

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第5389937号
(P5389937)

(45) 発行日 平成26年1月15日 (2014. 1. 15)

(24) 登録日 平成25年10月18日 (2013. 10. 18)

(51) Int. Cl.	F I
HO 4W 16/14 (2009. 01)	HO 4W 16/14
HO 4W 40/02 (2009. 01)	HO 4W 40/02 1 1 0
HO 4W 84/18 (2009. 01)	HO 4W 84/18

請求項の数 13 (全 11 頁)

(21) 出願番号	特願2011-536281 (P2011-536281)	(73) 特許権者	598036300
(86) (22) 出願日	平成21年3月23日 (2009. 3. 23)		テレフオンアクチーボラゲット エル エム エリクソン (パブル)
(65) 公表番号	特表2012-509008 (P2012-509008A)		スウェーデン国 ストックホルム エスー 1 6 4 8 3
(43) 公表日	平成24年4月12日 (2012. 4. 12)		
(86) 国際出願番号	PCT/SE2009/050303	(74) 代理人	100076428
(87) 国際公開番号	W02010/056179		弁理士 大塚 康德
(87) 国際公開日	平成22年5月20日 (2010. 5. 20)	(74) 代理人	100112508
審査請求日	平成24年2月23日 (2012. 2. 23)		弁理士 高柳 司郎
(31) 優先権主張番号	61/114, 579	(74) 代理人	100115071
(32) 優先日	平成20年11月14日 (2008. 11. 14)		弁理士 大塚 康弘
(33) 優先権主張国	米国 (US)	(74) 代理人	100116894
			弁理士 木村 秀二
		(74) 代理人	100130409
			弁理士 下山 治

最終頁に続く

(54) 【発明の名称】 無線リソースへのアクセスを制御する方法および装置

(57) 【特許請求の範囲】

【請求項 1】

無線システムで用いる無線ノード（400）であって、前記無線ノードは、前記無線システムの他の無線ノードと情報を交換できるようになされており、一次ユーザによる無線リソースの使用を検出する手段（403）と、前記検出した無線リソースへのアクセスをブロックするためのメッセージを前記無線システムにおいて前記無線ノードの通信範囲内の少なくとも1つの他の無線ノードに送信する手段（401、411）とを備え、前記無線ノードは、特定の時間の間、アクセスをブロックするように構成されており、

前記送信する手段は、初期値を設定したカウンタを含む前記メッセージを前記無線システムにおいて前記無線ノードの通信範囲内の少なくとも1つの他の無線ノードに送信し、

前記メッセージを受信した受信無線ノードは、前記メッセージ中のカウンタの値を更新し、該更新後のカウンタの値が規定値に達した場合には該メッセージの送信を停止し、該更新後のカウンタの値が規定値に達していない場合には、該メッセージを前記無線システムにおいて前記受信無線ノードの通信範囲内の少なくとも1つの他の無線ノードに送信する

ことを特徴とする無線ノード。

【請求項 2】

前記無線ノードは、アクセスをブロックするためのメッセージを複数のホップにわたって転送するように構成されることを特徴とする請求項 1 に記載の無線ノード。

【請求項 3】

10

20

前記送信する手段は、ホップ／距離依存フィールドを更新することを特徴とする請求項2に記載の無線ノード。

【請求項4】

無線ノードが特定の無線リソースの使用を検出したときはいつでも、ホップ／距離依存フィールドを初期値にリセットする手段をさらに備えることを特徴とする請求項2または3に記載の無線ノード。

【請求項5】

前記初期値は動的に設定されることを特徴とする請求項4に記載の無線ノード。

【請求項6】

前記無線ノードは、アクセスをブロックするための前記メッセージの時間フィールドを設定するように構成されることを特徴とする請求項1乃至5の何れか1項に記載の無線ノード。

【請求項7】

前記無線ノードは、どの無線リソースにアクセスすべきかを決定するとき、アクセスをブロックするためのメッセージをチェックするように構成されることを特徴とする請求項1乃至6のいずれか1項に記載の無線ノード。

