(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4295122号
(P4295122)
(45)発行日　平成21年7月15日(2009.7.15)　(24)登録日　平成21年4月17日(2009.4.17)

(51)Int.Cl.　　F I
H04W 24/00 (2009.01)　　H04L 12/28　300M
H04W 84/12 (2009.01)

請求項の数 36　(全 25 頁)

(21)出願番号	特願2003-585339 (P2003-585339)
(86)(22)出願日	平成15年4月8日 (2003.4.8)
(65)公表番号	特表2005-522935 (P2005-522935A)
(43)公表日	平成17年7月28日 (2005.7.28)
(86)国際出願番号	PCT/US2003/010727
(87)国際公開番号	WO2003/088547
(87)国際公開日	平成15年10月23日 (2003.10.23)
審査請求日	平成18年4月7日 (2006.4.7)
(31)優先権主張番号	60/371,084
(32)優先日	平成14年4月8日 (2002.4.8)
(33)優先権主張国	米国(US)

(73)特許権者　504324981
エアマグネット，　インコーポレイテッド
アメリカ合衆国　カリフォルニア　９４０８９，　サニーベール，　スイート　２００，　ロス　ドライブ　８９４
(74)代理人　100078282
弁理士　山本　秀策
(74)代理人　100062409
弁理士　安村　高明
(74)代理人　100113413
弁理士　森下　夏樹
(72)発明者　クアン，　チアーチー
アメリカ合衆国　カリフォルニア　９４０２４，　ロス　アルトス，　ロックヘブン　８９０

最終頁に続く

(54)【発明の名称】ローカルエリアネットワークのモニタ

(57)【特許請求の範囲】
【請求項１】
無線ローカルエリアネットワーク（ＷＬＡＮ）をモニタする方法であって、
該方法は、
該ＷＬＡＮ内に配置された検出器を用いて、該ＷＬＡＮ内の１つ以上のステーションとアクセスポイント（ＡＰ）との間で交換される伝送を受信することと、
該受信した伝送に基づいてデータベースを編集することであって、該データベースを編集することは、１つ以上のノード要素を生成することを含み、該生成されたノード要素は、受信した伝送と該ＷＬＡＮ内のノードとを関連付けるものであり、該ノード要素は、該ＷＬＡＮ内のノードを識別するデータと、該ノードに送信される該受信した伝送の数を追跡する第１の組の統計と、該ノードから送出される該受信した伝送の数を追跡する第２の組の統計とを含む、ことと、
該受信した伝送を分析することにより、ステーションの状態を決定することと、
該編集されたデータベースと該ステーションの該決定された状態とを用いて、該ステーションの接続上の問題点を診断することと
を含む、方法。
【請求項２】
前記受信することは、
前記ステーションの媒体アクセス制御（ＭＡＣ）アドレスを取得することと、
前記検出器を用いて伝送を受信することであって、該伝送は、ソースアドレスと宛先ア

ドレスとを含む、ことと、
該伝送の該ソースアドレスまたは該宛先アドレスが該ステーションの該ＭＡＣアドレスであるか否かを決定することと
を含む、請求項１に記載の方法。
【請求項３】
前記受信することは、
前記検出器を用いて、前記無線ローカルエリアネットワークで用いられる複数のチャネルを走査すること
を含み、
前記ステーションは、該複数のチャネルの走査中に伝送が受信されなかった場合にリブートするように構成されている、請求項１または２に記載の方法。
【請求項４】
前記ステーションは、リブートされた後に第１のチャネルで動作し、
該第１のチャネルは、前記無線ローカルエリアネットワークで用いられる前記複数のチャネルのうちの１つであり、
前記方法は、該無線ローカルエリアネットワークで用いられる該複数のチャネルのうちの他のチャネルよりも長い期間の間、前記検出器を用いて該第１のチャネルを走査することをさらに含む、請求項３に記載の方法。
【請求項５】
前記ノード要素は、前記ＷＬＡＮ内のステーションまたはＡＰに関連付けられており、
編集することは、前記受信した伝送に基づいてセッション要素を前記データベース内に生成することであって、セッション要素は、２つのノード要素の間で確立されたセッションに関連付けられている、ことと、
該受信した伝送に基づいてチャネル要素を該データベース内に生成することであって、チャネル要素は、該ＷＬＡＮ内のチャネルに関連付けられている、ことと
を含む、請求項１から４のいずれか一項に記載の方法。
【請求項６】
セッション要素は、２つのノード要素の間で第１の方向の伝送の数を追跡する第１の組の統計と、２つのノード要素の間で第２の方向の伝送の数を追跡する第２の組の統計とを含み、
チャネル要素は、前記チャネル内の伝送の数を追跡する一組の統計を含む、請求項５に記載の方法。
【請求項７】
ノード要素を生成することは、
前記ＷＬＡＮ内のノードからビーコンフレームを受信することと、
前記ビーコンフレームのソースフィールドと宛先フィールドとから該ノードのＭＡＣアドレスを決定することと、
前記データベース内のＡＰとして該ノードを識別することと、
該ノードに対応するノード要素が該データベース内に存在するか否かを決定することと、
該ノード要素が存在しない場合には、該ノードに対応する新たなノード要素を該データベースに追加し、該ノード要素の前記第２の組の統計を更新することと、
該ノード要素が存在する場合には、該ノード要素の該第２の組の統計を更新することと
を含む、請求項６に記載の方法。
【請求項８】
前記ビーコンフレームが受信されたチャネルを決定することと、
該チャネルに対応するチャネル要素が前記データ内に存在するか否かを決定することと、
該チャネル要素が存在しない場合には、該チャネルに対応する新たなチャネル要素を前記データベースに追加し、該新たなチャネル要素の前記一組の統計を更新することと、

