(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2007-89006
(P2007-89006A)
(43)公開日　平成19年4月5日(2007.4.5)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	12/28	(2006.01)	H04L	12/28	300M	5K033
H04B	7/26	(2006.01)	H04B	7/26	K	5K067
H04Q	7/34	(2006.01)	H04B	7/26	106B	
			H04Q	7/04	C	

審査請求 未請求　請求項の数 20　ＯＬ　外国語出願　（全 22 頁）

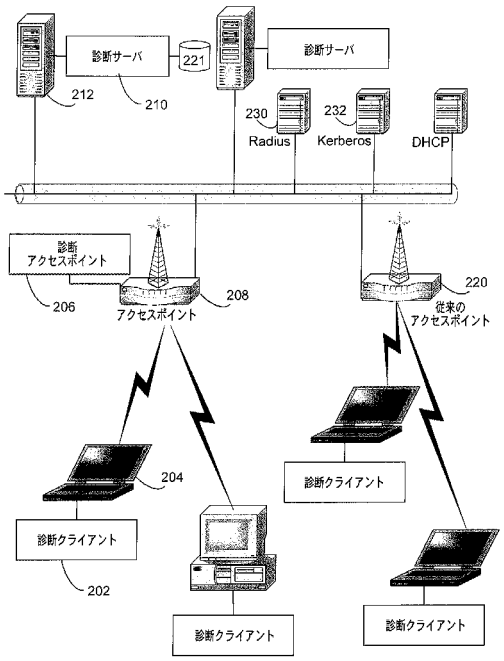
(21)出願番号　特願2005-277649 (P2005-277649)
(22)出願日　平成17年9月26日 (2005.9.26)

(71)出願人　500046438
マイクロソフト　コーポレーション
アメリカ合衆国　ワシントン州　９８０５２－６３９９　レッドモンド　ワン　マイクロソフト　ウェイ
(74)代理人　100077481
弁理士　谷　義一
(74)代理人　100088915
弁理士　阿部　和夫
(72)発明者　アトゥル　アドゥヤ
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内

最終頁に続く

(54)【発明の名称】無線ネットワーク内で接続を断たれたクライアントおよび不正なアクセスポイントを協調して見つけ出す方法

(57)【要約】
【課題】近隣のワイヤレスデバイスの協調を利用して、接続を断たれたワイヤレスデバイスおよび不正な無線アクセスポイントを見つけ出すことを可能にするための方法を提供する。
【解決手段】中央サーバは、近隣のクライアントの位置を計算し、それらの位置を使用して、接続を断たれたクライアントの位置を見積もる。これらの技術は、ＩＥＥＥ８０２．１１のビーコンメカニズムおよびプローブメカニズムを利用して、接続されているクライアントが、接続を断たれたクライアントを検出する上で不要なオーバーヘッドを費やさずにすむようにすることができる。近隣のデバイスから情報を協調して収集し、その情報をデータベースと比較することによって、不正なデバイスを検出してその位置を特定する。
【選択図】図２



【特許請求の範囲】
【請求項１】
第１のワイヤレスデバイスの位置を割り出すためのコンピュータ実行可能命令を含むコンピュータ可読媒体であって、前記コンピュータ実行可能命令は、前記第１のデバイスの付近に位置してインフラストラクチャネットワークに接続されている１つまたは複数の他のワイヤレスデバイス上で実行され、
前記第１のデバイスから１つまたは複数の信号を受信するステップと、
前記信号に従って前記第１のデバイスに関する信号強度情報を記録するステップと、
前記第１のデバイスの前記位置を見積もるために前記信号強度情報を診断サーバに送信するステップとを実行し、
前記診断サーバは、
前記送信された信号強度情報を受信するステップと、
前記１つまたは複数の他のワイヤレスデバイスの位置の見積もりを計算するステップと、
前記受信した信号強度情報および前記計算した前記１つまたは複数の他のワイヤレスデバイスの前記位置の見積もりを使用して前記第１のデバイスの前記位置を概算するステップとを実行することによって、前記第１のデバイスの前記位置を見積もることを特徴とするコンピュータ可読媒体。
【請求項２】
前記信号はビーコン信号であることを特徴とする請求項１に記載のコンピュータ可読媒体。
【請求項３】
前記信号は、前記第１のデバイスが前記インフラストラクチャネットワークに接続されていないと判定されたことに応答して、前記第１のデバイスによって送信されることを特徴とする請求項１に記載のコンピュータ可読媒体。
【請求項４】
前記第１のデバイスは、不正なまたは障害のある無線アクセスポイントであることを特徴とする請求項１に記載のコンピュータ可読媒体。
【請求項５】
前記第１のデバイスの前記位置は、約１２メートル以内の誤差で概算されることを特徴とする請求項１に記載のコンピュータ可読媒体。
【請求項６】
前記第１のデバイスの前記位置は、ＲＦホールにほぼ一致することを特徴とする請求項１に記載のコンピュータ可読媒体。
【請求項７】
第１のワイヤレスデバイスの位置を割り出すためのコンピュータ実行可能命令を含むコンピュータ可読媒体であって、前記ワイヤレスデバイスは、インフラストラクチャネットワークに接続されている１つまたは複数の他のワイヤレスデバイスの付近にあり、前記コンピュータ実行可能命令は、サーバ上で実行され、
前記１つまたは複数の他のデバイスから前記第１のデバイスに関する信号強度情報を受信するステップと、
前記１つまたは複数の他のワイヤレスデバイスの位置の見積もりを計算するステップと、
前記計算した見積もりおよび前記受信した信号強度情報を使用して前記第１のデバイスの前記位置を概算するステップとを実行することを特徴とするコンピュータ可読媒体。
【請求項８】
前記１つまたは複数の他のデバイスは、
前記第１のデバイスから１つまたは複数のビーコン信号を受信するステップと、
前記ビーコン信号に従って前記第１のデバイスに関する信号強度情報を記録するステップと、

前記第１のデバイスの前記位置を見積もるために前記信号強度情報を送信するステップとを実行することを特徴とする請求項７に記載のコンピュータ可読媒体。

【請求項９】

前記ビーコン信号は、前記第１のデバイスが前記インフラストラクチャネットワークに接続されていないと判定されたことに応答して、前記第１のデバイスによって送信されることを特徴とする請求項８に記載のコンピュータ可読媒体。

【請求項１０】

前記第１のデバイスは、不正なまたは障害のある無線アクセスポイントであることを特徴とする請求項７に記載のコンピュータ可読媒体。

【請求項１１】

前記第１のデバイスの前記位置は、約１２メートル以内の誤差で概算されることを特徴とする請求項７に記載のコンピュータ可読媒体。

【請求項１２】

前記第１のデバイスの前記位置は、ＲＦホールにほぼ一致することを特徴とする請求項７に記載のコンピュータ可読媒体。

【請求項１３】

インフラストラクチャネットワーク内で不正な無線アクセスポイントを識別するための方法において、

疑わしいアクセスポイントに関する情報を受信するステップであって、前記情報は１つまたは複数の付近のワイヤレスコンピューティングデバイスまたはアクセスポイントによって収集されるステップと、

前記情報をアクセスポイントデータベースと比較するステップと、

前記情報が前記アクセスポイントデータベースと整合しない場合に、前記疑わしいアクセスポイントを不正なものとして識別するステップとを含むことを特徴とする方法。

【請求項１４】

前記情報は、信号強度情報、ＭＡＣアドレス、ＳＳＩＤ、およびチャネル情報のうちの１つまたは複数の組合せを含むことを特徴とする請求項１３に記載の方法。

【請求項１５】

前記情報はＭＡＣアドレスを含み、前記ＭＡＣアドレスは、前記疑わしいアクセスポイントのビーコンを聴くことによって、前記１つまたは複数の付近のワイヤレスデバイスによって得られることを特徴とする請求項１３に記載の方法。

【請求項１６】

前記情報はＭＡＣアドレスを含み、前記ＭＡＣアドレスは、

プローブ要求を送信するステップと、

前記疑わしいアクセスポイントからプローブ応答を受信するステップと、

前記プローブ応答から前記ＭＡＣアドレスを検索するステップとを含む方法を実行することによって、前記１つまたは複数の付近のワイヤレスデバイスによって得られることを特徴とする請求項１３に記載の方法。

【請求項１７】

前記情報は信号強度情報を含み、前記方法は、

受信した前記信号強度情報を使用して、前記疑わしいアクセスポイントの位置を見積もるステップと、

前記見積もった位置が前記アクセスポイントデータベースと整合しない場合に、前記疑わしいアクセスポイントを不正なものとして識別するステップとをさらに含むことを特徴とする請求項１３に記載の方法。

