け入れる疑似ランダム番号発生器を使用することによってなされることができる。発生された第１の疑似ランダムビットシーケンスは、例えば、一連のバイナリ値であってもよい。動作はステップ３１１からステップ３１２に進む。

【００２９】

ステップ３１２では、第１の通信装置１０２はエアリンク上で第３の通信装置、例えば、第３の装置１０４と通信するために発生された第１の疑似ランダムビットシーケンスを使用する。第３の通信装置１０４は、例えば、第１のスペクトラムアクセスキーも有し、そして第２の通信装置１１２から、第１の信号、例えば、信号１１３も受信したもう１つのＰ２Ｐ通信装置である。例えば、第１の通信装置１０２が認可されたスペクトラムを使

用している第３の装置１０４と通信することを探索するシナリオを考えられたい。われわれは両通信装置が認可されたそして正当な加入者であり、そして第２の装置１１２からのタイミング信号と同様にセキュリティ認証オーソリティサーバ１４０からスペクトラムアクセスキーを受信したと仮定する。これらの環境下では、通信装置１０２、１０１は認可されたスペクトラムを使用して通信することができるかもしれない。いくつかの、しかし必ずしも全部ではない実施形態では、ステップ３１２はサブステップ３１４および／またはサブステップ３１８を含む。いくつかの実施形態では、第１の通信装置１０２がトラフィックデータを、例えば、シンボル値の形式で、第３の装置１０４に通信することを探索する例として、サブステップ３１４が行われることができる。エアリンク上で第３の通信装置と通信するために発生された疑似ランダムビットシーケンスを使用している部分として行われる、サブステップ３１４では、第１の通信装置１０２は第３の通信装置１０４に伝えられるべき、第１の疑似ランダムビットシーケンスに基づいたシンボル値（例えば、トラフィックデータ）を含む通信信号を発生する。例えば、通信されるべきシンボル値を含んでいる通信信号はある種のフォーマットに入れられることができ、および／または第１のスペクトラムアクセスキーを有し、そして第１のタイミング信号１１３を受信した、認可された受信装置、例えば、第３の装置１０４は、意味のある手法で通信された信号を解釈することができるであろうが、しかし他の装置は通信されたデータを正確に解釈することができないであろうように、（第１の通信装置１０２によって発生された）第１の疑似ランダムビットシーケンスを使用してコード化される（coded）ことができる。疑似ランダムシーケンス発生器への２つの入力、例えば、第２の通信装置１１２から受信されたタイミング信号またはスペクトラムアクセスキーのいずれかを欠く装置は、通信信号からトラフィックデータを再生することはできないであろう。いくつかの実施形態では、サブステップ３１４を実行することはまた、第１の通信装置１０２が、通信信号を発生する部分として、発生された疑似ランダムシーケンスに基づいてシンボルスクランブリング動作（symbol scrambling operation）を行うオプションのサブステップ３１６を実行することも含むことができる。そのような事例では発生された疑似ランダムシーケンスはシンボルがシンボルスクランブリング手順の部分として再整理される順番を制御することができる。いくつかの実施形態では、シンボルスクランブリングを実行することは通信信号の送信より前にシンボルを再整理することを含む。オプションのサブステップ３１４は、オプションのサブステップ３１８が通信動作の部分としてデータが受信される場合を処理する間に、疑似ランダムシーケンスが伝送をサポートするために使用される場合を処理する。

【００３０】

いくつかの実施形態では、第３の通信装置１０４が第１の通信装置１０２に、例えば、シンボル値の形式で、トラフィックデータを通信することを探索する例として、サブステップ３１８が実行されることができる。ステップ３１８では第１の通信装置１０２は発生された第１の疑似ランダムビットシーケンスに基づいて通信されたシンボル値を再生するために、前記第３の通信装置１０４から受信されたシンボル値を含む通信信号を処理する。通信装置１０２は第１のスペクトラムアクセスキーも有し、そして第２の装置１１２からタイミング信号を受信した正当な装置であるので、第１の装置１０２は、例えば、発生された疑似ランダムビットシーケンスを使用することによって通信されたシンボル値を再生して、正確に解釈することができる。いくつかの実施形態では、シンボルスクランブリング動作が第３の装置１０４から第１の通信装置１０２に通信された通信信号を発生している間に行われたかもしれない例として、サブステップ３１８もオプションのサブステップ３２０を実行することを含んでもよい。サブステップ３２０では、第１の通信装置１０２は、受信された通信信号から通信されたシンボル値を再生する部分として、発生された疑似ランダムシーケンスに基づいてシンボルデスクランブリング動作（symbol de-scrambling operation）を実行する。いくつかの実施形態では、シンボルデスクランブリング動作を実行することはそれらをそれらの原のスクランブル解除順に戻すために受信された通信信号から再生されたシンボルの再整理を含む。動作は（サブステップ３１４、３１６、３１８および３２０を含むことができる）ステップ３１２からステップ３２２に進む。