該チャネル要素が存在する場合には、該チャネル要素の該一組の統計を更新することとをさらに含む、請求項７に記載の方法。

【請求項９】

ノード要素を生成することは、

前記ＷＬＡＮ内のノードからプローブ要求を受信することと、

前記受信したプローブ要求から該ノードのサービス設定識別アドレス（ＳＳＩＤ）を決定することと、

該ノードをステーションとして識別することと、

該ノードに対応するノード要素が前記データベース内に存在するか否かを決定することと、

該ノード要素が存在しない場合には、該ノードに対応する新たなノード要素を該データベースに追加し、該ノード要素の前記第２の組の統計を更新することと、

該ノード要素が存在する場合には、該ノード要素の該第２の組の統計を更新することとを含む、請求項６から８のいずれか一項に記載の方法。

【請求項１０】

前記受信したプローブ要求から宛先ノードを決定することと、

該受信したプローブ要求から該宛先ノードのＳＳＩＤを決定することと、

該宛先ノードをＡＰとして識別することと、

該宛先ノードに対応するノード要素が前記データベース内に存在するか否かを決定することと、

該ノード要素が存在しない場合には、該宛先ノードに対応する新たなノード要素を該データベースに追加し、該ノード要素の前記第１の組の統計を更新することと、

該ノード要素が存在する場合には、該ノード要素の該第１の組の統計を更新することとをさらに含む、請求項９に記載の方法。

【請求項１１】

ノード要素を生成することは、

前記ＷＬＡＮ内のノードからデータフレームを受信することと、

該データフレーム内のヘッダから該ノードを識別することと、

該ノードに対応するノード要素が前記データベース内に存在するかどうかを判定することと、

該ノード要素が存在しない場合、該ノードに対応する新たなノード要素を前記データベースに追加し、該ノード要素の前記第２の組の統計を更新することと、

前記ノード要素が存在する場合、該ノード要素の該第２の組の統計を更新することとを含む、請求項６から１０のいずれか一項に記載の方法。

【請求項１２】

前記ノードを識別することは、

前記ヘッダにおいて該ノードが配信システムとして示されている場合には、該ノードをＡＰとして識別することと、

該ヘッダにおいて該ノードが配信システムとして示されていない場合には、該ノードをステーションとして識別することと

を含む、請求項１１に記載の方法。

【請求項１３】

前記受信したデータフレームから宛先ノードを決定することと、

前記ヘッダから該宛先ノードを識別することと、

該宛先ノードに対応するノード要素が前記データベース内に存在するか否かを決定することと、

該ノード要素が存在しない場合には、該宛先ノードに対応する新たなノード要素を該データベースに追加し、該ノード要素の前記第１の組の統計を更新することと、

該ノード要素が存在する場合には、該ノード要素の該第１の組の統計を更新することとをさらに含む、請求項１１または１２に記載の方法。

【請求項１４】
前記宛先ノードを識別することは、
前記ヘッダにおいて該宛先ノードが配信システムとして示されている場合には、該宛先ノードをＡＰとして識別することと、
該ヘッダにおいて該宛先ノードが配信システムとして示されていない場合には、該宛先ノードをステーションとして識別することと
を含む、請求項１３に記載の方法。
【請求項１５】
セッション要素を生成することは、
前記ノードと前記宛先ノードとの間のセッションを識別することと、
該識別されたセッションに対応するセッション要素が前記データベース内に存在するか否かを決定することと、
該セッション要素が存在しない場合には、該識別されたセッションに対応する新たなセッション要素を該データベースに追加し、該新たなセッション要素の前記第１／第２の組の統計を更新することと、
該セッション要素が存在する場合には、該セッション要素の該第１／第２の組の統計を更新することと
を含む、請求項１３または１４に記載の方法。
【請求項１６】
ある期間において、伝送が受信され、前記データベースが編集される、請求項１から１５のいずれか一項に記載の方法。
【請求項１７】
分析することは、
受信した伝送を調べることと、
該受信した伝送に関連付けられた前記ステーションの表示状態を決定することと
を含む、請求項１から１６のいずれか一項に記載の方法。
【請求項１８】
前記ステーションの第１の状態は、第１の組の伝送に関連付けられており、
決定することは、
前記受信した伝送が該第１の組の伝送のうちの１つであるか否かを決定することと、
該受信した伝送が該第１の組の伝送のうちの１つであると決定された場合には、該ステーションの状態を該第１の状態として識別することと
を含む、請求項１７に記載の方法。
【請求項１９】
前記ステーションの第２の状態は、第２の組の伝送に関連付けられており、
決定することは、
前記受信した伝送が該第２の組の伝送のうちの１つであるか否かを決定することと、
該受信した伝送が該第２の組の伝送のうちの１つであると決定された場合には、該ステーションの状態を該第２の状態として識別することと
を含む、請求項１８に記載の方法。
【請求項２０】
前記ステーションの第３の状態は、第３の組の伝送に関連付けられており、
決定することは、
前記受信した伝送が該第３の組の伝送のうちの１つであるか否かを決定することと、
該受信した伝送が該第３の組の伝送のうちの１つであると決定された場合には、該ステーションの状態を該第３の状態として識別することと
を含む、請求項１９に記載の方法。
【請求項２１】
前記第１の状態は、前記ステーションが認証されていない、または、該ステーションが前記アクセスポイントに関連付けられていないことを示し、

前記第２の状態は、該ステーションが認証されているが、該ステーションが該アクセスポイントに関連付けられていないことを示し、
前記第３の状態は、該ステーションが認証されており、かつ、該ステーションが該アクセスポイントに関連付けられていることを示す、請求項２０に記載の方法。
【請求項２２】
前記ステーションと前記アクセスポイントとの間で交換される前記伝送は、ローカルエリアネットワークプロトコル上の拡張可能認証（ＥＡＰＯＬ）プロトコルに準拠する、請求項１から２１のいずれか一項に記載の方法。
【請求項２３】
分析することは、
伝送のリストを検出器上に表示することであって、該リストは、前記ステーションと前記アクセスポイントとの間で潜在的に交換される異なるタイプの伝送を含む、ことと、
受信したメッセージが該伝送のリスト内の複数のタイプの伝送のうちの１つに対応する場合には、該受信したメッセージに対応するタイプの伝送が受信されたことを該伝送のリスト上に示すことと
を含む、請求項１から２２のいずれか一項に記載の方法。
【請求項２４】
前記複数のタイプの伝送は、ローカルエリアネットワークプロトコル上の拡張可能認証（ＥＡＰＯＬ）プロトコルに従って、認証処理の間に前記ステーションと前記アクセスポイントとの間で交換される伝送を含む、請求項２３に記載の方法。
【請求項２５】
診断することは、
前記編集されたデータベース内のＳＳＩＤに対してクライアントステーションＳＳＩＤをマッチさせることによって、ミスマッチのＳＳＩＤ問題を検出することと、
ヌルのＳＳＩＤに対してクライアントステーションＳＳＩＤをマッチさせることによって、ワイルドカードＳＳＩＤ問題を検出することと、
各チャネルでステーションにより送信されるトラフィックを追跡することによって、ミスマッチのチャネル問題を検出することと、
前記ＡＰの可能出力属性に対してステーションの可能出力属性をマッチさせることによって、ミスマッチの速度、プライバシ、ネットワークタイプ、またはプリアンブル問題を検出することと、
認証応答パケットを追跡することによって、認証失敗問題を検出することと、
関連応答パケットを追跡することによって、関連失敗問題を検出することと、
パケットがステーションから伝送されない場合に、機器故障問題を検出することと、
前記編集されたデータベース内のＡＰ信号強度をチェックすることによって、弱いＡＰ信号問題を検出することと、
ステーションが関連状態に達し、該ステーションがデータパケットを伝送したが、関連付けられたＡＰが該ステーションにパケットを返送しない場合に、ミスマッチのワイヤード同等プライバシ（ＷＥＰ）キー問題を検出することと、または、
ステーションとＡＰとの間で成功したデータ交換を検出することによって上位層プロトコル問題と
を含む、請求項１から２４のいずれか一項に記載の方法。
【請求項２６】
無線ローカルエリアネットワーク（ＷＬＡＮ）をモニタするシステムであって、
該ＷＬＡＮ内の１つ以上のステーションとアクセスポイント（ＡＰ）との間で交換される伝送を受信する検出器と、
該受信した伝送に基づいて編集されたデータベースと
を備え、
該データベースは、該受信した伝送に基づいて生成された１つ以上のノード要素を含み、該生成されたノード要素は、該受信した伝送と該ＷＬＡＮ内のノードとを関連付けるも

のであり、
該ノード要素は、該ＷＬＡＮ内の該ノードを識別するデータと、該ノードに送信される受信した伝送の数を追跡する第１の組の統計と、該ノードから送出される受信した伝送の数を追跡する第２の組の統計とを含み、
該検出器は、該編集されたデータベースと該ステーションの該決定された状態とを用いて、該ＷＬＡＮ内の該ステーションの接続上の問題点を診断する、システム。
【請求項２７】
前記データベースは、
前記ＷＬＡＮ内のステーションまたはＡＰに関連付けられたノード要素と、
２つのノード要素の間で確立されるセッションに関連付けられたセッション要素と、
該ＷＬＡＮ内のチャネルに関連付けられたチャネル要素と
を備える、請求項２６に記載のシステム。
【請求項２８】
前記ＷＬＡＮ内のノードからビーコンフレームを受信することと、
該ビーコンフレームのソースフィールドと宛先フィールドとから該ノードのＭＡＣアドレスを決定することと、
前記データベース内のＡＰとして該ノードを識別することと、
該ノードに対応するノード要素が該データベース内に存在するか否かを決定することと、
該ノード要素が存在しない場合には、該ノードに対応する新たなノード要素を該データベースに追加することと
によってノード要素が生成される、請求項２７に記載のシステム。
【請求項２９】
前記ＷＬＡＮ内のノードからプローブ要求を受信することと、
該受信したプローブ要求から該ノードのサービス設定識別アドレス（ＳＳＩＤ）を決定することと、
該ノードをステーションとして識別することと、
該ノードに対応するノード要素が前記データベース内に存在するか否かを決定することと、
該ノード要素が存在しない場合には、該ノードに対応する新たなノード要素を該データベースに追加することと、
該受信したプローブ要求から宛先ノードを決定することと、
該受信したプローブ要求から該宛先ノードのＳＳＩＤを決定することと、
該宛先ノードをＡＰとして識別することと、
該宛先ノードに対応するノード要素が該データベース内に存在するか否かを決定することと、
該ノード要素が存在しない場合には、該宛先ノードに対応する新たなノード要素を該データベースに追加することと
によってノード要素が生成される、請求項２７または２８に記載のシステム。
【請求項３０】
前記ＷＬＡＮ内のノードからデータフレームを受信することと、
該データフレーム内のヘッダから該ノードを識別することと、
該ノードに対応するノード要素が前記データベース内に存在するか否かを決定することと、
該ノード要素が存在しない場合には、該ノードに対応する新たなノード要素を該データベースに追加することと、
該受信したデータフレームから宛先ノードを決定することと、
該ヘッダから該宛先ノードを識別することと、
該宛先ノードに対応するノード要素が該データベース内に存在するか否かを決定することと、