【請求項１８】

前記位置を見積もるステップは、

前記付近のワイヤレスコンピューティングデバイスまたはアクセスポイントの位置の見積もりを計算するステップと、

前記計算した見積もりおよび受信した信号強度情報を使用して、前記疑わしいアクセス

ポイントの前記位置をさらに見積もるステップとを含むことを特徴とする請求項１７に記載の方法。
【請求項１９】
前記情報はチャネル情報を含み、前記方法は、
前記アクセスポイントデータベース内に示されているチャネルと重ならないチャネル上で前記疑わしいアクセスポイントが送信を行っている場合に、前記疑わしいアクセスポイントを不正なものとして識別するステップをさらに含むことを特徴とする請求項１３に記載の方法。
【請求項２０】
認証されたアクセスポイントから更新要求を受信したことに応答して、新たな情報によって前記アクセスポイントデータベースを更新するステップをさらに含むことを特徴とする請求項１３に記載の方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般にネットワークオペレーションに関し、より詳細には、無線ネットワーク内で接続を断たれたデバイスまたは無許可のデバイスを見つけ出すことに関する。
【背景技術】
【０００２】
無線ネットワーキングの利便性のために、無線ネットワーク（たとえばＩＥＥＥ８０２．１１ネットワーク）が広範囲に採用されている。企業、大学、家庭、および公共の場において、これらのネットワークは、著しい割合で展開されている。しかしエンドユーザおよびネットワーク管理者にとっては、相当な数の「悩みの種」が依然として存在している。ユーザは、断続的な接続性、貧弱なパフォーマンス、受信可能範囲の欠如、および認証の失敗など、複数の問題を経験する。これらの問題は、アクセスポイントの不適切な配置、デバイスの構成ミス、ハードウェアおよびソフトウェアのエラー、無線メディアの性質（たとえば干渉や伝搬）、ならびにトラフィックの混雑など、さまざまな理由で発生する。ユーザは、接続性およびパフォーマンスの問題に関して頻繁に不満を表明し、ネットワーク管理者は、企業のセキュリティおよび受信可能範囲を管理しつつ、これらの問題を診断することを期待されている。無線メディアの不確かな性質のため、またこれらの問題の原因を突き止めるためのインテリジェントな診断ツールがないため、彼らの課題は特に困難である。
【０００３】
ＩＥＥＥ８０２．１１ネットワークを大規模に展開する企業にとっては、多くの建物にわたって広がる数千のアクセスポイント（ＡＰ）が存在する場合がある。ネットワークに伴う問題の結果、エンドユーザのフラストレーションが生じ、企業にとっての生産性が失われる。さらに、１人のエンドユーザの不満を解消すれば、企業のＩＴ部門にとってはさらなるサポート要員のコストが発生する結果となる。このコストは数十ドルになる場合もあり、またこれには、エンドユーザの生産性が失われることによるコストは含まれていない。
【０００４】
ＩＥＥＥ８０２．１１インフラストラクチャネットワークにおける障害診断は、無線ネットワーキングの研究における他のより注目度の高い領域に比べて、研究団体から注目を集めていない。いくつかの企業が診断ツールの提供を試みているが、これらの製品には、複数の望ましい特徴が欠けている。たとえばこれらの製品は、データを収集および分析して、問題の原因として考えられるものを確立するという総合的なジョブを行わない。さらに大半の製品は、通常はＡＰからのデータを収集するのみであり、ネットワークのクライアント側からの視点を無視している。クライアントの視点からネットワークをモニタするいくつかの製品は、ハードウェアセンサを必要とし、これは展開および保守する上で高く

つく場合がある。また現在のソリューションは通常、接続を断たれたクライアントに対しては、たとえそれらが最も支援を必要とするクライアントであったとしても、何らサポートを提供しない。

【０００５】

【非特許文献１】the literature described by P. Bahl and V. N. Padmanabhan in "RADAR: An Inbuilding RF-based User Location and Tracking System," in Proc. of IEEE INFOCOM, Tel-Aviv, Israel, March 2000

【非特許文献２】the literature described by A. Ladd et al. in "Robotics-Based Location Sensing using Wireless Ethernet（登録商標）," in Proc. of ACM MobiCom, Atlanta, GA, Sept 2002

【発明の開示】

【発明が解決しようとする課題】

【０００６】

概略を上述したこの問題には、本明細書に記載するような無線ネットワーク内の障害を検出および診断するためのシステムおよび方法によって、少なくとも部分的に対処することができる。

【課題を解決するための手段】

【０００７】

以降では、読者に対して基本的な理解を提供するために、本開示の簡略化した概要を提示する。この概要は、本開示を網羅的または限定的に概観したものではない。この概要を提供する目的は、いかなる形においても、本発明の鍵となる要素および、または必要不可欠な要素を明らかにすることではなく、本発明の範囲を画定することでもなく、あるいは本発明の範囲を限定することでもない。その唯一の目的は、以降で提示されるさらに詳細な説明への前置きとして、開示される発想のいくつかを簡略化した形態で提示することである。

【０００８】

一実施形態では、本明細書に記載のモニタリングアーキテクチャは、無線ネットワークからの接続を断たれたクライアントマシンを見つけ出すために使用される。別の実施形態では、このアーキテクチャは、企業の無線ネットワーク内で不正な(rogue)または無許可のアクセスポイントを検出するために使用される。

【０００９】

一実施形態では、接続を断たれたワイヤレスコンピューティングデバイスの位置を割り出すためのコンピュータ実行可能命令を含むコンピュータ可読メディアが提供され、このワイヤレスコンピューティングデバイスは、インフラストラクチャネットワークからの接続を断たれており、このコンピュータ実行可能命令は、接続を断たれたデバイスの付近にある１つまたは複数の接続されたワイヤレスコンピューティングデバイス上で実行され、接続を断たれたデバイスから１つまたは複数のビーコン信号を受信するステップと、そのビーコン信号に従って接続を断たれたデバイスに関する信号強度情報を記録するステップと、接続を断たれたデバイスがインフラストラクチャネットワークに接続されていないことを診断サーバに知らせるステップと、接続を断たれたデバイスの位置を見積もるために信号強度情報を診断サーバに送信するステップとを実行し、ビーコン信号は、接続を断たれたデバイスがインフラストラクチャネットワークに接続されていないと判定されたことに応答して、そのデバイスによって送信される。

【００１０】

別の実施形態では、接続を断たれたワイヤレスコンピューティングデバイスの位置を割り出すためのコンピュータ実行可能命令を含むコンピュータ可読メディアが提供され、このワイヤレスコンピューティングデバイスは、インフラストラクチャネットワークからの接続を断たれており、インフラストラクチャネットワークに接続されている１つまたは複数のワイヤレスデバイスの付近にあり、このコンピュータ実行可能命令はサーバ上で実行され、接続を断たれたデバイスに関する信号強度情報を１つまたは複数の接続されたデバ

イスから受信するステップと、１つまたは複数の接続されたデバイスの位置の見積もりを計算するステップと、計算した見積もりおよび受信した信号強度情報を使用して、接続を断たれたデバイスの位置を概算するステップとを実行する。

【００１１】

さらに別の実施形態では、インフラストラクチャネットワーク内で不正な無線アクセスポイントを識別するための方法が提供され、この方法は、疑わしいアクセスポイントに関する情報を受信するステップであって、その情報は１つまたは複数の付近のワイヤレスコンピューティングデバイスまたはアクセスポイントによって収集されるステップと、その情報をアクセスポイントデータベースと比較するステップと、その情報がアクセスポイントデータベースと整合しない場合に、その疑わしいアクセスポイントを不正なものとして識別するステップとを含む。

【００１２】

添付の特許請求の範囲は、特殊性を有する本発明の特徴を説明しているが、本発明およびその利点は、以降の詳細な説明を添付の図面と併せて読めば、最もよく理解することができる。

【発明を実施するための最良の形態】

【００１３】

接続を断たれたクライアントを見つけ出し、不正なアクセスポイントを検出するための方法およびシステムについて、好ましい実施形態を参照して説明するが、本発明の方法およびシステムは、それらに限定されるものではない。さらに本明細書に記載の方法およびシステムは代表的なものにすぎず、本発明の趣旨および範囲から逸脱することなく変形形態を作成できることを当業者なら容易に理解するであろう。この説明を吟味すれば、説明の内容は単なる例示であり、限定ではなく、例として提示されているにすぎないことが、当業者には明らかになるはずである。多数の修正および他の例示的な実施形態は、当技術分野の標準的な技術の１つの範囲内にあり、本発明の範囲内に収まるものと考えられる。詳細には、本明細書で提示される例の多くは、方法の工程やシステムの要素の具体的な組合せを含むが、それらの工程およびそれらの要素を他の方法で組み合わせても、同じ目的を達成できることが理解できるはずである。１つの実施形態にのみ関連して論じられている工程、要素、および特徴は、他の実施形態における同様の役割から除外されることを意図するものではない。さらに、請求項の要素を修飾するために請求項内で「第１の」および「第２の」などの序数の用語を使用すること自体は、１つの請求項要素の別の請求項要素に対する何らかの優先度、優位性、または序列、あるいは方法の工程が実行される時間的な順序を示すものではなく、ある名前を有する１つの請求項要素を（序数用語の使用を除いて）同じ名前を有する別の要素から区別するためのラベルとして使用して、請求項の要素を区別しているにすぎない。

【００１４】

企業の無線ネットワークを使用および保守する際にユーザおよびネットワーク管理者が直面する問題の多くを以下に列挙する。

【００１５】

接続性の問題：エンドユーザは、建物の特定のエリアにおけるネットワーク接続性の不整合または欠如に関して不満を表明する。このような「デッドスポット」(dead spot)または「ＲＦホール」は、弱いＲＦ信号、信号の欠如、環境条件の変化、または障害物のために発生することがある。ＲＦホールを自動的に見つけ出すことは、無線管理者にとって重要である。その結果、彼らは、問題のエリア内でＡＰの配置を変えるか、またはＡＰの密度を高めることによって、あるいは受信可能範囲(coverage)を改善するために付近のＡＰ上の電力設定(power setting)を調整することによって、問題を解決することができる。