【００３１】
ステップ３２２では、第１の通信装置１０２は第２の装置１１２、例えば、ビーコン送信器から、例えば、第２の装置１１２からの第１の信号の受信に続いて起こる、第２の信号を、一度に、受信する。従って、いくつかの実施形態では第１の通信装置１０２は第２の装置１１２からの信号を周期的にまたは非周期的に受信することができ、そしてこの手順はあるレートで繰り返してもよい。第２の装置１１２は第２の信号をネットワーク１０１内の通信装置にブロードキャストすることができ、したがって第２の信号はまた通信装置１０４を含んでいる他の通信装置によって受信されることもできる。このように、いろいろな装置は時間と共に変化する第２の装置１１２によって送信された信号として疑似ランダムシーケンス発生器への入力の１つの更新されたバージョンを受信することができる。動作は、第１の通信装置１０２が受信された第１のスペクトラムアクセスキーに基づいて、そして第２の通信装置１１２からの第２の信号に基づいて第２の疑似ランダムビットシーケンスを発生する、ステップ３２２からステップ３２４に進む。第２の疑似ランダムビットシーケンスを発生する手順は初期に検討された疑似ランダムビットシーケンス発生手順と類似であるが、しかしながら今回、第２の疑似ランダムビットシーケンスを発生するために使用された入力が第２の信号、例えば、第２の装置１１２から受信されたおよび第１のスペクトラムアクセスキーから受信された、現タイミング信号であることは認識されるべきである。したがって入力、例えば、第２の信号は第２の（２ｎｄ）装置１１２からの第１の信号とは異なるので、出力は異なるであろう。

【００３２】
動作はステップ３２４からステップ３２６に進み、ここにおいて第１の通信装置１０２はエアリンク上で第３の通信装置１０４と通信するために発生された第２の疑似ランダムビットシーケンスを使用する。第３の通信装置１０４はまた第２の（2^{nd}）装置１１２から第２の信号も受信する。ステップ３２６内の動作は、ステップ３２６では第２の疑似ランダムビットシーケンスが第３の（３ｒｄ）通信装置１０４と通信するために使用されることを除いては、ステップ３１２に関して検討されたことと類似している。動作はステップ３２６からステップ３２８に進む。ステップ３２８では第１の通信装置１０２は第２のスペクトラムアクセスキーを受信する。一度に受信される、例えば、第１のスペクトラムアクセスキーの受信に続いて起こる、第２のスペクトラムアクセスキーは同じソース、例えば、セキュリティ認証オーソリティサーバ１４０から受信されることができる。いくつかの実施形態では、例えば、通信装置１０２および１０４のような、認可された通信装置は、スペクトラムアクセスキーを、例えば、毎月一度またはある他の時間間隔で、受信することができる。新スペクトラムアクセスキーが異なる、例えば、第２の通信装置１１２からの異なる信号間の間隔よりも、長い間隔で、しばしば受信されることは認識されるべきである。動作はステップ３２８からステップ３３０に進む。

【００３３】
初期に述べられたように、第１の通信装置１０２は第２の装置１１２からの信号を周期的にまたは非周期的に受信することができる。従っていくつかの実施形態では、動作の間中通信装置１０２は第２の通信装置から第３の信号を受信する。ステップ３３０では、第１の通信装置１０２は受信された第２のスペクトラムアクセスキーに基づいておよび第２の通信装置、例えば、2^{nd}装置１１２から受信された第３の信号に基づいて第３の疑似ランダムビットシーケンスを発生する。動作はステップ３３０からステップ３３２に進み、ここにおいて第１の通信装置１０２は、エアリンク上で、第３の通信装置１０４と通信するために発生された第３の疑似ランダムビットシーケンスを使用するように動作される。この動作はステップ３３４によって示されたようにこの手法で継続することができる。認識されるべきであるように、スクランブリングのために使用された疑似ランダムシーケンスの受取および更新は通信セッションの間中何度も起こりうる。

【００３４】
図４は１つの例示的な実施形態に従う例示的な通信装置４００の図である。通信装置４００は多分、そして少なくとも１つの実施形態では、ピアツーピア通信をサポートし、そ

して図３のフローチャート３００に従う方法を実施している移動体無線端末である。通信装置４００は図１の第１の通信装置１０２として使用されることができる。通信装置４００はそれの上でいろいろなエレメント（４０２，４０４）がデータおよび情報を交換することができるバス４０９によって共に結合されたプロセッサ４０２およびメモリ４０４を含む。通信装置４００は、示されたようなプロセッサ４０２に結合されることができる入力モジュール４０６および出力モジュール４０８をさらに含む。しかしながら、いくつかの実施形態では入力モジュールおよび出力モジュール４０６，４０８はプロセッサ４０２内に位置している。入力モジュール４０６は入力信号を受信することができる。入力モジュール４０６は無線受信器および／または入力を受信するための有線または光入力インターフェイスを含むことができ、そしていくつかの実施形態ではそれを行う。出力モジュール４０８は、無線送信器および／または送信出力のための有線または光出力インターフェイスを含むことができ、そしていくつかの実施形態ではそれを行う。いくつかの実施形態では、プロセッサ４０２は、下記をするように構成される：第１のスペクトラムアクセスキーを受信する、第２の通信装置から第１の信号を受信する、受信された第１のスペクトラムアクセスキーに基づいておよび第２の通信装置からの第１の信号に基づいて第１の疑似ランダムビットシーケンスを発生する、および前記第１のスペクトラムアクセスキーも有し、そして第２の通信装置から前記第１の信号を受信した第３の（３ｒｄ）通信装置とエアリンク上で通信するために発生された第１の疑似ランダムビットシーケンスを使用する。