該ノード要素が存在しない場合には、該宛先ノードに対応する新たなノード要素を該データベースに追加することと
によってノード要素が生成される、請求項２７、２８または２９のいずれか一項に記載のシステム。
【請求項３１】
前記ノードと前記宛先ノードとの間のセッションを識別することと、
該識別されたセッションに対応するセッション要素が前記データベース内に存在するか否かを決定することと、
該セッション要素が存在しない場合には、該識別されたセッションに対応する新たなセッション要素を該データベースに追加することと
によってセッション要素が生成される、請求項２７から３０のいずれか一項に記載のシステム。
【請求項３２】
前記ステーションの状態は、
受信した伝送を調べることと、
該受信した伝送と関連付けられた前記ステーションの表示状態を決定することと
によって決定される、請求項２６から３１のいずれか一項に記載のシステム。
【請求項３３】
前記ステーションの第１の状態は、第１の組の伝送に関連付けられており、該ステーションの第２の状態は、第２の組の伝送に関連付けられており、該ステーションの第３の状態は、第３の組の伝送に関連付けられており、
決定することは、
前記受信した伝送が該第１の組の伝送のうちの１つであるか否かを決定することと、
該受信した伝送が該第１の組の伝送のうちの１つであると決定された場合には、該ステーションの状態を該第１の状態として識別することと、
該受信した伝送が該第２の組の伝送のうちの１つであるか否かを決定することと、
該受信した伝送が該第２の組の伝送のうちの１つであると決定された場合には、該ステーションの状態を該第２の状態として識別することと、
該受信した伝送が該第３の組の伝送のうちの１つであるか否かを決定することと、
該受信した伝送が該第３の組の伝送のうちの１つであると決定された場合には、該ステーションの状態を該第３の状態として識別することと
を含む、請求項３２に記載のシステム。
【請求項３４】
前記第１の状態は、前記ステーションが認証されていない、または、該ステーションが前記アクセスポイントに関連付けられていないことを示し、
前記第２の状態は、該ステーションが認証されているが、該ステーションが該アクセスポイントに関連付けられていないことを示し、
前記第３の状態は、該ステーションが認証されており、かつ、該ステーションが該アクセスポイントに関連付けられていることを示す、請求項３３に記載の方法。
【請求項３５】
前記編集されたデータベース内のＳＳＩＤに対してクライアントステーションＳＳＩＤをマッチさせることによって、ミスマッチのＳＳＩＤ問題を検出することと、
ヌルのＳＳＩＤに対してクライアントステーションＳＳＩＤをマッチさせることによって、ワイルドカードＳＳＩＤ問題を検出することと、
各チャネルでステーションによって送信されるトラフィックを追跡することによって、ミスマッチのチャネル問題を検出することと、
前記ＡＰの可能出力属性に対してステーションの可能出力属性をマッチさせることによって、ミスマッチの速度、プライバシ、ネットワークタイプ、またはプリアンブル問題を検出することと、
認証応答パケットを追跡することによって、認証失敗問題を検出することと、

関連応答パケットを追跡することによって、関連失敗問題を検出することと、
パケットがステーションから伝送されない場合に、機器故障問題を検出することと、
該編集されたデータベース内のＡＰ信号強度をチェックすることによって、弱いＡＰ信号問題を検出することと、
ステーションが関連状態に達し、該ステーションがデータパケットを伝送したが、関連付けられたＡＰが該ステーションにパケットを返送しない場合に、ミスマッチのワイヤード同等プライバシ（ＷＥＰ）キー問題を検出することと、または、
ステーションとＡＰとの間で成功したデータ交換を検出することによって、上位層プロトコル問題と
によって、該編集されたデータベースと該ステーションの決定された状態とを用いて、該ＷＬＡＮ内のステーションの接続上の問題点が診断される、請求項２６から３４のいずれか一項に記載のシステム。

【請求項３６】
無線ローカルエリアネットワーク（ＷＬＡＮ）をモニタするためのコンピュータ実行可能なコードを含むコンピュータ読み取り可能な格納媒体であって、該コードがコンピュータ上で実行されると、該コードが該コンピュータに請求項１から２５のいずれか一項に記載の方法を実行させる、コンピュータ読み取り可能な格納媒体。

【発明の詳細な説明】
【技術分野】
【０００１】
関連出願に関する記載
本願は、「ローカルエリアネットワークのモニタ」という名称のすでに出願済みの米国仮出願第６０／３７１，０８４号（２００２年４月８日出願）の利益を請求するものであり、上記出願内容全体は本願明細書で参照により援用される。

【０００２】
背景
１．技術分野
本発明は一般に無線ローカルエリアネットワークに関する。特に、本発明は無線ローカルエリアネットワークのモニタに関する。

【背景技術】
【０００３】
２．関連技術についての説明
コンピュータは従来有線のローカルエリアネットワーク（“ＬＡＮ”）を通じて相互通信を行ってきた。しかし、ラップトップ型コンピュータ、個人用情報機器、等の移動用コンピュータに対する需要の増加と共に、無線信号、赤外線信号、等を利用する無線媒体を介する伝送信号によりコンピュータの相互通信を行う方法として、無線ローカルエリアネットワーク（“ＷＬＡＮ”）が発達した。

【０００４】
ＩＥＥＥ８０２．１１規格は、ＷＬＡＮ間の相互運用性並びに有線ＬＡＮとの相互運用性の促進を意図して、ＷＬＡＮ用の国際標準規格として開発されたものである。一般に、ＩＥＥＥ８０２．１１規格は、無線媒体を介するデータのトランスポートを可能にしながら、ＩＥＥＥ８０２有線ＬＡＮと同じインタフェースをユーザに提供するために設計されたものである。

【０００５】
ＩＥＥＥ８０２．１１規格によれば、アクセスポイントからサービスを受ける前に、ステーションの認証が行われ、ステーションはＷＬＡＮ内のアクセスポイントと関連づけられる。上記認証処理と関連づけ処理とが行われている間、ステーションは３つの段階すなわち３状態（状態１、状態２、状態３）の中を進むことになる。状態１では、ステーションは認証も関連づけも受けない。状態２では、ステーションは認証は受けるが関連づけは受けない。状態３では、ステーションは認証と関連づけとを受ける。アクセスポイントか

らサービスを受けるのが困難であるなどの接続上の問題がステーションに生じた場合、接続上の問題の原因を診断することが困難になる場合がある。

【発明の開示】

【課題を解決するための手段】

【０００６】

概要

１つの実施形態例では、ＷＬＡＮに配置された検出器を用いて、ＷＬＡＮ内の１または２以上のステーションとアクセスポイント（ＡＰ）間で交換される伝送信号の受信により無線ローカルエリアネットワーク（ＷＬＡＮ）のモニタが行われる。受信した伝送信号に基づいてデータベースが編集される。上記受信済み伝送信号を分析してステーション状態が判定される。上記編集済みデータベースと、上記判定済みステーション状態とを利用してステーションの接続問題が診断される。

【０００７】

添付図面と関連して行う以下の詳細な説明を参照することにより本発明を最も良く理解することができる。添付図面では、同様の部分は同じ参照番号により参照することができる。

【０００８】

詳細な説明

本発明についてのさらに完全な理解を供するために、以下の記載によって多数の具体的な構成、パラメータ、実例などの特定の詳細事項が提示される。しかし、このような記載は、本発明の範囲に対する限定を意図するものではなく、実施形態例についてより良く説明することを意図するものであると認識すべきである。

【０００９】

図１と関連して、例示の開放型システム間相互接続（ＯＳＩ）の７つの階層モデルを示すが、この図はこれら階層モデルのそれぞれの機能に応じて層に分けられるネットワークシステムの抽象的モデルを表すものである。特に、これら７つの層には、層１に対応する物理層と、層２に対応するデータリンク層と、層３に対応するネットワーク層と、層４に対応するトランスポート層と、層５に対応するセッション層と、層６に対応するプレゼンテーション層と、層７に対応するアプリケーション層とが含まれる。ＯＳＩモデル内の個々の層は、層のすぐ上の層または層のすぐ下の層としか直接の通信は行わない。

【００１０】

図１に描かれているように、異なるコンピュータ同士は物理層のみにおいて直接通信を行うことができる。しかし、異なるコンピュータ同士が共通のプロトコルを利用して同じ層で効果的に通信を行うことが可能である。例えば、１つのコンピュータは、フレームが物理層に達するまで、アプリケーション層からこの層の下に在る個々の層を通り抜けてそのフレームを伝播することにより、アプリケーション層で別のコンピュータと通信を行うことが可能である。次いで、別のコンピュータの物理層へフレームを伝送し、このフレームが当該コンピュータのアプリケーション層に達するまで、物理層の上に在る個々の層を通り抜けてフレームを伝播することが可能である。