【請求項8】

無線システムで用いる無線ノードにおける無線リソースアクセスを制御する方法であって、前記無線ノードは前記無線システムの他の無線ノードと情報を交換し、一次ユーザによる無線リソースの使用を検出する工程(501)と、前記検出した無線リソースへのアクセスをブロックするためのメッセージを前記無線システムにおいて前記無線ノードの通信範囲内の少なくとも1つの他の無線ノードに送信する工程(503)とを備え、前記アクセスのブロックは特定の時間の間行われるように設定されており、

前記送信する工程では、初期値を設定したカウンタを含む前記メッセージを前記無線システムにおいて前記無線ノードの通信範囲内の少なくとも1つの他の無線ノードに送信し

、
前記メッセージを受信した受信無線ノードは、前記メッセージ中のカウンタの値を更新し、該更新後のカウンタの値が規定値に達した場合には該メッセージの送信を停止し、該更新後のカウンタの値が規定値に達していない場合には、該メッセージを前記無線システムにおいて前記受信無線ノードの通信範囲内の少なくとも1つの他の無線ノードに送信する

ことを特徴とする方法。

【請求項9】

アクセスをブロックするための前記メッセージは複数のホップにわたって転送されることを特徴とする請求項8に記載の方法。

【請求項10】

前記送信する工程では、ホップ／距離依存フィールドを更新することを特徴とする請求項9に記載の方法。

【請求項11】

特定の無線リソースの使用を検出したときはいつでも、ホップ／距離依存フィールドを初期値にリセットする工程をさらに備えることを特徴とする請求項9または10に記載の方法。

【請求項12】

前記時間はアクセスをブロックするための前記メッセージの中に設定されることを特徴とする請求項8乃至11の何れか1項に記載の方法。

【請求項13】

どの無線リソースにアクセスすべきかを決定するとき、アクセスをブロックするためのメッセージをチェックする工程をさらに備えることを特徴とする請求項8乃至12のいずれか1項に記載の方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、無線リソースへのアクセスを制御する方法およびデバイスに関する。本発明は特に、無線システムにおいてオポチュニスティック (opportunistic) スペクトルアクセスを可能にする無線リソース制御に関する。

【背景技術】

【0002】

最近の研究が示すところでは、無線スペクトルの使用はかなり効率の悪いことが多い。この主要因の1つは、現在のスペクトルの認可制度にある。すなわち、無線スペクトルのある部分が、無線通信システムの1つのオペレータなどの1つの団体に認可され、この団体は、無線スペクトルのこの部分の使用に対して占有権を与えられる。例えば、有用なスペクトルの大部分が認可されているけれども、いくつかの測定値 (例えば、非特許文献1を参照) が、このスペクトルの一部があまり利用されていないことを示している。それ故、利用可能な無線スペクトルの使用の最適化すなわち最大化を目標として、無線スペクトルをより柔軟に使用することが研究集約的な課題になっている。

【0003】

上に示す課題に取り組むために、FCC (連邦通信委員会、Federal Communications Commission) は、2005年にいわゆるスペクトルの二次利用の可能性を開くイニシアチブを取った。すなわち、一方の団体である一次利用者が例えば認可などを受けて所有する無線リソースは、一次利用者の業務 (一次利用) に含まれない目的 (二次利用) のために、他者 (二次ユーザ) によっても使用されてもよい。その結果として、二次ユーザは、認可を持たずに、且つ一次利用者と明示的な契約を結ぶことなしに、一次利用者が所有する無線リソースを使用しうる。二次ユーザとして無線リソースにアクセスするための要件は、二次利用が引き起こす有害な干渉に、一次利用者を晒してはならないというものである。それ故、一次利用者が実際上影響を受けないことを保証できる場合だけ、二次ユーザは、一次利用者が所有する無線リソースで送信することを許容される。

【先行技術文献】

【非特許文献】

【0004】

【非特許文献1】T. Erpek, K. Steadman, D. Jones 共著、「スペクトル利用測定値：アイルランド国ダブリンで2007年4月16～18日収集 (Spectrum Occupancy Measurements: Dublin, Ireland, Collected On April 16-18, 2007)」、Shared Spectrum Company Report、2007年