【００３５】

いくつかの実施形態では、第１のスペクトラムアクセスキーは暗号化形式で受信される。プロセッサ４０２は前記第１の疑似ランダムビットシーケンスを発生するために第１のスペクトラムアクセスキーを使用するより前に前記受信された第１のスペクトラムアクセスキーを解読するようにさらに構成されることができ、そしていくつかの実施形態ではそのように構成される。いくつかの実施形態ではプロセッサ４０２は、第１のスペクトラムアクセスキーを受信するより前に、認証および認可手順の部分としてスペクトラムアクセスキーソースに認証および認可情報を通信するようにさらに構成される。少なくともいくつかの実施形態では、第２の通信装置からの第１の信号はブロードキャストタイミング信号である。少なくとも１つの実施形態では、第２の通信装置はビーコン送信器である。

【００３６】

いくつかの実施形態では、プロセッサ４０２は下記をするようにさらに構成される：前記第１の疑似ランダムビットシーケンスに基づいて通信されるべきシンボル値を含んでいる通信信号を発生する、そして受信された通信信号から通信されたシンボル値を再生するために通信されたシンボル値回復動作を実行する、前記回復動作は第１の疑似ランダムビットシーケンスに基づいている。いくつかの実施形態では、プロセッサ４０２は通信信号を発生する部分として前記発生された第１の疑似ランダムビットシーケンスに基づいてシンボルスクランブリング動作を実行するようにさらに構成される。いくつかの実施形態では、シンボルスクランブリングは前記通信信号を発生するためにシンボルの再整理を含む。いくつかの実施形態では、プロセッサ４０２は、受信された通信信号から通信されたシンボル値を再生する部分として前記発生された第１の疑似ランダムビットシーケンスに基づいてシンボルデスクランブリング動作を実行するようにさらに構成される。いくつかのそのような実施形態ではシンボルデスクランブリングは受信された通信信号から再生されたシンボルの再整理を含む。

【００３７】

いくつかの実施形態では、プロセッサ４０２は下記をするようにさらに構成される：第２の通信装置からの前記信号の受信に続いて起こる第２の通信装置からの第２の信号を一度に受信する、受信された第１のスペクトラムアクセスキーに基づいておよび第２の通信装置からの第２の信号に基づいて第２の疑似ランダムビットシーケンスを発生する、および第２の通信装置から前記第２の信号も受信する前記第３の通信装置と前記エアリンク上で通信するために発生された第２の疑似ランダムビットシーケンスを使用する。

【００３８】
いくつかの実施形態では、プロセッサ４０２は下記をするようにさらに構成される：第２のスペクトラムアクセスキーを受信する、受信された第２のスペクトラムアクセスキーに基づいておよび第２の通信装置からの第３の信号に基づいて第３の疑似ランダムビットシーケンスを発生する、および第３の通信装置と前記エアリンク上で通信するために発生された第３の疑似ランダムビットシーケンスを使用する。
【００３９】
図５は図４に図示された通信装置内で使用されることができ、そしていくつかの実施形態ではそのように使用されるモジュールのアセンブリ５００である。アセンブリ５００内のモジュールは、例えば、個々の回路として、図４のプロセッサ４０２内のハードウェアで実施されることができる。あるいは、モジュールはソフトウェアで実施されることができ、そして図４内に示された通信装置４００のメモリ４０４内に蓄積されることができる。単一のプロセッサ、例えば、コンピュータとして図４の実施形態内に示された一方で、プロセッサ４０２が１つまたはそれ以上のプロセッサ、例えば、複数コンピュータとして実施されてもよいことは認識されるべきである。
【００４０】
ソフトウェアで実施された時にこのモジュールは、プロセッサ４０２によって実行した時に、このモジュールに対応する機能を実施するようにプロセッサを構成する、コード（code）を含む。モジュールのアセンブリ５００がメモリ４０４内に蓄積される実施形態では、メモリ４０４は、少なくとも１つのコンピュータ、例えば、プロセッサ４０２に、対応するモジュールの機能を実施させるためのコード、例えば、各モジュールについての個々のコードを具備しているコンピュータ可読媒体を備えているコンピュータプログラム製品である。
【００４１】
完全にハードウェアベースのまたは完全にソフトウェアベースのモジュールが使用されることができる。しかしながら、ソフトウェアおよびハードウェア（例えば、実施された回路）モジュールが機能を実施するために使用されうることは認識されるべきである。認識されるべきであるように、図５内に図示されたモジュールは、図３の方法のフローチャート内に図示された対応するステップの機能を実行するために、通信装置４００またはプロセッサ４０２のようなその中のエレメントを制御するおよび／または構成する。
【００４２】
図５に図示されたように、モジュールのアセンブリ５００は第２の通信装置から第１の信号を受信するためのモジュール５０２、認証および認可手順の部分として、スペクトラムアクセスキーソース、例えば、認証および認可サーバに認証および認可情報を通信するためのモジュール５０４、第１のスペクトラムアクセスキーを受信するためのモジュール５０６、前記受信された第１のスペクトラムアクセスキーを解読するためのモジュール５０８、受信された第１のスペクトラムアクセスキーに基づいておよび第２の通信装置からの第１の信号に基づいて第１の疑似ランダムビットシーケンスを発生するためのモジュール５１０、前記第１のスペクトラムアクセスキーも有し、そして第２の通信装置から前記第１の信号を受信した第３の通信装置とエアリンク上で通信するために発生された第１の疑似ランダムビットシーケンスを使用するためのモジュール５１２を含む。いくつかの実施形態では、モジュール５１２は、もう１つの通信装置に通信されるべき、第１の疑似ランダムビットシーケンスに基づいた、シンボル値を含んでいる通信信号を発生するためのモジュール５１４、発生された第１の疑似ランダムビットシーケンスに基づいてシンボルスクランブリング動作を実行するためのモジュール５１６、第１の疑似ランダムビットシーケンスに基づいて受信された通信信号から通信されたシンボル値を再生するためのモジュール５１８、および発生された第１の疑似ランダムビットシーケンスに基づいてシンボルデスクランブリング動作を実行するためのモジュール５２０を含む。
【００４３】
モジュールのアセンブリ５００はさらに第２の通信装置からの前記第１の信号の受信に