【００１１】

無線ローカルエリアネットワーク（“ＷＬＡＮ”）を対象とするＩＥＥＥ８０２．１１規格は、上述のように、ＯＳＩの７つの階層モデルの層２に対応するデータリンク層で機能するものである。ＩＥＥＥ８０２．１１がＯＳＩの７つの階層モデルの層２で機能することに起因して、層３およびその上に在る層は、ＩＥＥＥ８０２有線ＬＡＮに関して使用される同じプロトコルに従って機能することが可能となる。さらに、層３およびその上に在る層は、層２およびこの層の下に在る層で実際にデータをトランスポートしているネットワークについて意識せずにすますことができる。したがって、層３およびその上に在る層は、ＩＥＥＥ８０２の有線ＬＡＮとＩＥＥＥ８０２．１１のＷＬＡＮにおいて全く同様に機能することができる。さらに、有線ＬＡＮまたはＷＬＡＮのいずれを使用するかに関係なくユーザに対して同じインタフェースを提供することができる。

【００１２】
図２と関連して、ＩＥＥＥ８０２．１１規格に準拠してＷＬＡＮを形成する拡張サービス設定の１例が、３つの基本サービス設定（“ＢＳＳ”）を含む形で描かれている。個々のＢＳＳはアクセスポイント（“ＡＰ”）と１または２以上のステーションとを備える。ステーションとは、ＷＬＡＮとの接続に利用可能な構成要素であり、移動局、携帯局、固定局、等であってもよく、ネットワークアダプタまたはネットワークインタフェースカードと呼ばれる場合もある。例えば、ステーションはラップトップコンピュータ、個人用情報機器、等であってもよい。さらに、ステーションは、認証、認証解除（ｄｅａｕｔｈｅｎｔｉｃａｔｉｏｎ）、プライバシ、データの配信、等のステーションによるサービスをサポートするものであってもよい。

【００１３】
個々のステーションは、ＷＬＡＮ送信機と受信機間での無線信号や赤外線信号による伝送手段のようなエアリンクを通じてＡＰと直接通信を行うことが可能である。個々のＡＰは上述のようなステーションサービスのサポートが可能であり、さらに、関連付け、関連付け解除（ｄｉｓａｓｓｏｃｉａｔｉｏｎ）、配信、統合化、等の配信サービスをサポートすることが可能である。したがって、ＡＰは、そのＢＳＳ内の１または２以上のステーションと、ＷＬＡＮの基幹を形成する、一般に配信システムと呼ばれる媒体を通じて別のＡＰとの通信を行うことが可能となる。この配信システムは無線接続と有線接続の双方を含むものであってもよい。

【００１４】
図２と図３とを参照すると、現在のＩＥＥＥ８０２．１１規格の下では、個々のステーションは、ＢＳＳの一部分となるために、かつ、ＡＰからサービスを受けるために、ＡＰに対して認証され、かつ、ＡＰとの関連付けを行う必要がある。したがって、図３を参照すると、ステーションは、認証も、ＡＰとの関連づけも受けない状態１で作動を開始する。状態１で、ステーションは、ステーションによるＡＰ位置の検出や、ＡＰの認証などを可能とするような限られた数のフレームタイプを使用することができるにすぎない。

【００１５】
ＡＰに対する認証に成功した場合、ステーションは、状態２へ上がることが可能となり、この状態でＡＰに対する認証は受けられるが、ＡＰとの関連付けは受けられない。状態２で、ステーションは、ステーションがＡＰとの関連づけを受けることなどを可能とするような限られた数のフレームタイプを使用することができる。

【００１６】
次いで、ステーションがＡＰとの関連づけまたは再関連づけに成功した場合、ステーションは、状態３へ上がり、この状態で、認証と関連付けとを受けることが可能となる。状態３で、ステーションは任意のフレームタイプを使用して、ＷＬＡＮ内のＡＰおよび別のステーションとの通信を行うことが可能となる。ステーションが関連付け解除通知を受信した場合、ステーションは状態２への遷移が可能となる。さらに、ステーションは、認証解除通知を受信した場合、状態１への遷移が可能となる。ＩＥＥＥ８０２．１１規格の下では、ステーションは異なるＡＰに対して同時に認証を受けることはできるが、関連付けについてはいつも１つのＡＰとの関連付けしか受けることはできない。

【００１７】
再度図２を参照すると、ひとたびステーションがＡＰに対する認証を受け、ＡＰとの関連づけを受けると、ステーションはＷＬＡＮ内の別のステーションと通信を行うことが可能となる。特に、ステーションはソースアドレス、基本サービス設定識別アドレス（ｂａｓｉｃ ｓｅｒｖｉｃｅ ｓｅｔ ｉｄｅｎｔｉｆｉｃａｔｉｏｎ ａｄｄｒｅｓｓ）（“ＢＳＳＩＤ”）および宛先アドレスを含むメッセージをステーションの関連するＡＰへ伝送することが可能となる。次いで、ＡＰは、宛先アドレスとしてメッセージに指定されたステーションへこのメッセージを配信することができる。この宛先アドレスは、配信システムを通じてＡＰとリンクされた同じＢＳＳ内の、あるいは、別のＢＳＳ内のステーションを指定することができる。

【００１８】
図２は、各々が３つのステーションを備えた３つのＢＳＳを有する拡張サービス設定を描くものであるが、拡張サービス設定を行うことにより、任意の数のステーションを設けることが可能な任意の数のＢＳＳを備えることが可能となる。
【００１９】
図４を参照すると、検出器を用いてＷＬＡＮをモニタすることができる。さらに詳細には、ＷＬＡＮ上で伝送信号を受信し、次いで、受信した伝送信号に基づいてデータベースを編集できるように検出器を構成することができる。以下説明するように、データベースで編集した情報を利用して、種々のイベントの発生に対するＷＬＡＮのモニタおよび／または問題点の診断を次に行うことが可能となる。
【００２０】
図５を参照すると、１つの構成では、検出器により編集されたデータベースには、ノード要素、セッション要素およびチャネル要素が含まれる。図５は、検出器が編集したデータベースの構造を抽象的に描くことを意図したものであって、データベースの実際の構造を描くことを意図するものではないことに留意されたい。
【００２１】
ノード要素はＡＰやステーションのようなＷＬＡＮ内のノードと関連づけられる。１つの構成では、ノード要素は、フレームのソースフィールドと宛先アドレスフィールドとから得ることができるＭＡＣアドレスにより索引付けが行われる。データベース内の個々のノード要素には、当該ノードの中へ入ってくる伝送信号の数を追跡する１組の統計と、当該ノードから出てゆく伝送信号の数を追跡する別の組の統計とが含まれる。上記組の統計では、フレームタイプ（ビーコン、プローブ、など）、アドレスタイプ（ユニキャスト、マルチキャスト、放送、など）、受信無線属性（信号強度、ノイズ、ＣＲＣエラー、伝送信号速度など）に基づいて伝送信号の類別が行われる。個々のノード要素は１または２以上の以下のフィールドを含むことができる。
－　ｃｒｅａｔｅｔｉｍｅ（ノードを発見する時間）
－　ＭＡＣａｄｄｒｅｓｓ（ノードのＭＡＣアドレス）
－　ＢｅａｃｏｎＩｎｔｅｒｖａｌ（ノードがＡＰである場合のビーコン間隔）
－　Ｃａｐａｂｉｌｉｔｙ（ＥＳＳ／ＩＢＳＳのビットマップ、ＣＦ－ｐｏｌｌ、有線と同レベルのプライバシ（ｗｉｒｅｄ　ｅｑｕｉｖａｌｅｎｔ　ｐｒｉｖａｃｙ：ＷＥＰ）、プリアンブル、チャネルの軽快さ（ａｇｉｌｉｔｙ）、など）
－　ＡｕｔｈＡｌｇｏｓ（オープンシステムまたは共有鍵の認証）
－　ＩｓＩｎＥｓｓＭＯＤＥ（インフラストラクチャモード）
－　ＨａｓＰｒｉｖａｃｙ（作動可能ＷＥＰ）
－　ＳｕｐｐｏｒｔＳｈｏｒｔＰｒｅａｍｂｌｅ（サポートされている短いプリアンブル）
－　ＩｓＡＰ（このノードはＡＰである）
－　ＩｓＢｒｉｄｇｅ（このノードはブリッジである）
－　ＡｐＡｎｎｏｕｎｃｅｄＳＳＩＤ（ＡＰの場合、ＳＳＩＤに通知した）
－　ＳＳＩＤ（ノードのＳＳＩＤ（ＡＰまたはステーション））
－　ＡＰＮＡＭＥ（ノードがＡＰの場合、ノードの、通知を受けたＡＰ名）
－　ＤＳＰａｒａｍＳｅｔ（チャネル割当て）
－　ＳｕｐｐｏｒｔｅｄＲａｔｅｓ（１、２、５．５または１１ｍｂｐｓ）
－　ＩＰＡｄｄｒｅｓｓ（ノードのＩＰアドレス）
ステーションが認証を受け、ＡＰとの関連付けを受けた場合などに、セッション要素は任意の２つのノード間で確立されたセッションと関連づけられる。データベース内の個々のセッション要素には、２つのノード間での１方向の伝送信号の数を追跡する１組の統計と、２つのノード間での別方向の伝送信号の数を追跡する別の組の統計とが含まれる。例えば、ステーションとＡＰ間にセッションが生じた場合、一方の組の統計はステーションからＡＰへの伝送信号の数を追跡し、他方の組の統計はＡＰからステーションへの伝送信