【非特許文献2】Ford Fulkerson 著、「ネットワーク内のフロー (Flows in Networks)」

【発明の概要】

【発明が解決しようとする課題】

【0005】

一次ユーザに悪影響を与えることなしに二次ユーザがいつ送信できるかを決定するために、ある種のメカニズムが提供されなければならない。そうすることによって、一次ユーザの通信品質が (実質上) 影響を受けないとき、二次ユーザは許容されるべきであり、そのメカニズムは、二次ユーザが一次ユーザのスペクトルにアクセスするのを可能にすべきである。スペクトルの (瞬間的な) 一次利用を評価する1つのアプローチは、一次送信が存在するかどうかの測定を目標とした感知を行う、すなわち (無線受信機の) センサを使用することである。感知の結果が一次利用のないことを示す場合、測定されたスペクトルは二次アクセスのために利用されてもよい。このタイプのメカニズムは、感知ベースのオポチュニスティックスペクトルアクセスと呼ばれることが多い。全体的目的は、簡潔に言うと、容量および個々のユーザのスループットを増加することである。既存のアプローチは、<http://www.academypublisher.com/jcm/vo102/no02/jcm02027182.pdf> および http://www.eecs.berkeley.edu/~sahai/Papers/ICC06_final.pdf で検討および評価されている。

【0006】

簡潔には、協調センシングは、複数のセンサの情報を収集することによって、検出確率の増加および誤認警報確率の減少をもたらせるという発想を基礎にしていると言ってもよい。

【0007】

また、水面下の環境にある現場の適用協調センシングに関する分散アルゴリズムが、http://perso.eleves.bretagne.ens-cachan.fr/~huguenin/UUST07_DistributedSampling.pdf に提示されている。発想は1つには、現場でのサンプリングを改善するために、分散的なやり方で共同して、集めた情報を処理しノード位置を制御するノード群を形成することである。

10

【0008】

しかし、上で参照した方法のどれも、望ましくない（干渉を引き起こす）二次スペクトルアクセスからより大きなエリアを保護できない。従って、無線システムにおいてオポチュニスティックスペクトルアクセスを可能にするように改良した無線リソース制御方法が必要である。

【0009】

本発明の1つの目的は、無線システムのオポチュニスティックスペクトルアクセスを制御する既存の方法に関する問題のいくつかを克服または少なくとも軽減することである。

【課題を解決するための手段】

20

【0010】

この目的は、添付の特許請求の範囲に記載されている本発明によって達成される。要するに、無線ノードが連絡を取り合っている無線システムにおいては、無線ノードは、近隣のノードと情報を交換できるようになされている。さらに一実施形態では、直接通信の範囲外にある離れたノードとは、複数のホップにわたってデータを転送することによって通信しうる。ノードが、ユーザ特に一次ユーザを検出すると、そのノードの近くの他のノードにスペクトルアクセス・ブロッキングメッセージを送信し、それによって他者の使用が検出された地理的エリアにおける無線リソースのブロックが可能になる。この意味することは、そのエリアにおいて無線リソースが、一次ユーザ以外のユーザによるアクセスからブロックされるということである。ブロッキングメッセージは、任意の適切なやり方で配信されてもよく、これから行うアプリケーションに適合されてもよい。

30

【0011】

一実施形態によれば、ホップ／距離依存フィールドがホップごとに更新され、ノードはこのフィールドに対応してメッセージを転送するように構成される。例えば、減少可能なフィールドがホップごとに減少され、カウンタフィールドがマイナスでない場合スペクトルアクセスを控え、カウンタフィールドがプラスである限りメッセージを転送し続ける。

【0012】

一実施形態によれば、ホップ／距離依存フィールドは、ノードが無線チャネルなどの特定の無線リソースに関して一次ユーザを検出したときはいつでも、初期値にリセットされる。初期値は、非固定値にも設定されてもよい。このような非固定の初期値は、例えば受信信号強度に従って設定されてもよい。