【００１６】

パフォーマンスの問題：このカテゴリは、クライアントがパフォーマンスの低下、たとえば低いスループットや長い待ち時間を目にするすべての状況を含む。パフォーマンスの

問題が存在する理由としては、たとえば混雑によるトラフィックの減速、電子レンジやコードレス電話によるＲＦの干渉、多経路干渉、不適切なネットワーク計画または不適切に構成されたクライアント／ＡＰによる大規模な同一チャネル干渉など、複数の理由が考えられる。またパフォーマンスの問題は、たとえば低速のサーバまたはプロキシによるネットワークの非無線部分における問題の結果として発生する場合もある。したがって、問題が無線ネットワーク内にあるのかまたは他の部分にあるのかどうかを診断ツールが判断できることは有用である。さらに、無線部分内の原因を識別することは、ネットワーク管理者がシステムをよりよく設定し、エンドユーザにとっての経験を改善できるようにする上で重要である。

【００１７】

ネットワークのセキュリティ：大企業は、自らのネットワークを保護するために、ＩＥＥＥ８０２．１ｘなどのソリューションを使用していることが多い。しかし従業員が、無許可のＡＰを企業のネットワークのイーサネット（登録商標）タップへ接続することによって、ネットワークのセキュリティを無意識のうちに危険にさらすと、ＩＴマネージャにとっては悪夢のようなシナリオが発生する。この問題は、一般に「不正なＡＰの問題」と呼ばれる。これらの不正なＡＰは、無線ネットワークのセキュリティに対する最も頻繁に発生する深刻な侵害の１つである。このようなＡＰの存在によって、外部のユーザが、企業のネットワーク上のリソースにアクセスすることができ、これらのユーザは、情報を漏洩するか、または他の損害を招くことがある。さらに、不正なＡＰは、付近にある他のアクセスポイントへの干渉を引き起こす場合がある。大規模なネットワーク内で手動のプロセスを介して不正なＡＰを検出することには、費用および時間がかかるため、このようなＡＰを事前対処的に検出することが重要である。

【００１８】

認証の問題：ＩＴサポートグループのログによれば、複数の不満は、ユーザが自分自身をネットワークに対して認証できないことに関連している。ＩＥＥＥ８０２．１ｘなどの技術によって保護されている無線ネットワークでは、認証の失敗は通常、証明書がないこと、またはその有効期限が切れていることに起因する。したがって、このような認証の問題を検出して、クライアントが有効な証明書をブートストラップするのを補助することが重要である。本発明は、以降の詳細な説明を通じてより完全に理解され、これは添付の図面と併せて読むべきである。この説明では、同様の番号は、本発明のさまざまな実施形態における同様の要素を指している。本発明の態様は、適切なコンピューティング環境内に実装されるものとして示されている。必須ではないが、本発明については、パーソナルコンピュータによって実行される、プロシージャなどのコンピュータ実行可能命令という一般的なコンテキストにおいて説明する。一般にプロシージャは、特定のタスクを実行したり特定の抽象データ型を実装したりするプログラムモジュール、ルーチン、関数、プログラム、オブジェクト、コンポーネント、データ構造などを含む。さらに本発明は、ハンドヘルドデバイス、マルチプロセッサシステム、マイクロプロセッサベースの家庭用電化製品またはプログラム可能な家庭用電化製品、ネットワークＰＣ、ミニコンピュータ、メインフレームコンピュータなどを含む他のコンピュータシステム構成と共に実施できることを当業者なら理解するであろう。本発明は、通信ネットワークを介してリンクされるリモート処理デバイスによってタスクが実行される分散コンピューティング環境において実施することもできる。分散コンピューティング環境では、プログラムモジュールは、ローカルメモリストレージデバイスおよびリモートメモリストレージデバイスの双方に配置することができる。コンピュータシステムという用語は、分散コンピューティング環境内で見受けられるようなコンピュータのシステムを指すために使用することができる。

【００１９】

図１は、本発明の態様を実装できる適切なコンピューティングシステム環境１００の一例を示している。このコンピューティングシステム環境１００は適切なコンピューティング環境の一例にすぎず、本発明の使用または機能の範囲に対して何らかの限定を提示することを意図するものではない。またコンピューティングシステム環境１００が、この典型

的な動作環境１００内に示されたコンポーネントの任意の１つまたは組合せに関して何らかの依存性または必要性を有すると解釈すべきでもない。本発明の一実施形態は、典型的な動作環境１００に示されているそれぞれのコンポーネントを実際に含むが、本発明の別のより典型的な実施形態では、必須ではないコンポーネント、たとえばネットワーク通信に必要とされる以外の入力／出力デバイスは除外される。

【００２０】

図１を参照すると、本発明を実装するための典型的なシステムは、汎用コンピューティングデバイスをコンピュータ１１０の形態で含む。コンピュータ１１０のコンポーネントは、処理装置１２０と、システムメモリ１３０と、システムメモリを含むさまざまなシステムコンポーネントを処理装置１２０に結合するシステムバス１２１とを含むことができるが、これらには限定されない。システムバス１２１は、メモリバスまたはメモリコントローラと、ペリフェラルバスと、さまざまなバスアーキテクチャのいずれかを使用するローカルバスとを含む複数のタイプのバス構造のいずれにすることもできる。たとえばこのようなアーキテクチャは、ＩＳＡ（Ｉｎｄｕｓｔｒｙ Ｓｔａｎｄａｒｄ Ａｒｃｈｉｔｅｃｔｕｒｅ）バス、ＭＣＡ（Ｍｉｃｒｏ Ｃｈａｎｎｅｌ Ａｒｃｈｉｔｅｃｔｕｒｅ）バス、ＥＩＳＡ（Ｅｎｈａｎｃｅｄ ＩＳＡ）バス、ＶＥＳＡ（Ｖｉｄｅｏ Ｅｌｅｃｔｒｏｎｉｃｓ Ｓｔａｎｄａｒｄｓ Ａｓｓｏｃｉａｔｉｏｎ）ローカルバス、およびメザニンバスとしても知られているＰＣＩ（Ｐｅｒｉｐｈｅｒａｌ Ｃｏｍｐｏｎｅｎｔ Ｉｎｔｅｒｃｏｎｎｅｃｔ）バスを含むが、これらには限定されない。

【００２１】

コンピュータ１１０は通常、さまざまなコンピュータ可読メディアを含む。コンピュータ可読メディアは、コンピュータ１１０によってアクセスできる利用可能な任意のメディアとすることができ、揮発性メディアおよび不揮発性メディア、ならびに取り外し可能メディアおよび固定式メディアの双方を含む。たとえばコンピュータ可読メディアは、コンピュータストレージメディアおよび通信メディアを含むことができるが、これらには限定されない。コンピュータストレージメディアは、コンピュータ可読命令、データ構造、プログラムモジュール、他のデータなどの情報を記憶するための任意の方法または技術において実装される揮発性メディアおよび不揮発性メディア、ならびに取り外し可能メディアおよび固定式メディアを含む。コンピュータストレージメディアは、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリまたは他のメモリ技術、ＣＤ－ＲＯＭ、デジタル多用途ディスク（ＤＶＤ）または他の光ディスクストレージ、磁気カセット、磁気テープ、磁気ディスクストレージまたは他の磁気ストレージデバイス、あるいは希望の情報を保存するために使用可能で、コンピュータ１１０によってアクセス可能な他の任意のメディアを含むが、これらには限定されない。通信メディアは通常、搬送波や他の伝送メカニズムなどの変調されたデータ信号内のコンピュータ可読命令、データ構造、プログラムモジュール、または他のデータを具体化し、任意の情報伝達メディアを含む。「変調されたデータ信号」という用語は、情報をその信号内でコード化するような方法で設定または変更されたその特性のうちの１つまたは複数を有する信号を意味する。たとえば通信メディアは、有線ネットワークや直接有線接続などの有線メディアと、音波メディア、ＲＦメディア、赤外線メディア、他の無線メディアなどの無線メディアとを含むが、これらには限定されない。また上記のいずれの組合せも、コンピュータ可読メディアの範囲内に含まれるものである。

【００２２】

システムメモリ１３０はコンピュータストレージメディアを読み取り専用メモリ（ＲＯＭ）１３１およびランダムアクセスメモリ（ＲＡＭ）１３２などの揮発性メモリおよび／または不揮発性メモリの形態で含む。基本入出力システム１３３（ＢＩＯＳ）は、起動中などにコンピュータ１１０内の要素間における情報伝達を補助する基本ルーチンを含み、通常はＲＯＭ１３１内に格納されている。ＲＡＭ１３２は通常、処理装置１２０がすぐにアクセスできるか、および／または処理装置１２０によってその時点で操作されているデータモジュールおよび／またはプログラムモジュールを含む。図１は、例としてオペレー