続いて起こる第２の通信装置からの第２の信号を一度に受信するためのモジュール５２２、受信された第１のスペクトラムアクセスキーに基づいておよび第２の通信装置からの第２の信号に基づいて第２の疑似ランダムビットシーケンスを発生するためのモジュール５２４、第２の通信装置から前記第２の信号も受信する第３の通信装置と前記エアリンク上で通信するために発生された第２の疑似ランダムビットシーケンスを使用するためのモジュール５２６、第２のスペクトラムアクセスキーを受信するためのモジュール５２８、受信された第２のスペクトラムアクセスキーに基づいておよび第２の通信装置からの第３の信号に基づいて第３の疑似ランダムビットシーケンスを発生するためのモジュール５３０、および第３の通信装置とエアリンク上で通信するために発生された第３の疑似ランダムビットシーケンスを使用するためのモジュール５３２を含む。

【００４４】

いろいろな実施形態の技術はソフトウェア、ハードウェアおよび／またはソフトウェアとハードウェアとの組合せを使用して実施されることができる。いろいろな実施形態は装置、例えば、移動体端末、基地局、通信システムのようなモバイルノード（mobile nodes）に向けられる。いろいろな実施形態はまた方法、例えば、モバイルノード、基地局、通信装置および／または通信システム、例えば、ホストを制御するおよび／または動作させる方法にも向けられる。いろいろな実施形態はまた機械、例えば、コンピュータ、可読媒体、例えば、ＲＯＭ，ＲＡＭ，ＣＤ，ハードディスク、などにも向けられ、それは方法の１つまたはそれ以上のステップを実施するように機械を制御するための機械可読命令を含む。

【００４５】

いろいろな実施形態ではこの中に記述されたノードは１つまたはそれ以上の方法に対応するステップ、例えば、信号処理、決定ステップ、メッセージ発生、メッセージシグナリング、スイッチング、受信および／または送信ステップを実行するために１つまたはそれ以上のモジュールを使用して実施される。このように、いくつかの実施形態ではいろいろな特徴はモジュールを使用して実施される。そのようなモジュールはソフトウェア、ハードウェアまたはソフトウェアとハードウェアとの組合せを使用して実施されることができる。上記の方法または方法のステップの多くは、例えば、１つまたはそれ以上のノードにおいて、上記された方法の全部または一部を実施するために、機械、例えば、追加のハードウェア付きのまたは無しの汎用コンピュータを制御するために、メモリ装置、例えば、ＲＡＭ、フロッピディスク、等のような機械可読媒体内に含まれた、ソフトウェアのような、機械実行可能な命令を使用して実施されることができる。よって、特に、いろいろな実施形態は機械、例えば、プロセッサおよび関連するハードウェアに上記の方法の１つまたはそれ以上のステップを実行させるための機械実行可能命令を含んでいる機械可読媒体に向けられる。いくつかの実施形態は、現出願内に記述された１つまたはそれ以上の方法のステップの１つ、複数または全部を実施するように構成されたプロセッサを含んでいる装置、例えば、通信装置に向けられる。

【００４６】

いくつかの実施形態では、１つまたはそれ以上の装置、例えば、無線端末のような通信装置のプロセッサまたは複数プロセッサ、例えば、ＣＰＵｓはこの通信装置によって実行されているとして記述された方法のステップを実行するように構成される。よって、いくつかのしかし全部ではない実施形態は、その中にプロセッサが含まれる装置によって実行されたいろいろな記述された方法のステップの各々に対応するモジュールを含むプロセッサを有する装置、例えば、通信装置に向けられる。いくつかのしかし全部ではない実施形態では装置、例えば、通信装置は、その中にプロセッサが含まれる装置によって実行されたいろいろな記述された方法のステップの各々に対応するモジュールを含む。このモジュールはソフトウェアおよび／またはハードウェアを使用して実施されることができる。