40

【0013】

一実施形態によれば、スペクトルアクセスは、特定の時間の間ブロックされる。この時間は、ブロッキングメッセージの中に設定されてもよいし、またシステムがデフォルトのブロッキング時間設定を有してもよい。

【0014】

一実施形態によれば、一次ユーザがいない無線システムで本発明を使用するとき、本明細書に記載のスペクトルブロッキング方法は、無線システムのユーザがどの無線リソースにアクセスすべきかを決定するために使用しうる情報メッセージとして使用されてもよい。

50

【0015】

これより本発明について、非限定的例を用い添付の図面を参照して、より詳細に説明する。

【図面の簡単な説明】

【0016】

【図1】スペクトルアクセス・ブロッキングメッセージを示す図である。

【図2】第1のシナリオを示す図である。

【図3】第2のシナリオを示す図である。

【図4】ノードの機能ブロックを示す図である。

【図5】無線ノードが実行する手順のいくつかのステップを示すフロー図である。

10

【発明を実施するための形態】

【0017】

本発明によれば、ノードが、単独でまたは他のノードと一緒に、例えば一次ユーザまたは別のユーザなどのユーザが特定の無線リソース、特に無線システムの1つのチャンネル（または複数のチャンネルさえ）を占有するなどの、無線リソースの使用を検出する。この検出に応じて、スペクトルアクセス・ブロッキングメッセージ（SABメッセージ、Spectrum Access Blocking message）と呼んでも良いメッセージが生成され、無線システム内で配信される。SABメッセージは、一実施形態によれば、対象としているチャンネルを示すフィールド、および／または例えば減算可能(down-countable)フィールドなどの距離フィールド、および／または対応するブロッキングの有効制限時間を含んでもよい。

20

【0018】

SABメッセージを受信するノードは、一実施形態によれば、所定の分散的距離制限規則に基づき距離フィールドを更新するように構成されてもよい、あるいは、それぞれのノードもまた対応するリソースで一次ユーザまたは別のユーザを検出した（且つそのノードが関連のSABメッセージをまだ送信していなかった）場合、カウンタをその元の値および制限時間に、または例えば受信信号強度などに依存してもよい非固定値にリセットし、そのメッセージをフィールドが所定の値に到達するまで近隣のノードにさらに転送するように構成されてもよい。カウンタ値のリセットのおかげで、個別のノードによるスペクトルアクセスから保護される必要のあるエリアを合同したエリアが保護される。

【0019】

30

SABメッセージを受信するノードは、ブロックが有効であることを距離フィールドが示す場合、対応するリソースへのアクセスを止めるように構成されてもよい。追加の前提条件は、ブロックの制限時間が満了していないことでもよい。

【0020】

一次利用を検出したノードの周りのエリアをブロックするスペクトルアクセス・ブロッキングメッセージは、種々のフォーマットを有してもよい。いくつかの例が図1に示されている。これを基にすると、ブロッキングメッセージは、スペクトルブロッキング情報を備えることを示すフィールド101を備えてもよい。メッセージは、送信元ノードのIDを示すフィールド103を備えてもよい。メッセージは、メッセージが移動した距離を示す更新可能なフィールド105を備えてもよい。メッセージは、メッセージのIDを示すフィールド107を備えてもよい。メッセージは、ブロックが有効である時間を示すフィールド109を備えてもよい。メッセージは、どの無線リソース／チャンネルがブロックされるかを示すフィールド111を備えてもよい。

40

【0021】

メッセージの不要な転送を制限するために、情報の各部分（または多くのより小さな情報部分を有するメッセージ）には、メッセージがそのノードによって既に転送されたかどうか、まだ有効か否か（タイムスタンプによればブロッキングメッセージは古すぎるかもしれない）、または同じリソースをブロックするメッセージがその受信ノードによって最近送信されたかどうかを、受信ノードが判定するのを可能にする連続番号または時間タグが付けられてもよい。一実施形態によれば、メッセージが有効であると判定された場合だ