号の数を追跡する。

【００２２】

チャネル要素はＷＬＡＮ内のチャネルと関連づけられる。ＩＥＥＥ８０２．１１規格の現在の実施構成では、合衆国で合計１１チャネルが使用され、ヨーロッパで１３チャネルが使用され、日本で１４チャネルが使用されている。データベース内の個々のチャネル要素には、当該チャネル内の伝送信号の数を追跡する１組の統計が含まれる。

【００２３】

検出器により編集されるデータベースの基本構成について説明したが、以下、検出器により受信できる異なるタイプの伝送信号と、伝送信号から取得できるタイプの情報とについての説明する：

【００２４】

【表１】

伝送信号のタイプ	取得情報
ビーコンフレーム	ビーコン間隔、ケイパビリティ、プライバシプリアンブル（Privacy Preamble）、ＳＳＩＤ、サポートレート、チャネル、ＡＰ名
プローブ要求	伝送側ノードのＳＳＩＤ、ＳＳＩＤのサポートレート
プローブ応答	ビーコン間隔、ケイパビリティ、プライバシプリアンブル、ＳＳＩＤ、サポートレート、チャネル、ＡＰ名
認証フレーム	認証アルゴリズム（オープンシステムまたは共有化鍵）、認証状態情報（認証シーケンス番号）
認証解除フレーム	セッションが終了した旨の表示
関連付け要求＆再関連付け	伝送側の可能出力、サポートレート、ＳＳＩＤ
関連付け応答	可能出力、セッションが確立された旨を確認する。
データフレーム	ＩＰアドレス、セッションが確立された旨を確認する、伝送側の識別番号、使用ＡＰの識別番号

表１

次いで、受信した伝送信号から得られる情報を利用して、データベースの編集および／または更新を行うことができる。例えば、検出器が、データベースに追加されていないビーコンフレームをノードから受信すると仮定する。これによって、新たなノード要素がデータベース内に形成されることになり、このノードにノード１のラベルをつけるものとする。上述のように、ＭＡＣアドレスはフレームのソースフィールドと宛先アドレスフィールドとから取得することができる。さらに、ビーコンフレームはＡＰにより伝送される。したがって、ノード１はＡＰとして、かつ、そのＭＡＣアドレスにより特定することができる。さらに、上述のように、ビーコンフレームは、ビーコン間隔、ケイパビリティ、プライバシプリアンブル、ＳＳＩＤ、サポートレート、チャネル、ＡＰ名などの情報を含むことができる。したがって、ノード１の適切なフィールドが上記情報で更新されることになる。さらに、ノード１として外へ向かう伝送信号を追跡する組の統計が更新される。適切なチャネル要素の組の統計も更新される。

【００２５】

次に、プローブ要求が、データベースに追加されていないノードから受信されたと仮定

する。このため、新たなノード要素がデータベース内に形成され、このノードにノード２のラベルをつけることにする。さらに、プローブ要求がステーションにより伝送される。したがって、ノード２をステーションとして特定することが可能となる。さらに、上述のように、プローブ要求は、伝送側ノードのＳＳＩＤおよび伝送側ノードのサポートレートなどの情報を含むことができる。したがって、ノード２の適切なフィールドが上記情報で更新されることになる。さらに、ノード２用として外へ向かう伝送信号を追跡する組の統計が更新される。さらに、やはりプローブ要求から決定することができるノード１へプローブ要求が伝送されると仮定すると、ノード１用として内へ向かう伝送信号を追跡する組の統計が更新される。適切なチャネル要素用の統計フィールドも更新される。

【００２６】

ビーコンフレーム内でＡＰのＳＳＩＤの抑制が可能となり、これはビーコンフレームからＳＳＩＤを取得できないことを意味する。このような例では、ＡＰへプローブ要求を伝送するステーションのプローブ要求からＡＰのＳＳＩＤを得ることができる。そして、ＡＰはプローブ応答をステーションへ伝送する。プローブ要求が正しいＳＳＩＤを含まなければ、ＡＰはステーションへプローブ応答を伝送しない。このようにして、ステーションがＡＰへ伝送するプローブ要求に基づいてＡＰのビーコン内のＡＰのＳＳＩＤを抑制するＡＰのＳＳＩＤを決定することが可能となる。

【００２７】

次に、データベースへ追加されていないノードからデータフレームが受信されたと仮定する。したがって、データベースで新たなノード要素が形成され、このノードにノード３のラベルをつけることにする。また、本例では、データフレームがノード３からノード１へ伝送されていると仮定する。ノード３とノード１の識別番号はデータフレームのヘッダ情報、特に、宛先アドレスとソースアドレスとをチェックすることにより得ることが可能である。したがって、たとえノード１の存在がわかっていなくても、データフレームからノード１の存在を識別することが可能となる。ノード３とノード１間でのデータフレームの伝送信号によって、２つのノードが同じチャネルで作動していること、および、同じ認証アルゴリズムを利用していることも確定される。したがって、ノード３とノード１用の適切なフィールドの更新が可能となる。ノード３用の外へ向かう伝送信号を追跡する組の統計と、ノード１用の内へ向かう伝送信号を追跡する組の統計と、適切なチャネル要素の組の統計も更新される。

【００２８】

さらに、データフレームのヘッダに基づいてステーションまたはＡＰとしてノード１とノード３とを特定することができる。具体的には、データフレームのヘッダ内の配信システムとしてＡＰが特定される。したがって、ノード３からノード１へのデータフレームの宛先アドレスが配信システムを指定しさえすれば、ノード１をＡＰとして特定することが可能となり、ノード３をステーションとして特定することが可能となる。しかし、宛先アドレスとソースアドレスの双方が配信システムを指定した場合、ノード１とノード３は双方ともＡＰとなる。さらに詳細には、ＡＰはブリッジとして作動することになる。このようにして、検出器で受信したデータフレームに基づいて、ＷＬＡＮ内でブリッジとして作動するノードの特定が可能となる。

【００２９】

データフレームの受信は、ノード３とノード１との間でセッションが確立したことを確認するものでもある。したがって、セッション要素がデータベースで形成され、このセッションにセッション１のラベルをつけることにする。次いで、ノード３からノード１への伝送信号を追跡する組の統計が更新される。

【００３０】

データフレームが暗号化されている場合、ノード１とノード３とを有線と同レベルのプライバシ（ＷＥＰ）暗号方式を利用するものとして特定することができる。次いで、ノード１とノード３内の適切なフィールドが更新される。

【００３１】

このようにして、ＷＬＡＮ内のノードと、セッションと、チャネルとからなるデータベースの編集を検出器により行うことが可能となる。しかし、上記例はデータベースの編集処理についての包括的な説明を意図するものではないことに留意されたい。上記例は、説明ではなくむしろ上記編集処理の例示を意図するものである。

【００３２】

本実施形態例では、検出器は、ある期間にわたって伝送信号を受信することによりデータベースの編集を行う。１つの構成では、検出器は、５分、１０分またはそれ以上の分などの数分の時間にわたってデータベースの編集を行う。しかし、この期間は状況に応じて変動する場合があることに留意されたい。例えば、ＷＬＡＮのさらに包括的なアセスメントを行うために、１時間またはそれ以上の時間のようなさらに長期間を費やす場合もある。

【００３３】

上述のように、検出器は、ＷＬＡＮ内の利用可能なチャネルのスキャニングを行うことにより、ＷＬＡＮを介して伝送信号の受信が可能である。上記とは別に、専用チャネルの選択により走査を行うことが可能である。上記記載のように、利用可能なチャネル数も国に依って変動する場合がある。例えば、合衆国では合計１１チャネルが使用され、ヨーロッパでは１３チャネルが使用され、日本では１４チャネルが使用されている。

【００３４】

検出器がチャネルを走査して伝送信号を受信するとはいえ、検出器は受動的に伝送信号の受信を行う。このことは検出器がＷＬＡＮで信号を放送しないことを意味する。受動的にＷＬＡＮがモニタされる利点として、ＷＬＡＮ上で追加の帯域幅が消費されないという点が挙げられる。