【００４７】

開示された手順内のステップの特定の順番または階層が例示的なアプローチの１例であることは理解される。設計選択に基づいて、この手順内のステップの特定の順番または階

層が現開示の範囲内に留まっている間に再調整されうることは理解される。添付している方法はサンプルオーダー内のいろいろなステップの現在の要素をクレームし、そして示された特定の順番または階層に限定されることを意味しない。

【００４８】

いくつかの実施形態は、コンピュータ可読媒体、例えば、コンピュータ、または複数のコンピュータに、いろいろな機能、ステップ、行動および／または動作、例えば、上記された１つまたはそれ以上のステップを実施させるためのコードを備えている、物理的媒体を備えているコンピュータプログラム製品に向けられる。この実施形態による、コンピュータプログラム製品は、実行されるべき各ステップについて異なるコードを含むことができ、そして時々これをする。このように、コンピュータプログラム製品は方法、例えば、通信装置またはノードを制御することに関する方法の各個々のステップについてのコードを含むことができ、そして時々それをする。コードはマシン、例えば、コンピュータの形式内にあり、ＲＡＭ（ランダムアクセスメモリ）、ＲＯＭ（読出し専用メモリ）または他タイプの蓄積装置のようなコンピュータ可読媒体上に蓄積された実行可能な命令であってもよい。コンピュータプログラム製品に向けられているほかに、いくつかの実施形態は上記された１つまたはそれ以上のいろいろな機能、ステップ、行動および／または動作の１つまたはそれ以上を実施するように構成されたプロセッサに向けられる。よって、いくつかの実施形態はこの中に記述された方法のステップのいくつかまたは全部を実施するように構成されたプロセッサ、例えば、ＣＰＵに向けられる。プロセッサは現出願内に記述された通信装置または他の装置内での使用のためにあることができる。

【００４９】

Ｐ２Ｐスペクトラムは直交周波数分割多重化（ＯＦＤＭ）信号を使用することができる。しかしながら、いろいろな実施形態の方法および装置の少なくともいくつかはＣＤＭＡシステムのような多くの非ＯＦＤＭおよび／または非セルラシステムを含んでいる広範囲の通信システムに適用可能であることは認識されるべきである。

【００５０】

上記されたいろいろな実施形態の方法および装置に関する多数の更なる変形は、上記説明を考慮して、当業者には明らかであろう。そのような変形は範囲内であると考慮されるべきである。この方法および装置は、ＣＤＭＡ、直交周波数分割多重化（ＯＦＤＭ）、および／またはアクセスノードとモバイルノードとの間の無線通信リンクを供給するために使用されることができるいろいろな他のタイプの通信技術とともに使用されることができ、そしていろいろな装置内で使用される。いろいろな実施形態では、ピアツーピア通信装置は、ノートブックコンピュータ、パーソナルデータアシスタント（ＰＤＡｓ）、またはこの方法を実施するための、受信器／送信器回路および論理および／またはルーチンを含んでいる他の携帯型装置として実施される（implemented）。