50

け、メッセージは転送される。

【0022】

この検出は主に狭い地域だけに関連するので、好ましくは、この情報のフラッディング (flooding) は、何らかの局所的な制約を使用して行われるべきである。ホップ数、ノード間距離の累積推定値等のような種々のタイプの情報が、更新可能な距離フィールドに使用されてもよい。

【0023】

ホップ：一例として、メッセージの中のホップごとに減算されるホップカウンタをNに設定することによって、要求メッセージを最大Nホップ送信してもよいと指定してもよい。ホップカウンタがゼロに達すると、それ以上の転送は行われない。ホップは長さが異なってもよいので、これは簡単ではあるが、かなり粗いアプローチである。

10

【0024】

累積距離推定値：推定距離について距離フィールドの距離の値に基づくこともできよう。この距離の値は、受信電力レベル、送信電力の知識、およびメッセージが送信された距離を推定するための伝播条件の想定から推論してもよい。この場合、フラッディングされたメッセージの許容される距離を表すカウンタが、更新されてもよい、例えばそれ以降の転送が許容されないゼロに達するかそれを超えるまで減算されてもよい。

【0025】

SABメッセージの多くのノードへの配信は、いくつかのやり方で達成することができ、例えば以下のものがある。

20

ーブロードキャストリング：メッセージは、所定のブロードキャストツリーパスに沿って進む。ツリーは、先立つ感知段階に確立されてもよい。

ーフラッディング：新しいメッセージを聞いたら、どのユーザもそれを転送しようとする。

【0026】

ブロードキャストツリーを使用するブロードキャストリングは、一般的にフラッディングより信頼性を高くすることができるが、ツリーを作ることでオーバーヘッドを必要とする。信頼性の面は様々な要素を備えている。例えば、ブロードキャストツリーは、メッセージの衝突確率（すなわち、使用するデータレートを利用可能にするには、瞬間的な信号対雑音比 (SNR) が低すぎる）が低くなるように、またはツリーに定められたリンクが正しく受信されたデータに対して肯定応答を使用し、転送に失敗した場合に再送信が何回か行われるように、定められてもよい。

30

【0027】

ブロードキャストツリーは、様々なやり方で決定されてもよい。ツリーは、ホップ、推定ホップ距離、推定パスロス、推定逆比等のようなある測定基準を入力として使用するベルマンフォードアルゴリズムに基づいて計算されてもよい。これについては、例えば非特許文献2を参照されたい。

【0028】

図2は、自システムの中に6つのノードを有する例示的シナリオを示しており、本明細書に記載の方法およびノード1～6もさらに示している。また、図2の中には、他の（他のいくつかの）システムの他のユーザ10および11が存在する。この事例では、ノード1が、別のシステムのいくつかのリソースにおいて、ある種の通信が進行中であることを（誤ってまたは正しく）検出し、自ノードおよび自システム内の近くのノードによるこれらのリソースの使用をブロックするつもりである。ノード1は、リソースを内部でブロックし、ホップカウンタ値を2に設定したSABメッセージを、フラッディングを使用して送信する。ノード2、3、4は、ノード1から届くところにあり、SABメッセージを受信する。それらのノードのそれぞれは、ホップカウンタを1だけ減少して値1にし、ブロックされたチャンネルを内部登録し、フラッディングを使用してSABメッセージを転送する。ノード1は、ノード2、3、4から転送されたSABメッセージを受信するが、自ノードが送信したのと同じメッセージと認識し、それ以上の動作は行わない。ノード3、4

40

50

は、届く範囲内にあり、互いから転送されたSABメッセージを受信する。しかし、そのメッセージを自ノードが既に受信して対応したメッセージと認識し、それ以上の動作は行わない。ノード5は、ノード4からSABメッセージを受信し、ブロックされたチャンネルを内部登録する。次いで、ホップカウンタを値0に減少し、メッセージをこれ以上転送すべきでないことに気付く。従って、ノード6は、ノード5から届く範囲内にあるがSABメッセージを受信せず、チャンネルの使用を自由に考慮できる。これは道理にかなっている。ノード6はノード1から十分に離れているので、ノード6の位置ではリソースを利用可能かもしれないからである。