ティングシステム１３４、アプリケーションプログラム１３５、他のプログラムモジュール１３６、およびプログラムデータ１３７を示しているが、これらには限定されない。

【００２３】

またコンピュータ１１０は、他の取り外し可能／固定式、揮発性／不揮発性コンピュータストレージメディアを含むこともできる。図１は、例示のみを目的として、固定式の不揮発性の磁気メディアとの間で読み取りや書き込みを行うハードディスクドライブ１４１と、着脱式不揮発性の磁気ディスク１５２との間で読み取りや書き込みを行う磁気ディスクドライブ１５１と、ＣＤ－ＲＯＭや他の光メディアなどの着脱式不揮発性の光ディスク１５６との間で読み取りや書き込みを行う光ディスクドライブ１５５とを示している。典型的な動作環境において使用できる他の取り外し可能／固定式、揮発性／不揮発性コンピュータストレージメディアとしては、磁気テープカセット、フラッシュメモリカード、デジタル多用途ディスク、デジタルビデオテープ、ソリッドステートＲＡＭ、ソリッドステートＲＯＭなどがあるが、これらには限定されない。ハードディスクドライブ１４１は通常、インターフェース１４０などの固定式のメモリインターフェースを介してシステムバス１２１に接続されており、磁気ディスクドライブ１５１および光ディスクドライブ１５５は通常、インターフェース１５０などの着脱式メモリインターフェースによってシステムバス１２１に接続されている。

【００２４】

図１に示した上述のドライブおよびそれに関連するコンピュータストレージメディアは、コンピュータ１１０用のコンピュータ可読命令、データ構造、プログラムモジュール、および他のデータの記憶を提供する。たとえば図１において、ハードディスクドライブ１４１は、オペレーティングシステム１４４、アプリケーションプログラム１４５、他のプログラムモジュール１４６、およびプログラムデータ１４７を記憶するものとして図示されている。これらのコンポーネントは、オペレーティングシステム１３４、アプリケーションプログラム１３５、他のプログラムモジュール１３６、およびプログラムデータ１３７と同一とするか、または異なっていてもよい点に留意されたい。ここでは、オペレーティングシステム１４４、アプリケーションプログラム１４５、他のプログラムモジュール１４６、およびプログラムデータ１４７が最低限異なるコピーであることを示すために、異なる番号を割り当てている。ユーザは、タブレットまたは電子デジタイザ１６４、マイクロフォン１６３、キーボード１６２、および通常はマウス、トラックボール、またはタッチパッドと呼ばれるポインティングデバイス１６１などの入力デバイスを介してコンピュータ１１０にコマンドおよび情報を入力することができる。他の入力デバイス（図示せず）は、ジョイスティック、ゲームパッド、衛星放送受信用アンテナ、スキャナなどを含むことができる。これらの入力デバイスおよび他の入力デバイスは、システムバスに結合されているユーザ入力インターフェース１６０を介して処理装置１２０に接続される場合が多いが、パラレルポート、ゲームポート、ユニバーサルシリアルバス（ＵＳＢ）などの他のインターフェースおよびバス構造によって接続することもできる。またモニタ１９１や他のタイプのディスプレイデバイスをビデオインターフェース１９０などのインターフェースを介してシステムバス１２１に接続することもできる。モニタ１９１は、タッチスクリーンパネルなどと一体化することもできる。モニタおよび／またはタッチスクリーンパネルは、タブレットタイプのパーソナルコンピュータにおけるように、コンピュータ１１０が内蔵されている筐体に物理的に結合できる点に留意されたい。さらに、コンピューティングデバイス１１０などのコンピュータは、スピーカ１９７およびプリンタ１９６などの他の周辺出力デバイスを含むこともでき、これは周辺出力インターフェース１９４などを介して接続することができる。

【００２５】

コンピュータ１１０は、リモートコンピュータ１８０などの１つまたは複数のリモートコンピュータへの論理接続を使用して、ネットワーク化された環境内で動作することができる。リモートコンピュータ１８０は、パーソナルコンピュータ、サーバ、ルータ、ネットワークＰＣ、ピアデバイス、または他の一般的なネットワークノードとすることができ

、図１にはメモリストレージデバイス１８１しか示されていないが、通常はコンピュータ１１０に関連する上述の要素の多くまたはすべてを含む。図１に示されている論理接続は、ローカルエリアネットワーク（ＬＡＮ）１７１およびワイドエリアネットワーク（ＷＡＮ）１７３を含むが、他のネットワークを含むこともできる。こうしたネットワーキング環境は、オフィス、企業規模のコンピュータネットワーク、イントラネット、およびインターネットにおいてよく見受けられる。

【００２６】

ＬＡＮネットワーキング環境において使用する場合、コンピュータ１１０は、ネットワークインターフェースまたはアダプタ１７０を介してＬＡＮ１７１に接続される。ＷＡＮネットワーキング環境において使用する場合、コンピュータ１１０は通常、モデム１７２、またはインターネットなどのＷＡＮ１７３上で通信を確立するための他の手段を含む。モデム１７２は内蔵型または外付け型とすることができ、ユーザ入力インターフェース１６０または他の適切なメカニズムを介してシステムバス１２１に接続することができる。ネットワーク化された環境では、コンピュータ１１０に関連して示されているプログラムモジュール、またはその一部をリモートメモリストレージデバイス内に格納することができる。図１は、例としてリモートアプリケーションプログラム１８５をメモリデバイス１８１上に常駐するものとして示しているが、この形態には限定されない。示されているネットワーク接続は代表的なものであり、コンピュータ間に通信リンクを確立する他の手段も使用できることが理解できるであろう。とりわけコンピュータ１１０は、ＩＥＥＥ８０２．１１のプロトコルに従って動作する無線ネットワーキングインターフェースまたはワイヤレスカードを含むことが好ましい。

【００２７】

本発明の一実施形態では、図２に示されているように、システムは複数のコンポーネントから構成される。診断クライアント（ＤＣ）２０２は、ワイヤレスクライアントマシン２０４上で作動するソフトウェアである。診断ＡＰ（ＤＡＰ）２０６は、アクセスポイント２０８上で作動する。診断サーバ（ＤＳ）２１０は、組織のバックエンドサーバ２１２上で作動する。

【００２８】

本発明のいくつかの実施形態では、診断クライアントモジュール２０２は、ＲＦ環境、および近隣のクライアント２１４およびＡＰ２１６からのトラフィックの流れをモニタする。通常の活動中は、クライアントのワイヤレスカードは、混合モード(promiscuous mode)には設定されていない。ＤＣ２０２は、収集されたデータを使用して、ローカルな障害診断を実行する。個々の障害検出メカニズムに応じて、このデータの要約が、好ましくは定期的な間隔でＤＡＰ２０６またはＤＳ２１０へ送信される。その上、ＤＣ２０２は、たとえば混合モードへ切り替わって付近のクライアントのパフォーマンスの問題を分析することなど、オンデマンドのデータ収集を実行するためのコマンドをＤＡＰ２０６またはＤＳ２１０から受け入れるようにプログラムされている。ワイヤレスクライアント２０４の接続が断たれた場合、ＤＣ２０２は、データをローカルのデータベース／ファイルに記録する。このデータは、その後どこかの時点でネットワークの接続性が復旧した際にＤＡＰ２０６またはＤＳ２１０によって分析することができる。

【００２９】

診断ＡＰ２０６は、ＤＣ２０２から診断メッセージを受け入れ、自分自身の測定値(measurement)と共にそれらのメッセージをマージし、要約レポートをＤＳ２１０へ送信する。本発明のいくつかの実施形態は、診断ＡＰ２０６を含まない。ＤＡＰ２０６は、ＤＳ２１０の作業負荷を軽減する。本発明のいくつかの実施形態は、従来のＡＰ２２０とＤＡＰ２０６の混合形態を含み、ＡＰが従来のＡＰ２２０である場合、そのモニタリング機能はＤＣ２０２によって実行され、その要約機能およびチェックはＤＳ２１０によって実行される。

【００３０】

診断サーバ２１０は、ＤＣ２０２およびＤＡＰ２０６からデータを受け入れ、適切な分

析を実行して、さまざまな障害を検出および診断する。ＤＳ２１０は、それぞれのＡＰ２０８の位置を記憶するデータベース２２１にアクセスすることもできる。ネットワーク管理者は、システム内に複数のＤＳ２１０を展開して、たとえばそれぞれのＡＰのＭＡＣアドレスを特定のＤＳ２１０に細切れ(hash)にすることによって、負荷のバランスをとることができる。いくつかの実施形態では、診断サーバ２１０は、ＲＡＤＩＵＳ２３０およびＫｅｒｂｅｒｏｓ２３２のサーバなどの他のネットワークサーバと対話して、クライアントの認証およびユーザの情報を得る。

【００３１】

図２を参照して説明した典型的なシステムは、事後対処的なモニタリングと事前対処的なモニタリングの双方をサポートする。事前対処的なモニタリングでは、ＤＣおよびＤＡＰはシステムを継続的にモニタし、ＤＣ、ＤＡＰ、またはＤＳによって異常が検出されると、ネットワーク管理者が調査するよう警告を発する。事後対処的なモニタリングモードは、サポート要員がユーザの不満を診断したい場合に使用する。サポート要員は、問題を診断するためのデータを収集して分析するようＤＳの１つから特定のＤＣへ指示を出すことができる。