以下に、本願出願の当初の特許請求の範囲に記載された発明を付記する。

［Ｃ１］

第１の通信装置を動作させる方法であって、

第１のスペクトラムアクセスキーを受け取ることと、

第２の通信装置から第１の信号を受け取ることと、

前記第１のスペクトラムアクセスキーに基づき、そして、前記第２の通信装置からの前記第１の信号に基づいて、第１の疑似ランダムビットシーケンスを発生することと、

第３の通信装置とエアーリンク上で通信するために、前記発生された第１の疑似ランダムビットシーケンスを使用することと、

を備える方法。

［Ｃ２］

前記第３の通信装置もまた、前記第１のスペクトラムアクセスキーを有し、そしてそれは前記第１の信号を受け取っており、

前記第１のスペクトラムアクセスキーは、暗号化された形式で受け取られ、

前記方法は、さらに、

前記第１の偽似ランダムビットシーケンスを発生するために、前記第１のスペクトラムアクセスキーを使用する前に、前記受け取られた第１のスペクトラムアクセスキーを解読すること、
を備える、Ｃ１に記載の方法。
［Ｃ３］
前記第１のスペクトラムアクセスキーを受け取る前に、認証および承認手順の一部として、スペクトラムアクセスキーソースに認証および認可情報を通信すること、
をさらに備える、Ｃ２に記載の方法。
［Ｃ４］
前記第２の通信装置からの前記第１の信号はブロードキャストタイミング信号である、Ｃ２に記載の方法。
［Ｃ５］
前記第２の通信装置はビーコン送信器である、Ｃ４に記載の方法。
［Ｃ６］
前記発生された第１の疑似ランダムビットシーケンスを使用することは、前記第１の疑似ランダムビットシーケンスに基づいて通信されるべきシンボル値を含む通信信号を発生すること、および前記第１の疑似ランダムビットシーケンスに基づいて受信された通信信号から通信されたシンボル値を再生すること、の少なくとも１つを含む、Ｃ２に記載の方法。
［Ｃ７］
前記発生された第１の疑似ランダムビットシーケンスを使用することは、通信信号を発生することの一部として前記発生された第１の疑似ランダムビットシーケンスに基づいてシンボルスクランブリング動作を実行することを含む、Ｃ６に記載の方法。
［Ｃ８］
前記発生された第１の疑似ランダムビットシーケンスを使用することは、受信された通信信号から通信されたシンボル値を再生することの一部として前記発生された第１の疑似ランダムビットシーケンスに基づいてシンボルデスクランブリング動作を実行することを含む、Ｃ６に記載の方法。
［Ｃ９］
第１の通信装置であって、
第１のスペクトラムアクセスキーを受信し、
第２の通信装置から第１の信号を受信し、
前記受信された第１のスペクトラムアクセスキーおよび前記第２の通信装置からの前記第１の信号に基づいて第１の疑似ランダムビットシーケンスを発生し、そして
エアリンク上で第３の通信装置と通信するために前記発生された第１の疑似ランダムビットシーケンスを使用する、
ように構成された少なくとも１つのプロセッサと；
前記少なくとも１つのプロセッサに結合されたメモリと；
を備える第１の通信装置。
［Ｃ１０］
前記第３の通信装置はまた前記第１のスペクトラムアクセスキーを有しており、そしてそれは、前記第１の信号を受信しており、
前記第１のスペクトラムアクセスキーは暗号化形式で受信され、そして、
前記少なくとも１つのプロセッサは更に、前記第１の疑似ランダムビットシーケンスを発生するために前記第１のスペクトラムアクセスキーを使用する前に、前記受信された第１のスペクトラムアクセスキーを解読するように構成されている、
Ｃ９に記載の第１の通信装置。
［Ｃ１１］
前記少なくとも１つのプロセッサは更に、
前記第１のスペクトラムアクセスキーを受信する前に、認証および認可手順の一部とし

てスペクトラムアクセスキーソースに認証および認可情報を通信する、
ように構成されている、Ｃ１０に記載の第１の通信装置：
［Ｃ１２］
前記第２の通信装置からの前記第１の信号は、ブロードキャストタイミング信号である、Ｃ１０に記載の第１の通信装置。
［Ｃ１３］
前記第２の通信装置は１ビーコン送信器である、Ｃ１２に記載の第１の通信装置。
［Ｃ１４］
前記少なくとも１つのプロセッサはさらに、
前記第１の疑似ランダムビットシーケンスに基づいて通信されるべきシンボル値を含んでいる通信信号を発生し、そして、
前記第１の疑似ランダムビットシーケンスに基づいて受信された通信信号から通信されたシンボル値を再生する。
ように構成されている、Ｃ１０に記載の第１の通信装置。
［Ｃ１５］
前記少なくとも１つのプロセッサはさらに、通信信号を発生することの一部として、前記発生された第１の疑似ランダムビットシーケンスに基づいてシンボルスクランブリング動作を実行するように構成されている、Ｃ１４に記載の第１の通信装置。
［Ｃ１６］
前記少なくとも１つのプロセッサはさらに、受信された通信信号から通信されたシンボル値を再生することの一部として、前記発生された第１の疑似ランダムビットシーケンスに基づいてシンボルデスクランブリング動作を実行するように構成されている、Ｃ１４に記載の第１の通信装置。
［Ｃ１７］
第１の通信装置であって、
スペクトラムアクセスキーソースから第１のスペクトラムアクセスキーを受信するための手段と、
第２の通信装置から第１の信号を受信するための手段と、
前記受信された第１のスペクトラムアクセスキーに基づいて、そして前記第２の通信装置からの前記第１の信号に基づいて、第１の疑似ランダムビットシーケンスを発生するための手段と、
前記発生された第１の疑似ランダムビットシーケンスを使用して、第３の通信装置と、エアリンク上で通信するための手段と、
を備える第１の通信装置。
［Ｃ１８］
前記第３の通信装置はまた前記第１のスペクトラムアクセスキーを有し、そしてそれは、前記第１の信号を受信しており、
前記第１のスペクトラムアクセスキーは暗号化形式で受信され、
前記通信装置はさらに、
前記第１の疑似ランダムビットシーケンスを発生するために前記第１のスペクトラムアクセスキーを使用する前に前記受信された第１のスペクトラムアクセスキーを解読するための手段、を備える、
Ｃ１７に記載の第１の通信装置。
［Ｃ１９］
前記第１のスペクトラムアクセスキーを受信する前に、認証および認可手順の一部として、スペクトラムアクセスキーソースに認証および認可情報を通信するための手段、
を更に備える、Ｃ１８に記載の第１の通信装置。
［Ｃ２０］
前記第１の疑似ランダムビットシーケンスに基づいて通信されるべきシンボル値を含む通信信号を発生するための手段と、