【0029】

図3では、自システム内に、1～6と番号が付いており且つブロードキャストルーティングツリーで図に従って接続された、6つのノードを有する別の例示的シナリオが示されている。また、別の（他のいくつかの）システムの他のいくつかのユーザもいる。この事例では、ノード1が、別のシステムにおいてある種の通信が進行中であることを（誤ってまたは正しく）検出し、自ノードおよび自システム内の近くのノードによるこれらのリソースの使用をブロックするつもりである。ノード1は、リソースを内部でブロックし、ホップカウンタ値を2に設定したSABメッセージをブロードキャストツリーで隣接するノードに送信する。ノード2、3、4が、SABメッセージを受信する。それらのノードのそれぞれは、ホップカウンタを1だけ減少して値1にし、ブロックされたチャンネルを内部登録し、それぞれの隣接するノードにSABメッセージを転送する（が、ノード1には返送しない）。ノード5は、ノード4からSABメッセージを受信し、ブロックされたチャンネルを内部登録する。次いで、ホップカウンタを値0に減少し、メッセージをこれ以上転送すべきでないことに気付く。従って、ノード6は、ノード5に接続されているがSABメッセージを受信せず、チャンネルの使用を自由に考慮できる（これは道理にかなっている。ノード6はノード1から十分に離れているので、ノード6の位置ではリソースを利用可能かもしれないからである）。オプションで、正しく受信されたメッセージはそれぞれ、図3に示されるように肯定応答（ACK）されてもよい。

【0030】

図4には、本明細書に記載の例示の実施形態の1つに従って機能を実行できるノード400の機能ブロックが示されている。それ故、ノードは、一実施形態に従って、以下を備えてもよい。

【0031】

TRX：データを送受信するための送受信部401。

【0032】

感知検出部：少なくとも1つの自己測定値に基づき、リソースの使用確率の推定値を計算できるユニット403。

【0033】

SABメッセージ抽出部：メッセージをSABメッセージと識別し、ブロックされるチャンネルの情報を抽出し、その情報を制御部（制御部はどのチャンネルがブロックされているかを常に把握する）および／またはSABメッセージ転送部409に渡すユニット405。

【0034】

ACK／NAK：SABメッセージの信頼できる配信を保証するために、受信したSABメッセージに関してACKまたはNAKを送信しうるユニット407。

【0035】

SABメッセージ転送部：SABメッセージ転送部409は、受信したSABメッセージを転送すべきか否かを決定するように構成され、そのメッセージをTRX部401に渡す前に、正しいフォーマットを与え、（ホップカウンタや類似のものなどの）関連フィールドを更新する。

【0036】

SABメッセージ構成部：SABメッセージ構成部411は、制御部415からどのチ

10

20

30

40

50

チャンネルをどのくらいの間ブロックすべきか等の情報を与えられて、新しいSABメッセージを組み立てるように構成されたユニットである。

【0037】

ブロードキャストツリー・データベース：ブロードキャストツリー・データベース部413は、メッセージがブロードキャストツリーの中を送信される場合に、例えば1つ以上の転送テーブルなどで、隣接ノードを常に把握するように構成されたユニットである。

【0038】

制御：制御部415は、SAB機能を制御するように構成される。ユニット415は、例えば、どのチャンネルが現在ブロックされているかを常に把握しており、新しいSABメッセージを組み立てるべきかどうかを決定し、感知を実行すべきときはいつでもTRX部および感知検出部を起動するなどのように構成されてもよい。

【0039】

動作例A：

制御部415は、（例えば、周期的スキームに従って）感知をいつ実行すべきかを常に把握している。感知を実行する時間になると、制御部415は、TRX部401および感知検出部403を起動する。TRX部401からの情報に基づき、感知検出部403は、チャンネルが使用されている確率の推定値を作り、これを制御部415に転送する。制御部415は、少なくともこの確率に基づきチャンネルがブロックされるべきであると決定した場合、SABメッセージ構成部411に情報を送信して、SABメッセージ構成部411が（たぶんブロードキャストツリー・データベース部からの情報を使用して）SABメッセージを作りうるようにする。次いで、このSABメッセージは、TRX部401に送られ送信される。