【００３２】

この典型的なシステムは、電力管理に関してわずかなオーバーヘッドしか課さない。後述する事前対処的な技術と事後対処的な技術の双方は、ごくわずかな帯域幅、ＣＰＵ、またはディスクのリソースしか消費せず、結果としてバッテリー消費にわずかな影響しか及ぼさない。図２に示されている典型的なシステムアーキテクチャは、ＤＣ、ＤＡＰ、およびＤＳを使用することによって、本発明の実施形態における複数の機能をサポートする。サポートされる機能のいくつかは、接続を断たれたクライアントを見つけ出すステップと、接続を断たれたクライアントを補助するステップと、パフォーマンスの問題を隔離するステップと、不正なアクセスポイントを検出するステップとを含む。

【００３３】

本発明のいくつかの実施形態では、ＤＡＰ２０６は、より優れた拡張性とＡＰのパフォーマンスの分析を可能にするようにＡＰ２０８上でソフトウェアを修正したものである。ハードウェアの修正が不要なため、この実施形態を展開する上での制約は少なくなる。

【００３４】

クライアントマシン２０４およびアクセスポイント２０８は、ビーコンおよびプローブ(probe)を制御できることが好ましい。さらにクライアントマシン２０４は、インフラストラクチャネットワークを開始できること（すなわちＡＰになれること）、またはその場限りの（すなわちコンピュータからコンピュータへの）ネットワークを自分自身で開始できることが好ましく、この能力は、現在市販されている多くのワイヤレスカードによってサポートされる。本発明のいくつかの実施形態は、付近のクライアントまたはアクセスポイントの存在を利用する。ソフトウェアの「センサ」を備えた付近のクライアントおよびアクセスポイントを利用することによって、展開のコストは潜在的に少なくなる。

【００３５】

バックエンドサーバ２１２は、データベースを使用して、ネットワーク内のすべてのアクセスポイントの位置を保持することが好ましい。このような位置データベースは、ネットワーク管理者によって保守されることが好ましい。

【００３６】

図２に示されている典型的なシステムは、システム内のクライアントおよびＡＰの数に伴って拡張することができる。このシステムは、ＤＳおよびＤＡＰという２つの共有リソースを含む。単一の診断サーバが潜在的なネックにならないように、システムの負荷が増加するにつれて、さらなるＤＳを追加することが好ましい。さらに、いくつかの実施形態では、それぞれの個々のＤＳは、診断の負荷をＤＣおよびＤＡＰと共有することによって作業負荷を軽減することができ、ＤＳは、ＤＣおよびＤＡＰが問題を診断できず、分析に全体的な視点およびさらなるデータが必要な場合にのみ使用される（たとえば、接続を断たれたクライアントを見つけ出すために、複数のＤＡＰから得られた信号強度情報が必要

となる場合がある）。

【００３７】

同様に、ＤＡＰは共有リソースであるため、ＤＡＰに余分な作業をさせると、その関連するすべてのクライアントのパフォーマンスを潜在的に損なう可能性がある。ＤＡＰ上の負荷を軽減するために、本発明のいくつかの実施形態では最適化技術を使用し、これによってＡＰは、いずれかのクライアントがＡＰに関連付けられている場合は、能動的なスキャン(active scanning)を実行せず、その関連付けられているクライアントが、必要に応じてこれらのオペレーションを実行する。ＡＰは、引き続き受動的なモニタリング活動を実行し、これは、そのパフォーマンスにわずかな影響しか及ぼさない。関連付けられているクライアントがない場合、ＡＰは待機状態であり、これらのモニタリングオペレーションを実行することができる。このアプローチによって、ＡＰの周囲の物理的なエリアの大半が、ＡＰのパフォーマンスを損なうことなく確実にモニタされる。

【００３８】

一実施形態では、ＤＣ、ＤＡＰ、およびＤＳ間での対話は、ＩＥＥＥ８０２．１ｘを介して発行されるＥＡＰ－ＴＬＳ証明書を使用して保護される。公認の認証当局（ＣＡ）は、ＤＣ、ＤＡＰ、およびＤＳに証明書を発行し、これらの証明書を使用して、これらのエンティティ間のすべての通信が相互に確実に認証される。一実施形態は、正当なユーザによる悪意ある行為を検出するための公知の技術を含む。

【００３９】

障害診断システム内で接続を断たれたワイヤレスクライアントを自動的に見つけ出す能力は、展開の中で問題のある領域、たとえば不良な受信可能範囲や高い干渉（ＲＦホールを見つけ出すこと）を事前対処的に割り出す上で、または障害を起こす可能性のあるＡＰを見つけ出す上で潜在的に有用である。本発明の実施形態では、接続を断たれたクライアントは、（認証の失敗などの他の何らかの理由で接続を断たれた場合とは対照的に）どのＡＰからもビーコンが聞こえない場合、自分はＲＦホールの中にいると判断する。接続を断たれたクライアントの大まかな位置を割り出すために（したがってＲＦホールを見つけ出すのを支援するために）、これらの実施形態は、図３を参照して説明するＤＩＡＬ（Ｄｏｕｂｌｅ Ｉｎｄｉｒｅｃｔｉｏｎ ｆｏｒ Ａｐｐｒｏｘｉｍａｔｉｎｇ Ｌｏｃａｔｉｏｎ）と呼ばれる技術を使用する。

【００４０】

クライアント３０２は、自分が接続を断たれていることにステップ３０４で気づくと、ＡＰとなるか、またはその場限りのネットワークを開始し、ステップ３０６でビーコンの送信を開始する。このクライアントの大まかな位置を割り出すために、付近の接続されているクライアント３０８は、ステップ３１０でこのクライアント３０２のビーコンを聞き、ステップ３１２でこれらのパケットの信号強度（ＲＳＳＩ）を記録する。ステップ３１４では、付近の接続されているクライアント３０８は、クライアント３０２が接続を断たれていることをＤＳ３１６に知らせ、収集したＲＳＳＩデータを送信する。次いでステップ３１８において、ＤＳ３１６は、ＤＩＡＬの第１のステップを実行して、接続されているクライアントの位置を割り出す。これは、非特許文献１および非特許文献２などの文献において知られている任意の位置特定技術を使用して行うことができる。ステップ３２０では、ＤＳ３１６は、「アンカーポイント」としての接続されているクライアントの位置と、接続を断たれたクライアントのＲＳＳＩデータを使用して、その大まかな位置を見積もる。このステップは、上記の参照文献に記載されているスキームなど、マシンの位置を割り出すために複数のクライアントからのＲＳＳＩ値を使用する任意のスキームを使用して、または他の任意の公知の方法によって実行されることが好ましい。接続されているクライアントを見つけ出すことは、結果として何らかの誤差を生じるため、ひいては接続を断たれたクライアントをこれらのアンカーポイントによって見つけ出すことによって、その誤差がさらに拡大する可能性がある。しかしこの誤差は約１０から１２メートルであることが経験的に示されており、これは、接続を断たれたクライアントの位置を見積もる上で許容可能である。

【００４１】
図４を参照して、本発明の一実施形態による、不正なＡＰを検出する方法について論じる。不正なＡＰとは、企業や大学のネットワーク内のイーサネット（登録商標）タップに接続されている無許可のＡＰであり、このようなＡＰは、結果としてセキュリティーホール、ならびに不要なＲＦおよびネットワークの負荷につながる場合がある。不正なＡＰは、企業の無線ＬＡＮにとって重大なセキュリティ問題とみなされている。クライアントおよび（可能な場合は）ＡＰを使用して、それらの周囲の環境をモニタすることによって、本発明の実施形態は、不正なＡＰを検出する。そのアプローチは、クライアントおよびＤＡＰに付近のアクセスポイントに関する情報を収集させて、それをＤＳへ送信させることである。ＤＳは、ＡＰ　Ｘに関する情報を受信すると、ＡＰ位置データベースをチェックし、Ｘが予想された位置およびチャネルにおける登録されたＡＰであることを裏付ける。このアプローチは、市販のＩＥＥＥ８０２．１１に準拠したハードウェアを使用して、不正なＡＰを検出する。これは、現在の展開の中で直面している一般的なケースの不正なＡＰの問題に対処する低コストのメカニズムとして機能するには十分であり、多くのネットワーク管理者にとって、主要な目的は、実験または利便性のために従業員によって不注意にインストールされるＡＰを検出することである。他の実施形態は、準拠していない(non-compliant)不正なアクセスポイントおよびクライアントの検出を実施することもできる。２つの企業が、隣接する無線ネットワークを有している場合、他の企業のアクセスポイントは、不正なＡＰとして検出されることが好ましい。この分類が許容できない場合、それぞれの企業のネットワーク管理者は、自分たちのＡＰ位置データベースを共有することができる。

【００４２】
それぞれのＤＣ４０２は、その付近にあるパケットを（非混合モードで）モニタし、検出するそれぞれのＡＰ４０４ごとに、＜ＭＡＣアドレス、ＳＳＩＤ、チャネル、ＲＳＳＩ＞の４タプル(4-tuple)をＤＳ４０６に送信する。基本的にこの４タプルは、特定の位置およびチャネルのＡＰを一意に識別する。この情報を得るために、ＤＣ４０２は、その周囲のすべてのＡＰ４０４のＭＡＣアドレスを割り出す。