【００３５】

検出器は無線ローカルエリアネットワーク内のステーションであってもよい。さらに、検出器は、移動局、携帯局、固定局、等であってもよい。例えば、検出器はラップトップコンピュータ、個人用情報機器、等であってもよい。さらに、ＷＬＡＮをモニタするために、ユーザが診察用ツールとして検出器を利用したり、管理者が管理上のツールとして利用したりするもの等であってもよい。

【００３６】

例えば、検出器によって編集したデータベースを用いて、種々のイベントの発生に対してＷＬＡＮのモニタを行うことが可能である。以下の表は、編集済みデータベースに基づいて検出が可能な或るセキュリティとパフォーマンスイベントの例をリストするものである：

Ｉ．セキュリティイベント

【００３７】

【表２】

イベント	検出方法
ＷＥＰ使用禁止状態のＡＰ	ビーコンフレームをチェックする；データフレームをチェックして、データフレームが暗号化されているかどうかを判定する。
ＷＥＰ使用禁止状態のクライアント	データフレームをチェックして、データフレームが暗号化されているかどうかを判定する。
瑕疵のあるＷＥＰ暗号方式	３つのシーケンシャルなデータフレームをチェックして、暗号方式が予想可能なパターンにぴったり合っているかどうかを判定する。
使用オープンシステムの認証	認証要求および／または応答から判定する。
デバイス・プロービングネットワーク	長さ０のＳＳＩＤに対するプローブ要求フレームをチェックし、プローブ要求フレームがＳＳＩＤフィールドのみを有しているかどうかをチェックする。プローブ応答の受信後ステーションが認証を続行できないかどうかを判定する。
回数を超過した認証の失敗	認証失敗回数をカウントする。
ＡＰの未構成	ＡＰのＳＳＩＤをチェックしてＳＳＩＤがデフォルトのＳＳＩＤであるかどうかを判定する。
不正ＡＰの検出	既知の正規ＡＰのリストと比較する。
不正クライアントの検出	既知の正規クライアントのリストと比較する。
伝送欺瞞ＭＡＣアドレス	ノードへのおよび／またはノードからのパッケージのシーケンス番号をチェックする。

表２

ＩＩ．パフォーマンスイベント

【００３８】

【表３－１】

イベント	検出方法
信号強度の弱いＡＰ	ＷＬＡＮカードアンテナから受信したデータに基づいて測定を行う。２０％の相対信号強度表示（ＲＳＳＩ）などの設定しきい値以下であれば信号は弱いと考えることができる。
ＣＲＣエラー比率の超過	個々のチャネルとノードに対して伝送済みフレームからレートを算出する。総フレーム比率として２０％のＣＲＣエラーフレームなどのような設定しきい値以上の場合、エラー比率を上回ったものとする。
フレーム再試行レートの超過	個々のチャネルとノードとに対して伝送済みフレームからレートを算出する。総フレーム比率として８０２.１１の再試行フレームの１０％などのような設定しきい値以上であれば再試行レートを超過したものとする。
ｔｘを上回る低速レート	個々のチャネルとノードとに対して伝送済みフレームからレートの計算を行う。総データフレーム比率として７０％－１１ｍｂｐｓデータフレームなどの設定しきい値以上であればレートを上回ったものとする。
ＡＰ関連容量の満量	エラーコード＃１７に対して関連付け応答フレームをチェックする。
断片化レートの超過	個々のチャネルとノードとに対して伝送済みフレームからレートを算出する。総フレーム比率として５０％の断片化済みフレームなどのような設定しきい値以上であれば断片化レートを上回ったものとする。
帯域幅の使用超過	個々のチャネルとノードとに対して伝送済みフレームから伝送時間を計算する。
過度の脱落ビーコン	ＡＰカウント受信済みビーコンフレーム。予想されるビーコン比率の５０％の脱落ビーコンなどのような設定しきい値以上であれば脱落ＡＰビーコンが過度であるとする。
高速をサポートしていないＡＰ	ビーコンフレームとプローブ応答フレーム

【００３９】

【表３－２】

	とから判定する。
過負荷ＡＰ状態チャネル	同じチャネル内のアクセスポイントであるノードの数から判定する。
脱落パフォーマンスオプション	ビーコンフレームとプローブ応答フレーム内の互換性フィールドから判定する。
ＰＣＦとＤＣＦの双方がアクティブ	ビーコンフレームとプローブ応答フレーム内の互換性フィールドから判定する。
相互干渉状態のＡＰ	同じチャネル内のアクセスポイントであるノードの数と、アクセスポイントからの信号（ＲＦ）の数とから判定する。
矛盾するＡＰ構成	アクセスポイントとして特定されたノードと関連づけられたフィールドから決定する。例えば、複数のＡＰが同じＳＳＩＤを持っている場合。
高い雑音レベルを持つチャネル	ＷＬＡＮカードアンテナから受信したデータに基づいて判定する。
過度のマルチキャスト／放送	個々のチャネルとフレームとに対して、伝送済みフレームからマルチキャスト／放送フレームの数を決定する。総フレームの１０％などの設定しきい値よりも多ければ過剰な数とする。

表３

１つの構成では、上記リストしたイベントのうちの１つが検出されると、警報を出力するように検出器を構成することが可能である。しかし、どのイベントが警報および警報のタイプをトリガーするかはユーザが選択および／または変更できることに留意されたい。

【００４０】

データベースの編集に加えて、ステーションがサービスを受けるとき経験するかもしれない問題点を分析するとき、特定ステーションの状態を判定できることが望ましい場合がある。上述のように、現在のＩＥＥＥ８０２．１１規格によれば、ステーションは認証を受け、ＡＰと関連づけられてＢＳＳの一部となり、それによってサービスを受けることになる。また上記記載のように、認証処理および関連付け処理の際のステップは３つの状態（状態１、状態２、状態３）に類別される。

【００４１】

例えば、図６を参照して、ＡＰからサービスを受ける際、ステーションに問題が生じていると仮定する。ステーションが状態１に達することができるかどうかを判定すれば、状態２または状態３は問題のトラブルシューティングを助けることができる。

【００４２】

したがって、ＷＬＡＮ内に検出器を配置して、ステーションから送られてくる伝送信号と、ステーションが受信する伝送信号とを検出器が受信できるようにすることが可能となる。検出器は必ずしも物理的にステーションに隣接している必要はないことに留意された

い。代わりに、検出器の受信範囲がステーションとＡＰとをカバーするように検出器はステーションの十分近くに存在していればよい。

【００４３】

ステーションから伝送される伝送信号と、ステーションが受信する伝送信号とをチェックすることにより、検出器はステーションの状態を判定することが可能となる。さらに詳細には、異なるタイプの伝送信号を異なる状態を示すものとして特定することが可能となる。例として、異なるタイプの伝送信号と、これらの伝送信号が示す状態とを以下の表に示す：

【００４４】

【表４】

伝送信号のタイプ	状態
ステーションが伝送するプローブ要求	1
ＡＰが伝送するプローブ応答	1
ステーションが伝送する認証要求	1
認証応答ｗ／ＡＰが伝送する呼掛けテキスト	1
ステーションが伝送する認証呼びかけ応答	1
ＡＰが伝送する認証最終応答	1 － 否定応答時　2 － 肯定応答時
ＡＰが伝送する認証解除	1
ＡＰによる関連付け解除	1
ステーションが伝送した関連付け要求	2
ステーションが伝送した関連付け応答	2 － 否定応答時　3 － 肯定応答時
ステーションまたはＡＰが伝送する上位層プロトコルデータ	3

表４

したがって、ステーションへまたはステーションから伝送された伝送信号を受信したとき、検出器は伝送信号をチェックして、伝送信号が上記にリストされているタイプの伝送信号のうちの１つであるかどうかの判定を行う。そうであれば、検出器は、伝送信号を受信または伝送したステーションの状態を判定することができる。検出器は、編集済みデータベース内の、ステーション用として受信済みの伝送信号をベースにすることによってもステーションの状態を判定できることに留意されたい。

【００４５】

例えば、ステーションが伝送したプローブ要求フレームを検出器が受信した場合、検出器はステーションが状態１にあると判定することができる。ＡＰによりステーションへ伝送されたプローブ応答フレームを検出器が受信した場合、検出器はステーションが状態１にあると判定することができる。伝送済みまたは受信済みの上位層プロトコルデータであるデータフレームをステーションが受信した場合、検出器はステーションが状態３にあると判定することができる。

【００４６】

チェックリストとして伝送信号のタイプを表示するように検出器を構成することもできる。例えば、以下のチェックリストを提供することができる：

【００４７】

【表５】

ステーションが受信したビーコン
ステーションが伝送したプローブ要求
ステーションが受信したプローブ応答
ステーションが伝送した認証要求
ステーションが受信した認証呼びかけ
ステーションが受信した認証呼びかけ応答
ステーションが受信した認証最終応答
ステーションが伝送した相関付け要求
ステーションが受信した相関付け応答
ステーションが伝送したデータ
ステーションが受信したデータ