【0040】

動作例B：

TRX部401がメッセージを受信する。このメッセージは、SABメッセージ抽出部405に渡され、このSABメッセージ抽出部405は、そのメッセージをSABメッセージと識別し、どのチャンネルをどのくらいの間ブロックすべきかの情報を抽出する。1つのシナリオによれば、SABメッセージ抽出部405は、メッセージをACK部407に送り、このACK部407は、受け取ったSABメッセージに関してACK（またはメッセージが正しく受信されなかった場合、NAK）を送信する。SABメッセージ抽出部405が抽出した情報は、制御部415に送られ、この制御部415は、ブロックされるチャンネルを登録するが、デバイスが、どのチャンネルでも利用する前には、どのチャンネルがブロックされているかを制御部415にチェックし、それらの使用を避けることを意図してのことである。SABメッセージ情報は、SABメッセージ抽出部405からSABメッセージ転送部407にも送られ、このSABメッセージ転送部407は、メッセージを転送すべきか否かを決定する。メッセージを転送すべき場合、SABメッセージ転送部407は、メッセージフィールドを更新し、転送するためにそのメッセージをTRX部401に送る。

【0041】

図5には、上述の無線ノードが実行する手順のいくつかのステップを表すフロー図が示されている。こうして、無線システムの無線スペクトルへのアクセスを制御する無線ノードが提供される。無線ノードは、無線システムの他の無線ノードと連絡を取り、情報を交換する。無線ノードは、以下の手順ステップを実行しうる。まず、ステップ501において、無線ノードは無線システムのユーザによる無線リソースの使用を検出する。次にステップ503において、無線ノードは、無線システムの少なくとも1つの他の無線ノードに、検出した無線リソースへのアクセスをブロックするためのメッセージを送信する。ステップ505において、このアクセスをブロックするメッセージによって、無線ノードは無線リソースへのアクセスを制御する。

【0042】

無線システムにおいて本方法および本無線システムノードを使用することによって、（あるリソースで）一次ユーザを検出したユーザの近くのユーザが、そのスペクトルにアクセスして一次ユーザに干渉を引き起こすのを阻止する、非常に簡単な分散アプローチが提供されるであろう。