【００４３】
ＤＣ４０２は、混合モードに切り替わってデータパケットを観察することによって、ＡＰ４０４のＭＡＣアドレスを得ることができる（これは、そのパケット内のＦｒｏｍＤＳおよびＴｏＤＳのビットを使用して、どのアドレスがそのＡＰに属するかを割り出すことができる）。しかし次のアプローチを使用して、同じ効果を達成することが好ましい。ＩＥＥＥ８０２．１１は、ステップ４０８において、すべてのＡＰが定期的な間隔でビーコンを送信することを要求するため、ＤＣ４０２は、ステップ４１０において、それらのビーコンを聴こうと試み、ステップ４１２において、聞こえるすべてのＡＰの中からＡＰ４０４のビーコンからのＭＡＣアドレスを得る。ＤＣ４０２は、そのチャネル上のビーコンを聞くだけでなく、重なるチャネルからのビーコンを聞くこともできることが示されており、この特性によって、不正なＡＰが検出される可能性が高まる。

【００４４】
不正なＡＰが検出から漏れることのないように、ＡＰと重なるいずれのチャネル上にもクライアントが存在しない場合でさえ、これらの実施形態は、ＩＥＥＥ８０２．１１プロトコルのＡｃｔｉｖｅ　Ｓｃａｎｎｉｎｇメカニズムを使用し、クライアント４０２（たとえば、ワイヤレスコンピュータまたはアクセスポイント上で作動する診断クライアント）は、どのＡＰ４０４が付近にあるかを知りたい場合、（８０２．１１ｂの）１１のチャネルのそれぞれに行き、ステップ４１４においてプローブ要求を送信する。クライアント４０２は、ステップ４１６において、それらのプローブ要求を聞くすべてのＡＰからプローブ応答が返信されるのを待ち、ＤＣは、ステップ４１８において、これらの応答からＡＰ４０４のＭＡＣアドレスを得る。ＩＥＥＥ８０２．１１に準拠しているすべてのＡＰは、このような要求に応答しなければならず、いくつかのチップセットでは、この機能を無効にするための制御は提供されない。ＡＰが自分に関連付けられているクライアントを有

さない場合にのみ、ＡＰの付近でのアクティブなスキャンがＡＰによって実行されるように、Ｂｕｓｙ　ＡＰ　Ｏｐｔｉｍｉｚａｔｉｏｎを使用することが好ましい。本発明の実施形態では、たとえば診断クライアントおよび診断アクセスポイントを介して通信する際のネットワーク管理者の要望に応じて、オンデマンドでＡｃｔｉｖｅ　Ｓｃａｎｎｉｎｇを実行することが好ましい。あるいはＡｃｔｉｖｅ　Ｓｃａｎｎｉｎｇは、定期的な基準で、またはネットワーク管理者によって設定された方針に従って、規則的に実行される。

【００４５】

クライアント４０２は、ＡＰの情報を収集すると、ステップ４２０において４タプルをＤＳ４０６へ送信する。次いでＤＳ４０６は、そのＡＰが不正なＡＰかどうかをステップ４２２において判定する。これについては、より詳しく後述する。

【００４６】

図５を参照すると、ＤＳは、ステップ５０２においてさまざまなクライアントからＡＰ用の情報を受信すると、ステップ５０４においてＤＩＡＬを使用して、図３を参照して上述したような方法でこれらのクライアントの位置およびそれらからのＡＰのＲＳＳＩ値に基づいてＡＰの大まかな位置を見積もる。ＤＳは、ステップ５０６において、４タプルが、そのＤＳのＡＰ位置データベース内の既知の正当なＡＰに対応しない場合、すなわちそのＭＡＣアドレスがデータベース内に存在しない場合、またはステップ５０８において、ＡＰが予想されている位置にない場合、あるいはステップ５１０において、そのＳＳＩＤが組織内の（１つまたは複数の）予想されているＳＳＩＤと一致しない場合、そのＡＰを不正なものとして分類する。いくつかの実施形態では、ＡＰのＳＳＩＤがＳＯＳ　ＳＳＩＤに相当する場合、このＡＰは、Ｃｌｉｅｎｔ　Ｃｏｎｄｕｉｔプロトコルの接続セットアップフェーズを実行している接続を断たれたクライアントに実質的に相当するとみなすことができるため、ＤＳはさらなる分析を省略する。チャネル情報は、若干異なる方法で使用される。前述のように、ＡＰは、あるチャネル上にある場合、重なるチャネル上で聞くことができる。したがってステップ５１２において、ＡＰが存在するものと予想されているチャネルと重ならないチャネル上でＡＰが報告された場合にのみ、ＡＰは不正なものとして分類される。ＡＰ上のチャネルが変更された場合、ＤＡＰは、ＤＳにそのＡＰ位置データベースを更新するよう要求することが好ましい（ＤＡＰとＤＳの間の通信が認証されていることを想起されたい。そのＡＰが従来のＡＰであるならば、ＡＰのチャネルが変更された場合、管理者はＡＰ位置データベースを更新することができる）。

【００４７】

不正なＡＰ　Ｒは、検出されるのを回避するためにＭＡＣアドレスを使用してなりすますこと、すなわち本物のＡＰ　Ｇに対応するＭＡＣアドレスを使用してパケットを送信することを試みる場合がある。しかし本発明の実施形態におけるＤＳは、それでもやはりＲを検出する。これは、ＲがＧとは異なる位置またはチャネルに存在するためである（もしもＲがＧと同じチャネルおよび位置にあるならば、Ｇがすぐに Ｒを検出する）。不正なＡＰがＳＳＩＤをそのビーコンに含めて送信していない場合でも、ＤＣは依然としてそのビーコンからＡＰのＭＡＣアドレスを得ることができるため、不正なＡＰは検出される点に留意されたい。あるいはこのような無許可のＡＰは、企業のＬＡＮ内でＳＳＩＤを送信しないＡＰを許可しないことによっても検出される。

【００４８】

本発明の実施形態では、無許可のＡＰは、Ｘの位置の付近で既存のＡＰＸになりすまし、組織内で有効なＳＳＩＤにビーコンを送信し、どのＤＣまたはＡＰにもそのビーコンが聞こえないチャネル上にとどまることによって、短時間にわたって検出されずにとどまる場合がある。しかし付近のクライアントがアクティブなスキャンを実行する際に、この不正なＡＰは検出されることになる。このような不正なＡＰを検出するために、ＤＣは、こうしたスキャンを５分ごとに実行することが好ましい。

【００４９】

図６に注目すると、一実装態様の１つの実施形態の詳細が示されている。基本的なアーキテクチャは、それぞれクライアント、アクセスポイント、およびサーバ上で作動するＤ

Ｃ、ＤＡＰ、およびＤＳのデーモンから構成される。このシステムは、たとえばＭＩＣＲＯＳＯＦＴ　ＷＩＮＤＯＷＳ（登録商標）オペレーティングシステム上で標準的な市販の８０２．１１ｂカードと共に実装することができる。ＤＳ上では、デーモンプロセスはＤＡＰからの情報を受け入れる。ＤＳは、正当なＡＰのリストをファイルまたはデータベースから読み取る。ＤＣまたはＤＡＰ上のコードの構造は、ユーザレベルのデーモン６０２ならびにカーネルレベルのドライバ６０４および６０６を含むことが好ましい。これらの要素は、ユーザレベルのデーモン６０２内では機能を達成できない場合、またはパフォーマンスのペナルティが高すぎる場合にのみ、カーネルドライバ６０４および６０６にコードが追加されるように構造化されている。

【００５０】

典型的なシステムでは、ＭＩＣＲＯＳＯＦＴ　ＷＩＮＤＯＷＳ（登録商標）オペレーティングシステムにおけるＮａｔｉｖｅ　ＷｉＦｉドライバなどの、ミニポートドライバ６０４および中間ドライバ（ＩＭドライバ）６０６という２つのカーネルドライバがある。ミニポートドライバ６０４は、ハードウェアと直接通信し、パケットの送信／受信やチャネルの設定などの基本的な機能を提供する。また関連付けや認証などの機能をＩＭドライバ６０６内で処理できるように、十分なインターフェースを提示する。ＩＭドライバ６０６は、現在のチャネル、送信レベル、電力管理モード、ＳＳＩＤなどのさまざまなパラメータに関する問合せを行うための（ｉｏｃｔｌｓを介して提示された）複数のインターフェースをサポートする。これらのパラメータを設定できることに加えて、ユーザレベルのコードが、アクティブなスキャンの要求、特定のＳＳＩＤへの関連付け、パケットの取り込みなどを行えるようにする。全般に、ユーザレベルのコードに対してかなりの程度の柔軟性および制御を提供する。

【００５１】

多くのオペレーションがＩＭドライバ６０６内に既に存在しているが、本発明の実施形態は、特定の機能を提示するための修正、および特定のプロトコルのパフォーマンスを改善するための修正を使用する。ミニポートドライバ６０４に対しては、特定のタイプのパケットをＩＭドライバ６０６に提示するように、最小限の変更を行うことが好ましい。ＩＭドライバ６０６内では、パケットヘッダおよびパケットの取り込み、受信したパケットからのＲＳＳＩ値の保存、ＡＰ情報の追跡把握、およびプロトコルの効率のためのカーネルイベントサポートという各サポートを追加することが好ましい。次いで、これらの修正についてさらに詳しく論じる。

【００５２】

パケットヘッダおよびパケットの取り込み：本発明の実施形態では、たとえば特定のＭＡＣアドレス、パケットのタイプ、（管理パケットおよびビーコンパケットなどの）パケットのサブタイプ等に基づくフィルタなど、特定のパケットまたはパケットヘッダのみが取り込まれるようにフィルタを設定することができる。