表５

このリストの伝送信号のうちの１つが検出されると、当該タイプの伝送信号がマークされる。例えば、ステーションが伝送した認証要求が受信されると、検出器は上記から“認証要求伝送済み”の行に“照合印を付ける”ことができる。このようにして、ＷＬＡＮまたはトラブルシュータの管理者などの検出器のユーザはステーションの状態をさらに簡単に判定することができる。

【００４８】

さらに、以下説明するように、ステーションは１または２以上のチャネルの利用が可能である。これによって、利用可能なチャネルの各々について別々のチェックリストを提供することができる。

【００４９】

図７を参照すると、ステーションは、ＡＰからサービスが受けられるようになる前に認証を受ける必要がある。ＩＥＥＥ８０２．１ｘ規格に準拠するＬＡＮプロトコルを介して拡張可能認証プロトコル（ＥＡＰＯＬ）などのＷＬＡＮ環境で認証プロトコルを実行してセキュリティを上げることが可能となる。

【００５０】

現在のＥＡＰＯＬプロトコルによれば、認証を受けることを望むステーション（サプリカントと呼ばれる）は、遠隔認証ダイアルユーザサービス（ＲＡＤＩＵＳ）サーバなどの認証サーバを利用して認証を受ける。図７に描かれているように、ステーションはＡＰと通信し、ＡＰ（オーセンティケータ（ａｕｔｈｅｎｔｉｃａｔｏｒ）と呼ばれる）が認証サーバと通信を行ってステーションの認証を行う。

【００５１】

認証処理中、ステーション、ＡＰおよび認証サーバは複数の伝送信号を交換する。さらに詳細には、１つの例示処理モードで、ＡＰは“ＥＡＰ要求／識別番号”伝送信号をステーションへ伝送する。次いで、ステーションは“ＥＡＰ応答／識別番号”伝送信号をＡＰへ伝送する。次いで、ＡＰは受信済みの“ＥＡＰ応答／識別番号”伝送信号を認証サーバへ伝送する。これに応答して、認証サーバはトークンパスワードシステム（ｔｏｋｅｎ　ｐａｓｓｗｏｒｄ　ｓｙｓｔｅｍ）の場合と同じ様にＡＰへ呼びかけを伝送する。ＡＰはアクセス特権要求（ｃｒｅｄｅｎｔｉａｌ　ｒｅｑｕｅｓｔ）としてステーションへ呼びかけを伝送する。ステーションは、アクセス特権要求に対する応答をＡＰへ伝送する。ＡＰは認証サーバへ応答を伝送する。ステーションからの応答が正しければ、認証サーバは“ＥＡＰ成功”を示す伝送信号をＡＰへ伝送し、ＡＰはステーションへパッケージを伝送する。応答が適切なものでなければ、認証サーバは“ＥＡＰ失敗”を示す伝送信号をＡＰへ伝送し、ＡＰはこの伝送信号をステーションへ伝送する。ステーションと、ＡＰと、認証サーバとの間で交換される伝送信号の数とタイプは実行する処理モードに応じて変動が

可能であると認識すべきである。

【００５２】

上述のように、１つの実施形態例では、ＷＬＡＮ内に検出器を配置することが可能であり、それによって、ステーションから伝送され、ステーションが受信した伝送信号を検出器が受信できるようになっている。再言するが、検出器は必ずしも物理的にステーションに隣接している必要はないことに留意されたい。代わりに、検出器の受信範囲がステーションをカバーするように検出器はステーションの十分近くに存在していればよい。

【００５３】

ステーションから伝送され、受信される伝送信号をチェックすることにより、検出器はステーションの状態を判定することができる。さらに詳細には、検出器は、ＥＡＰＯＬプロトコルに従って上記記載の認証処理中、ステーションとＡＰ間で交換される伝送信号を受信することができる。次いで、検出器は受信した伝送信号に基づいてステーションの状態を判定することができる。具体的には、ＥＡＰＯＬトランザクションが８０２．１１データとして状態３で行われることに起因して、ステーションを状態３にあるものと判定することができる。

【００５４】

さらに、伝送信号のタイプをチェックリストとして表示するように検出器を構成することも可能である。例えば、以下のチェックリストを表示することができる：

【００５５】

【表６】

ステーションが伝送した８０２．１Ｘを開始
ステーションが伝送した識別番号要求
ステーションが受信した識別番号応答
ステーションが伝送したアクセス特権要求
ステーションが受信したアクセス特権応答
ステーションによる８０２．１Ｘ認証ＯＫ
ステーションが失敗した８０２．１Ｘ認証
ステーションが伝送した認証解除
ステーションが伝送したデータ
ステーションが受信したデータ

表６

上記リストの伝送信号のうちの１つが検出されると、当該タイプの伝送信号がマークされる。例えば、ＡＰが伝送した“ＥＡＰ要求／識別番号”パッケージが受信された場合、検出器は上記から“伝送された識別番号要求”の行に“照合印を付ける”ことができる。このようにして、ＷＬＡＮまたはトラブルシュータの管理者などの検出器のユーザはステーションの状態をさらに簡単に決定することができる。

【００５６】

さらに、以下に説明するように、ステーションは１または２以上のチャネルを使用することができる。したがって、利用可能なチャネルの各々について別々のチェックリストを提供することができる。

【００５７】

ステーションから伝送され、ステーションが受信した伝送信号を特定するために、検出器は、ステーションのＭＡＣアドレスを取得する。このＭＡＣアドレスは、伝送済みフレームのソースフィールドと宛先アドレスフィールドとから得ることができる。ＭＡＣアドレスは、ステーションから直接取得することも可能である。上記とは別に、ステーションのＭＡＣアドレスを格納し、ＭＡＣアドレス割当て表から検索することができる。ＷＬＡＮの管理者がこのＭＡＣアドレス割当て表の保守管理を行うことができる。

【００５８】
さらに、ステーションが通信を試行している特定の対象ＡＰがわかっていれば、当該ＡＰが作動している特定のチャネルをモニタすることが可能となる。ステーションが、複数のＡＰとの通信を試行していて、かつ、当該ＡＰの識別番号がわかっていれば、当該ＡＰが作動している特定のチャネルのモニタが可能である。
【００５９】
さらに、検出器は、無線ローカルエリアネットワークのチャネルを走査して、既知または未知のＡＰを持つステーションから伝送され、該ステーションが受信した伝送信号を受信することができる。上述のように、ＩＥＥＥ８０２．１１規格の現在の実施構成では、合衆国で合計１１チャネルが使用され、ヨーロッパで１３チャネルが使用され、日本で１４チャネルが使用されている。便宜上、以下の説明では検出器とＷＬＡＮとが合衆国内に配置されているものと仮定する。しかし、検出器は任意の個数のチャネルを用いて、および、様々な国々において作動するように構成することが可能であることに留意されたい。
【００６０】
１つの構成では、チャネル１をモニタすることにより検出器は走査を開始し、次いで、残りの１０チャネルの各々を下へ走査するように構成される。サービスを受ける際、ステーションに問題が生じると、ステーションは通常、チャネルを切り替え、関連付けの試行を繰り返し、関連付け失敗のシナリオを繰り返すことになる。ステーションは、サービスを受ける努力を行う際、チャネルを通じて連続サイクル処理を行うことができる。したがって、検出器は、十分な時間の間、特定のチャネルをモニタするように構成され、ステーションが１または２以上のサイクルを終了できるようになる。例えば、検出器は約３秒の間個々のチャネルのモニタを行うように構成することができる。
【００６１】
チャネルのすべてを走査後伝送信号が検出されなかった場合、ステーションはリブートされる。上述のように、サービスを受けようと試行する際、ステーションはチャネルを介して繰り返しサイクル処理を行うように構成することができる。しかし、１回のサイクルを試行するだけで最後のチャネルを試行した後、停止するようにステーションを構成してもよい。ステーションがリブートされると、ステーションは一般にチャネル１で作動を開始する。したがって、ステーションのリブートを行うことにより、さらに、チャネル１でモニタを行うことにより、ステーションへ伝送されるまたはステーションが受信する伝送信号の検出が可能となる。しかし、ステーションのリブートに若干の時間（一般に数秒）がかかる場合もある。したがって、検出器は、別のチャネルよりもより長い継続時間の間チャネル１をモニタするように構成される。例えば、１つの構成では、検出器は、３０秒間チャネル１をモニタするように構成される。
【００６２】
上述のように、検出器はＷＬＡＮで利用可能なチャネルを走査することができる。上記とは別に、専用チャネルを選択して、この専用チャネルを走査することができる。検出器は、チャネルの走査を行うとはいえ、受動的に伝送信号の受信を行う。この受動的受信は、ＷＬＡＮで信号を放送しないことを意味するものである。このことによって、ＷＬＡＮで追加の帯域幅が消費されないという利点が生じることになる。
【００６３】
検出器は、無線ローカルエリアネットワーク内のステーションであってもよい。さらに、検出器は、移動局、携帯局、固定局、等であってもよい。例えば、検出器はラップトップコンピュータ、個人用情報機器、等であってもよい。さらに、検出器はユーザが診察用ツールとして利用したり、管理者が管理上のツールとして利用したりするもの等であってもよい。
【００６４】
編集済みデータベースおよび／またはステーションの所定の状態に基づいて、ステーションの接続上の問題の原因を確定することができる。例えば、以下の表は生じ得る問題並びにこれら問題点の検出方法をリストするものである。