【図 1】

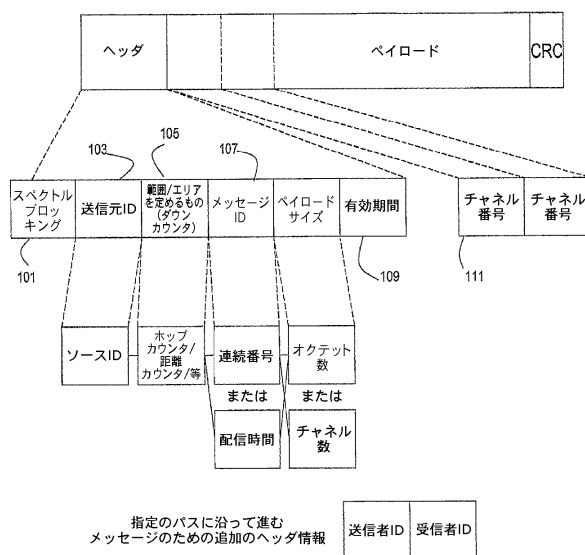


Fig. 1

【図 2】

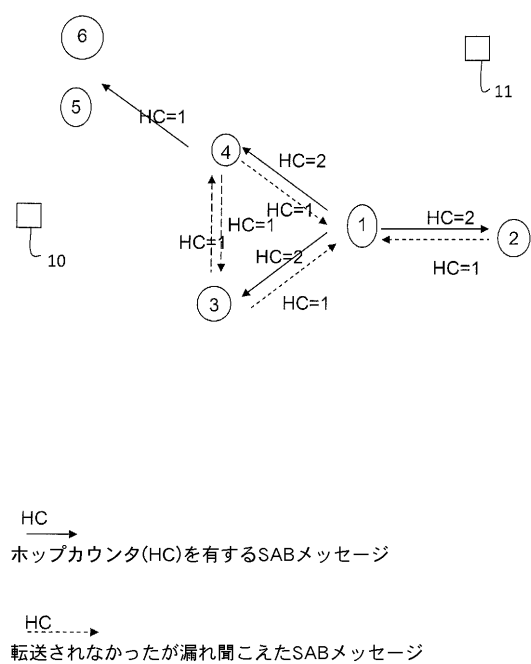


Fig. 2

【図 3】

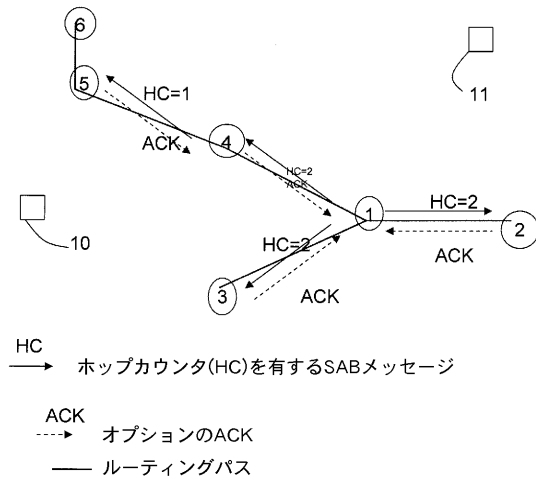


Fig. 3

【図 4】

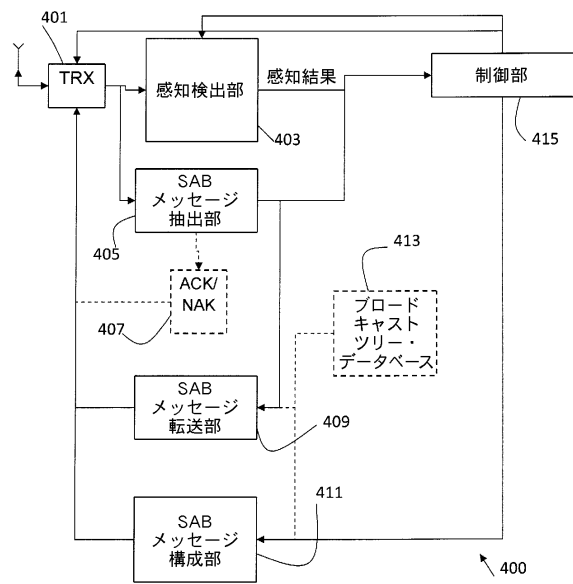


Fig. 4

【図 5】

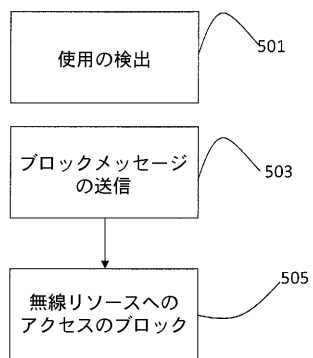


Fig. 5

フロントページの続き

- (72)発明者 ラーション, ペテル
スウェーデン国 ソルナ エス-169 71, バロンガタン 2, 1ティーアール
- (72)発明者 プライツ, ミカエル
スウェーデン国 レニンゲ エス-144 63, グスタフスルンズヴェーゲン 38
- (72)発明者 セレン, イングヴェ
スウェーデン国 ウプサラ エス-754 34, レストマカルガタン 8エー

審査官 小林 正明

- (56)参考文献 特開2002-198868 (JP, A)
特開2002-198867 (JP, A)
特開2007-166488 (JP, A)
特開2004-274192 (JP, A)
特開平11-177622 (JP, A)
国際公開第2007/056630 (WO, A2)
特表2009-514443 (JP, A)
特表2007-536841 (JP, A)
特開2005-222271 (JP, A)

- (58)調査した分野(Int.Cl., DB名)
- | | |
|------|-------|
| H04W | 16/14 |
| H04W | 40/02 |
| H04W | 84/18 |