【００５３】

受信したパケットからのＲＳＳＩ値の保存：本発明の実施形態では、受信したすべてのパケットのＲＳＳＩ値を入手し、（ＭＡＣアドレス上にインデックスを付けられた）それぞれの近隣からのＲＳＳＩ値を追跡把握するＮｅｉｇｈｂｏｒＩｎｆｏテーブルと呼ばれるテーブルを保持する。指数関数的加重平均(exponentially weighted average)が、何らかの、たとえば０．２５の重み係数を与えられた新たな値と共に保持される。ＲＳＳＩ情報は、ＤＩＡＬを使用して接続を断たれたクライアントおよびＡＰの位置を見積もるために使用されることが好ましい。

【００５４】

ＡＰ情報の追跡把握：ＮｅｉｇｈｂｏｒＩｎｆｏテーブル内では、この実施形態は、パケットが特定のＭＡＣアドレスから聞こえたチャネル、（ビーコンからの）ＳＳＩＤ情報、およびデバイスがＡＰであるかまたはステーションであるかを追跡把握する。この情報は、不正なＡＰを検出するためにＤＡＰ／ＤＳへ送信されることが好ましい。

【００５５】

プロトコルの効率のためのカーネルイベントサポート：カーネルレベルのコードとユーザレベルのコードの間で共有されるイベントが追加されることが好ましい。カーネルは、「関心のある」イベントが発生した場合にこのイベントをトリガし、これによってプロトコルのいくつかは、ポーリングベースではなく、割り込み駆動型とすることができる。

【００５６】

さらに、上述の情報を入手および消去するために、複数のｉｏｃｔｌｓを追加することが好ましい。

【００５７】

本発明の実施形態では、診断デーモン６０２は、デバイス上で動作し、情報を収集し、前述のさまざまなメカニズム、たとえば不正なＡＰを検出するためのＡＰのＭＡＣアドレスの収集などを実施する。デバイスは、ＡＰである場合、ＤＳおよびＤＣと診断情報を通信し、単にＤＣである場合、その関連付けられたＡＰと通信して、診断情報を伝達する。ＤＣ上の診断デーモンは、定期的な間隔で、たとえば３０秒ごとにカーネル６０８から最新のＮｅｉｇｈｂｏｒＩｎｆｏテーブルを入手する。何らかの新しいノードが見つかった場合、または既存のデータが大幅に変更された場合（たとえばクライアントのＲＳＳＩ値が、２の係数を上回って変化した場合）、最新のＮｅｉｇｈｂｏｒＩｎｆｏテーブルがＤＡＰに送信される。ＤＡＰもまた、ＭＡＣアドレス上にインデックスを付けられた同様のテーブルを保持することが好ましい。しかしＤＡＰは、接続を断たれたクライアントおよびＡＰに関する情報をＤＳに送信するだけであり、さもなければ、ＤＳはシステム内のすべてのクライアントに対する更新を受け取ることになり、その拡張性が低下することになる。ＤＡＰは、ＡＰに関する新たなまたは変更された情報をＤＳに定期的に（たとえば３０秒ごとに）送信する。さらにＤＡＰは、接続を断たれたクライアントＤに関する何らかの保留中の情報を有している場合、接続を断たれたクライアントがタイムリーにサービスを受けられるように、その情報をすぐにＤＳに知らせる。ＤＣからＤＡＰへの、そしてＤＡＰからＤＳへのメッセージはすべて、ＸＭＬメッセージとして送信されることが好ましい。ＤＣからのサンプルメッセージフォーマットが、以下に示されている（タイムスタンプは削除されている）。

【００５８】

【表１】

```
<DiagPacket Type="RSSIInfo" TStamp="...">
    <Clients TStamp="...">
        <MacInfo MAC="00:40:96:27:dd:cc" RSSI="23"
            Channels ="19" SSID="" TStamp="..."/>
    </Clients>
    <Real-APs TStamp="...">
        <MacInfo MAC="00:20:a6:4c:c7:85" RSSI="89"
            Channels="12" SSID="UNIV_LAN" TStamp="..."/>
        <MacInfo MAC="00:20:a6:4c:bb:ad" RSSI="7"
            Channels="10" SSID="EXPER" TStamp="..."/>
    </Real-APs>
    <Disconnected-Clients TStamp="...">
        <MacInfo MAC="00:40:96:33:34:3e" RSSI="57"
            Channels="2048" SSID="SOS_764" TStamp="..."/>
    </Disconnected-Clients>
</DiagPacket>
```

【００５９】

サンプルメッセージに示されているように、ＤＣは、他の接続されているクライアント、ＡＰ、および接続を断たれたクライアントに関する情報を送信する。ＤＣは、それぞれのこのようなエンティティのクラスごとに、マシンのＭＡＣアドレスを、ＲＳＳＩ、ＳＳＩＤ、および特定のデバイスが聞こえたチャネルを示すチャネルビットマップと共に送信する。

【００６０】

本発明の原理を適用できる多くの可能な実施形態を考慮すれば、本明細書で図面を参照して説明した実施形態は、例示のみを意図しており、本発明の範囲を限定するものと解釈すべきではないことが認識できるはずである。たとえば本発明の趣旨から逸脱することなく、例示した実施形態の構成および細部を修正できることを当業者なら認識するであろう。本発明については、ソフトウェアモジュールやソフトウェアコンポーネントの観点から説明しているが、これらはハードウェアコンポーネントに同等に置き換えることができることを当業者なら認識するであろう。したがって本明細書に記載の発明は、添付の特許請求の範囲およびその均等物の範囲内に収まることができるすべての実施形態を考慮している。

【図面の簡単な説明】

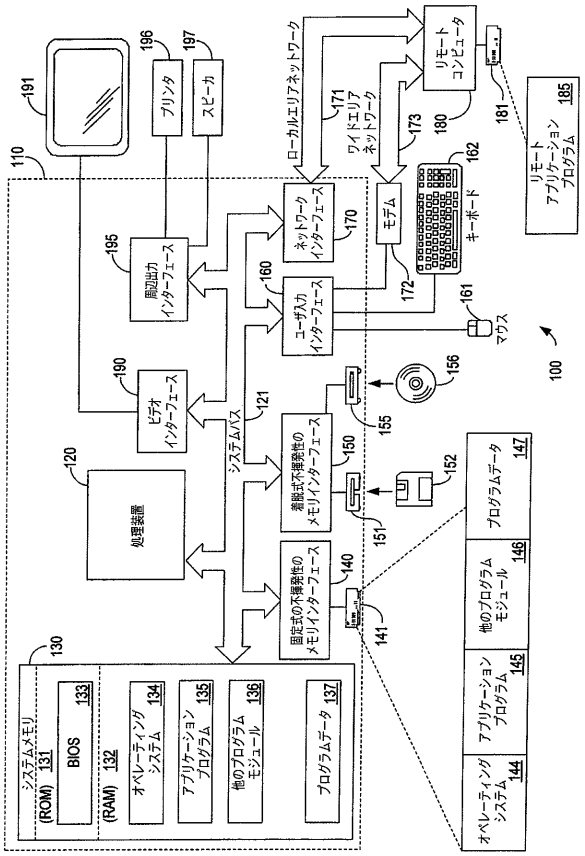
【００６１】

【図１】本発明の一実施形態に従って使用されるコンピューティングの典型的なアーキテクチャを示す概略図である。

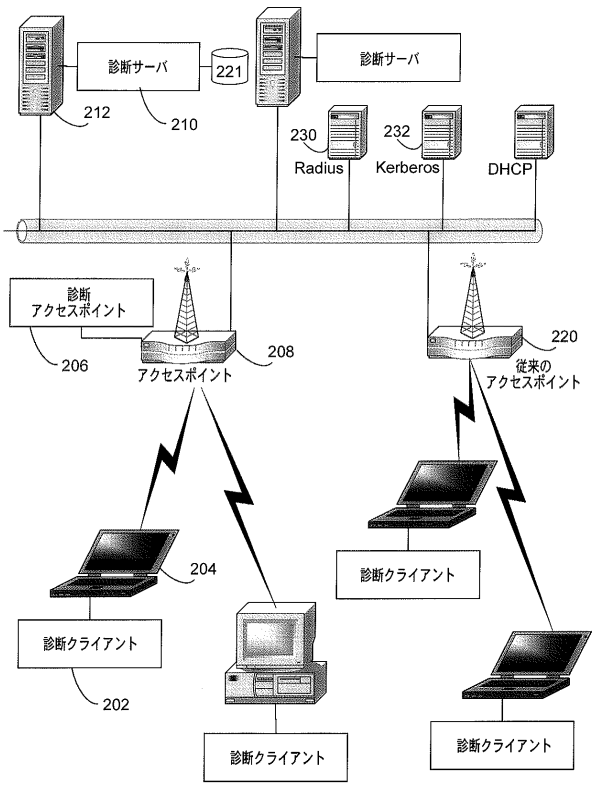
【図２】本発明の一実施形態による、接続を断たれたクライアントおよび不正なアクセスポイントを見つけ出すための典型的な無線ネットワークを示す図である。
【図３】本発明の一実施形態による、接続を断たれたクライアントを見つけ出すための方法を示す流れ図である。
【図４】本発明の一実施形態による、無線ネットワーク内のアクセスポイント上で協調して情報を得るための方法を示す流れ図である。
【図５】本発明の一実施形態による、アクセスポイントが不正であるかどうかを判定するための方法を示す流れ図である。
【図６】本発明の一実施形態による、接続を断たれたクライアントおよび不正なアクセスポイントを見つけ出すために使用されるソフトウェアコンポーネントを示す概略図である。