前記第１の疑似ランダムビットシーケンスに基づいて受信された通信信号から通信されたシンボル値を再生するための手段と、
を更に備える、Ｃ１８に記載の第１の通信装置。
［Ｃ２１］
通信信号を発生することの一部として、前記発生された第１の疑似ランダムビットシーケンスに基づいてシンボルスクランブリング動作を実行するための手段、
を更に備える、Ｃ２０に記載の第１の通信装置。
［Ｃ２２］
第１の通信装置において使用するためのコンピュータプログラム製品であって、
少なくとも１つのコンピュータに第１のスペクトラムアクセスキーを受信させるためのコードと、
前記少なくとも１つのコンピュータに第２の通信装置から第１の信号を受信させるためのコードと、
前記受信された第１のスペクトラムアクセスキーに基づいて、そして、前記第２の通信装置からの前記第１の信号に基づいて、第１の疑似ランダムビットシーケンスを発生させるためのコードと、
前記第１のスペクトラムアクセスキーも有し、そして前記第２の通信装置から前記第１の信号を受信した別の装置と、エアリンク上で通信するために、前記少なくとも１つのコンピュータに、前記発生された第１の疑似ランダムビットシーケンスを使用させるためのコードと、
を備えるコンピュータ可読媒体、
を備えるコンピュータプログラム製品。
［Ｃ２３］
前記第３の通信装置はまた前記第１のスペクトラムアクセスキーを有し、そしてそれは前記第１の信号を受信しており、
前記第１のスペクトラムアクセスキーは暗号化形式で受信され、
前記コンピュータ可読媒体はさらに、
前記少なくとも１つのコンピュータに、前記第１の疑似ランダムビットシーケンスを発生するために、前記第１のスペクトラムアクセスキーを使用する前に前記受信された第１のスペクトラムアクセスキーを解読させるためのコード、
を備えている、
Ｃ２２に記載のコンピュータプログラム製品。
［Ｃ２４］
前記コンピュータ可読媒体はさらに、
前記少なくとも１つのコンピュータに、前記第１のスペクトラムアクセスキーを受信する前に、認証および認可手順の一部としてスペクトラムアクセスキーソースへの認証および認可情報を通信させるためのコード、
を備える、
Ｃ２３に記載のコンピュータプログラム製品。