【００６５】
【表７】

問題点	検出方法
ＳＳＩＤのミスマッチ	編集済みデータベース内のクライアントステーションのＳＳＩＤをすべてのＳＳＩＤに対してマッチさせることにより
ワイルドカード（全てに一致する）ＳＳＩＤ	複数のＳＳＩＤがＷＬＡＮ内に存在する場合、クライアントステーションのＳＳＩＤをヌルに対してマッチさせることにより、ＳＳＩＤだけが問題であるようにすることができる。
チャネルのミスマッチ	個々のチャネルでステーションが伝送したトラフィックを追跡することにより、同じＩＤのＡＰが存在するけれども、ステーションがいずれのパケットも伝送しなかった旨をチャネルに報告する。
速度のミスマッチ、プライバシ、ネットワークタイプ、またはプリアンブル	ＡＰの可能出力属性に対してクライアントステーションの可能出力属性をマッチさせることにより。ステーションがプローブ要求を無視する場合、ＡＰがステート(stat)にマッチしないことを認知する。
認証の失敗	認証応答パケットを追跡することにより
関連付けの失敗	関連付け応答パケットを追跡することにより
機器の故障	パケットがステーションから全く伝送されていない旨を通知することにより
ＡＰ信号の弱化	編集済みデータベース内のＡＰ信号強度のチェックを行うことにより。検出器をステーションに隣接して配置して、信号強度の取得を図るようにしてもよい。
速度のミスマッチ	ＡＰのデータ転送速度に対してサポートされているデータ転送速度にステーションをマッチさせることにより
ＷＥＰキーのミスマッチ	関連付け状態に達し、クライアントステーションはデータパケットを伝送した。しかし、関連するＡＰはデータパケットを返送しない。
上位層プロトコル問題	ステーションとＡＰ間のデータ交換の成功を検出することにより

表７

或る実施形態、実例、適用例と関連して本発明について説明したが、本発明から逸脱することなく、種々の修正および変更を行うことも可能であることは当業者には明らかであろう。

【図面の簡単な説明】

【００６６】

【図１】図１は、例示の開放型システム間相互接続（ＯＳＩ）の７つの階層モデルを示す

。
【図２】図２は、無線ローカルエリアネットワーク（“ＷＬＡＮ”）で設定された例示の拡張サービスを示す。
【図３】図３は、ＷＬＡＮにおけるステーションの種々の状態を示す例示のフローチャートである。
【図４】図４は、伝送信号を交換するアクセスポイントとステーションの実施形態例を示す。
【図５】図５は、例示のデータベースの要素を示す。
【図６】図６は、伝送信号を交換する別の実施形態例を示す。
【図７】図７は、伝送信号を交換するさらに別の実施形態例を示す。

【図１】

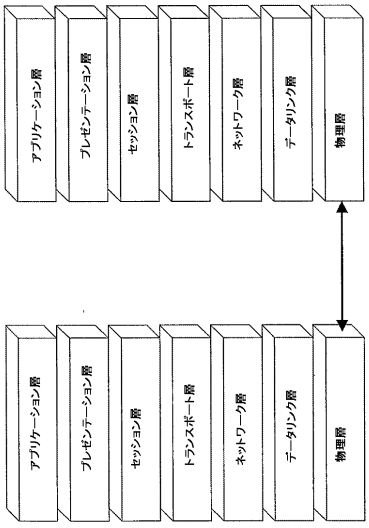

Fig. 1

【図２】

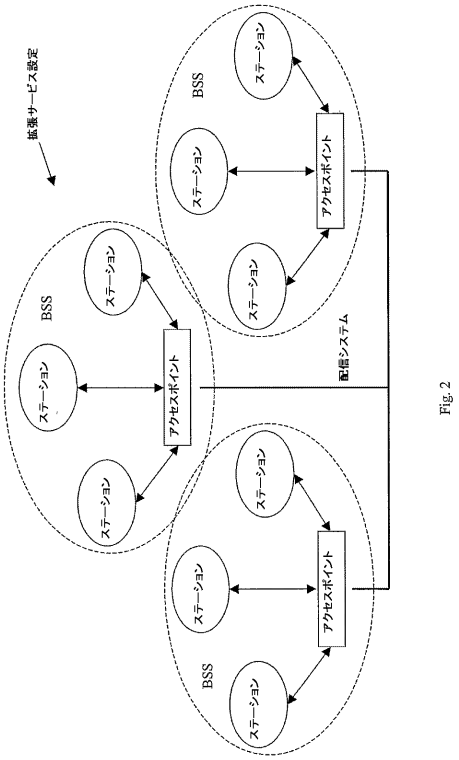

Fig. 2

【図３】

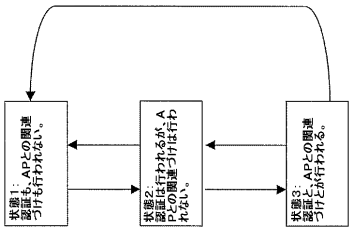

Fig. 3

【図４】

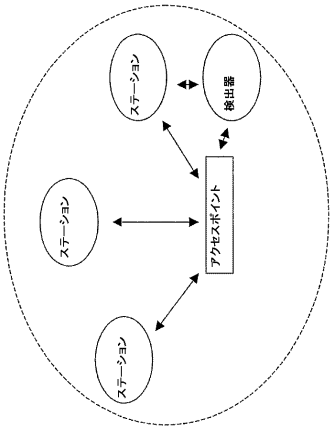

Fig. 4

【図５】

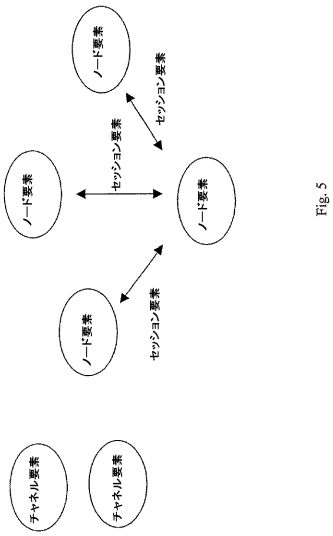

Fig. 5

【図６】

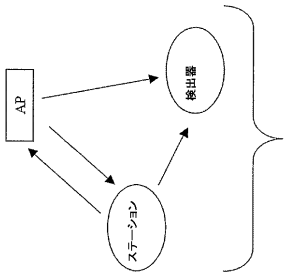

Fig. 6

【図７】

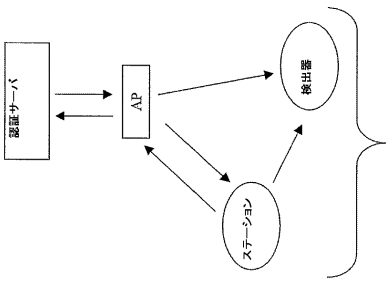

Fig. 7

フロントページの続き

(72)発明者 ウー, マイルズ
アメリカ合衆国 カリフォルニア ９４５３９, フレモント, クララ コート ２３１
(72)発明者 アウ, ディーン
アメリカ合衆国 カリフォルニア ９４０８６, サニーベール, コア コート ７０７

審査官 福岡 裕貴

(56)参考文献 特表２００１－５１２６３５（ＪＰ, Ａ）
特開平０８－２３７３３４（ＪＰ, Ａ）
特開平０９－１３０３３９（ＪＰ, Ａ）
特開２００１－０８６０７４（ＪＰ, Ａ）
Joe Bardwell, Assessing wireless Security with AirPeek, WildPackets, Inc., ２００２年１月１３日, ＵＲＬ, http://www.packetnexus.com/docs/AiroPeek_Security.pdf

(58)調査した分野(Int.Cl., ＤＢ名)
H04W 4/00-99/00
H04L 12/28-12/46