【符号の説明】
【００６２】
１２０　処理装置
１２１　システムバス
１３０　システムメモリ
１３４　オペレーティングシステム
１３５　アプリケーションプログラム
１３６　他のプログラムモジュール
１３７　プログラムデータ
１４０　固定式の不揮発性のメモリインターフェース
１４４　オペレーティングシステム
１４５　アプリケーションプログラム
１４６　他のプログラムモジュール
１４７　プログラムデータ
１５０　着脱式不揮発性のメモリインターフェース
１６０　ユーザ入力インターフェース
１６１　マウス
１６２　キーボード
１７０　ネットワークインターフェース
１７１　ローカルエリアネットワーク
１７２　モデム
１７３　ワイドエリアネットワーク
１８０　リモートコンピュータ
１８５　リモートアプリケーションプログラム
１９０　ビデオインターフェース
１９５　周辺出力インターフェース
１９６　プリンタ
１９７　スピーカ
２０２　診断クライアント
２０６　診断アクセスポイント
２０８　アクセスポイント
２１０　診断サーバ
２２０　従来のアクセスポイント
６０２　診断デーモン
６０４　診断ミニポートモジュール
６０６　診断ＩＭモジュール

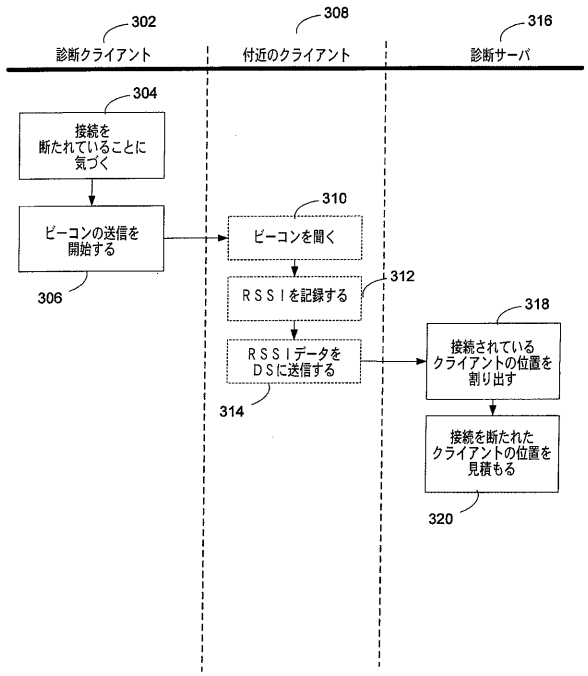
【図１】


ローカルエリアネットワーク
ワイドエリアネットワーク
リモートコンピュータ
リモートアプリケーションプログラム
プリンタ
スピーカ
ネットワークインターフェース
モデム
キーボード
周辺出力インターフェース
ユーザ入力インターフェース
マウス
ビデオインターフェース
システムバス
処理装置
着脱式不揮発性のメモリインターフェース
固定式の不揮発性のメモリインターフェース
システムメモリ
(ROM)
BIOS
(RAM)
オペレーティングシステム
アプリケーションプログラム
他のプログラムモジュール
プログラムデータ
プログラムデータ
他のプログラムモジュール
アプリケーションプログラム
オペレーティングシステム

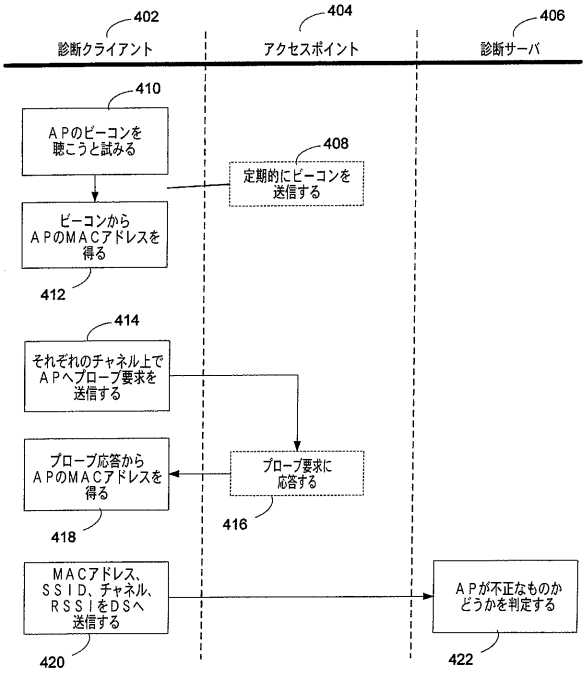
【図２】


診断サーバ
診断サーバ
Radius
Kerberos
DHCP
診断アクセスポイント
アクセスポイント
従来のアクセスポイント
診断クライアント
診断クライアント
診断クライアント
診断クライアント

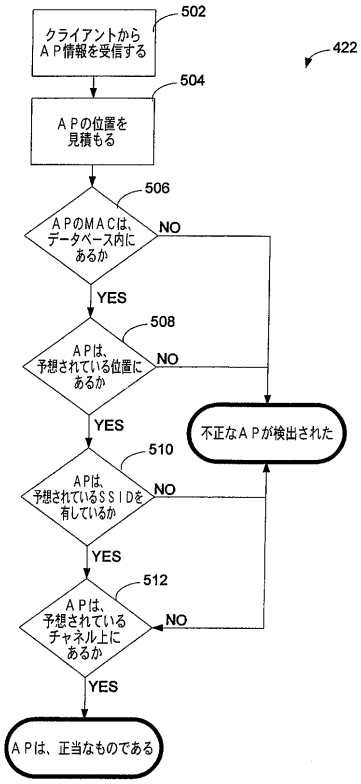
【図３】


診断クライアント
付近のクライアント
診断サーバ
接続を断たれていることに気づく
ビーコンの送信を開始する
ビーコンを聞く
RSSIを記録する
RSSIデータをDSに送信する
接続されているクライアントの位置を割り出す
接続を断たれたクライアントの位置を見積もる

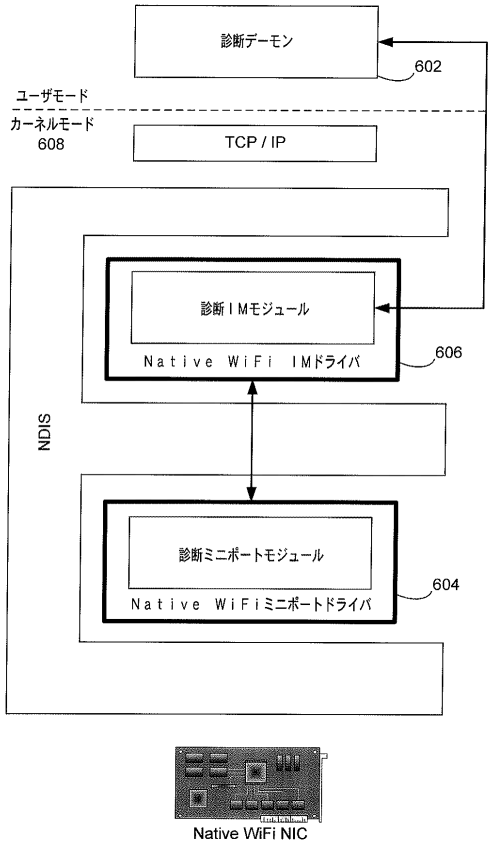
【図４】


診断クライアント
アクセスポイント
診断サーバ
APのビーコンを聴こうと試みる
定期的にビーコンを送信する
ビーコンからAPのMACアドレスを得る
それぞれのチャネル上でAPへプローブ要求を送信する
プローブ要求に応答する
プローブ応答からAPのMACアドレスを得る
MACアドレス、SSID、チャネル、RSSIをDSへ送信する
APが不正なものかどうかを判定する

【図５】


422
502
クライアントから
ＡＰ情報を受信する
504
ＡＰの位置を
見積もる
506
ＡＰのＭＡＣは、
データベース内に
あるか
NO
YES
508
ＡＰは、
予想されている位置に
あるか
NO
YES
不正なＡＰが検出された
510
ＡＰは、
予想されているＳＳＩＤを
有しているか
NO
YES
512
ＡＰは、
予想されている
チャネル上に
あるか
NO
YES
ＡＰは、正当なものである

【図６】


診断デーモン
602
ユーザモード
カーネルモード
608
TCP / IP
診断ＩＭモジュール
Ｎａｔｉｖｅ ＷｉＦｉ ＩＭドライバ
606
NDIS
診断ミニポートモジュール
Ｎａｔｉｖｅ ＷｉＦｉミニポートドライバ
604
Native WiFi NIC

フロントページの続き

(72)発明者　リリー　キュー
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内
(72)発明者　パランビア　バウル
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内
(72)発明者　ランビール　チャンドラ
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内

Ｆターム(参考) 5K033 AA06　AA08　DA17　DB20　EA05
5K067 AA33　BB21　EE02　EE10　EE16　HH22　JJ51　LL01　LL05

【外国語明細書】
2007089006000001.pdf