【図１】

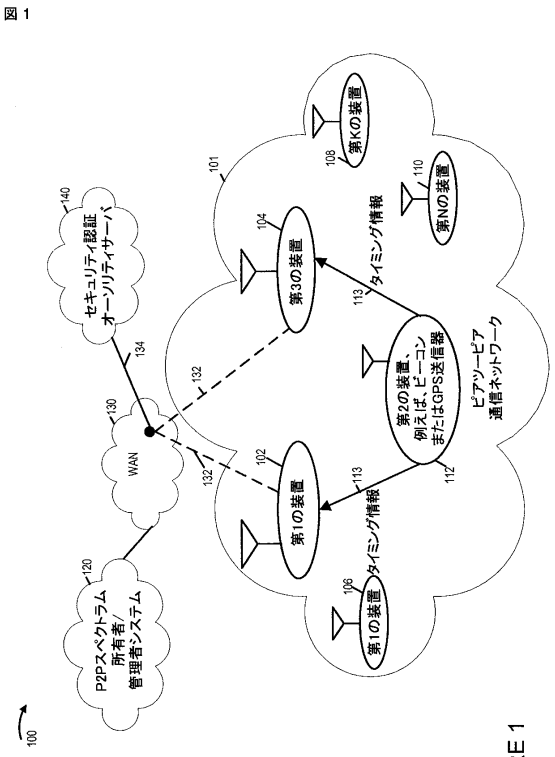

FIGURE 1

【図２】

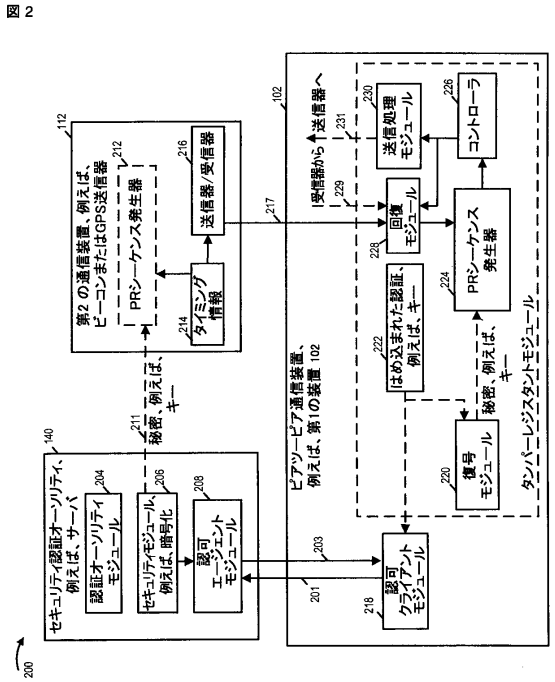

FIGURE 2

【図３】

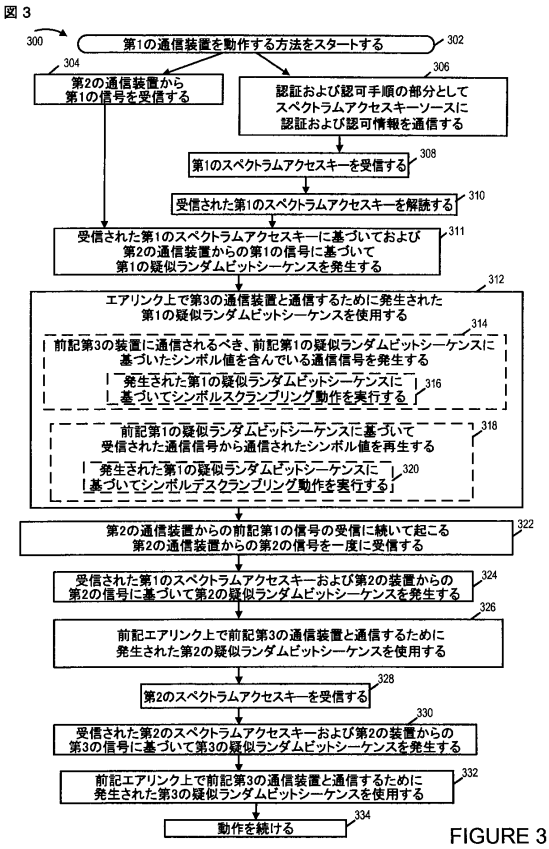

FIGURE 3

【図４】

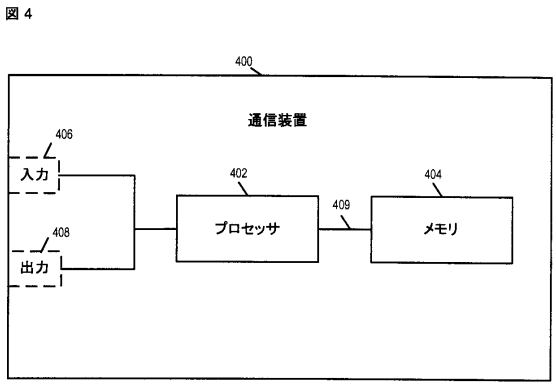

FIGURE 4

【図５】

図５

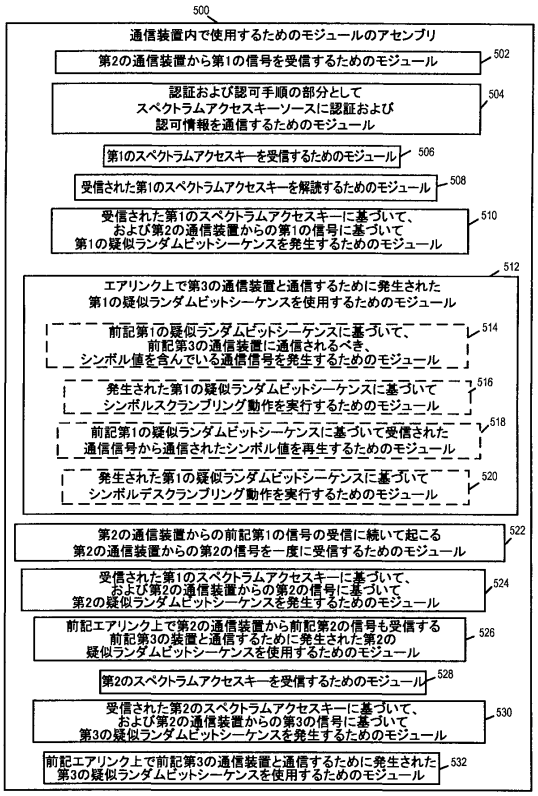

FIGURE 5

フロントページの続き

(74)代理人 100153051
弁理士 河野 直樹
(74)代理人 100140176
弁理士 砂川 克
(74)代理人 100158805
弁理士 井関 守三
(74)代理人 100179062
弁理士 井上 正
(74)代理人 100124394
弁理士 佐藤 立志
(74)代理人 100112807
弁理士 岡田 貴志
(74)代理人 100111073
弁理士 堀内 美保子
(72)発明者 パーク、ビンセント・ディー.
アメリカ合衆国、カリフォルニア州 ９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ ５７７５
(72)発明者 リチャードソン、トマス・ジェイ.
アメリカ合衆国、カリフォルニア州 ９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ ５７７５
(72)発明者 バンデルビーン・マイケラ
アメリカ合衆国、カリフォルニア州 ９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ ５７７５
(72)発明者 リ、ジュンイ
アメリカ合衆国、カリフォルニア州 ９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ ５７７５
(72)発明者 コーソン、マシュー・スコット
アメリカ合衆国、カリフォルニア州 ９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ ５７７５

審査官 東 昌秋

(56)参考文献 特開２００８－２０６１２４（ＪＰ，Ａ）
特開２００１－１４８７２９（ＪＰ，Ａ）
特開２００８－２２７８４６（ＪＰ，Ａ）
特開２００３－３３３０３１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｗ ４／００－９９／００
Ｈ０４Ｂ ７／２４－ ７／２６
Ｈ０４Ｌ ９／００