(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4571971号
(P4571971)

(45)発行日　平成22年10月27日(2010.10.27)　(24)登録日　平成22年8月20日(2010.8.20)

(51)Int.Cl.		F I		
H04W 24/00	(2009.01)	H04L	12/28	300M
H04W 84/12	(2009.01)	H04Q	7/00	186
H04W 12/12	(2009.01)	H04L	12/22	
H04L 12/22	(2006.01)			

請求項の数 19　(全 8 頁)

(21)出願番号	特願2007-503983 (P2007-503983)
(86)(22)出願日	平成17年3月11日 (2005.3.11)
(65)公表番号	特表2007-529957 (P2007-529957A)
(43)公表日	平成19年10月25日 (2007.10.25)
(86)国際出願番号	PCT/US2005/008292
(87)国際公開番号	WO2005/089242
(87)国際公開日	平成17年9月29日 (2005.9.29)
審査請求日	平成20年3月6日 (2008.3.6)
(31)優先権主張番号	10/800,556
(32)優先日	平成16年3月15日 (2004.3.15)
(33)優先権主張国	米国(US)

(73)特許権者　599101597
シンボル　テクノロジーズ　インコーポレイテッド
アメリカ合衆国　11742－1300
ニューヨーク州　ホウルツビル　メール　ストップ　エイ６　ワン　モトローラ　プラザ（番地なし）
(74)代理人　100082005
弁理士　熊倉　禎男
(74)代理人　100067013
弁理士　大塚　文昭
(74)代理人　100086771
弁理士　西島　孝喜
(74)代理人　100109070
弁理士　須田　洋之

最終頁に続く

(54)【発明の名称】クライアント－サーバーベースのワイヤレス侵入検出システム及び方法

(57)【特許請求の範囲】

【請求項１】

少なくとも１つのアクセスポイントと通信する少なくとも１つの移動ユニットを有するワイヤレスローカルエリアネットワークの無断使用を検出するための方法であって、

前記移動ユニットに対する受信メッセージの数を含む第１ネットワークトラフィックデータを移動ユニットで累積するステップと、

前記アクセスポイントに対する受信メッセージの数を含む第２ネットワークトラフィックデータをアクセスポイントで累積するステップと、

前記第１及び第２のネットワークトラフィックデータをコンピュータへ通信するステップと、

前記第１及び第２のネットワークトラフィックデータを前記コンピュータにおいて相関させ、相関していない第１及び第２のネットワークトラフィックデータを識別すると共に、前記相関していない第１及び第２のネットワークトラフィックデータがしきい値を越えたときにアラーム状態をシグナリングするステップと、を含むことを特徴とする方法。

【請求項２】

前記第１ネットワークトラフィックデータは、前記移動ユニットに対する送信メッセージの数を含む、請求項１に記載の方法。

【請求項３】

前記第１ネットワークトラフィックデータは、前記送信メッセージの行先アドレスを含む、請求項２に記載の方法。

【請求項４】
前記第１ネットワークトラフィックデータは、前記受信メッセージのソースアドレスを含む、請求項１に記載の方法。
【請求項５】
前記第１ネットワークトラフィックデータは、前記移動ユニットと前記アクセスポイントとの関連付け要求の記録を含む、請求項１に記載の方法。
【請求項６】
前記第１ネットワークトラフィックデータは、関連付け解除トランザクションの記録を含む、請求項１に記載の方法。
【請求項７】
前記第１ネットワークトラフィックデータは、前記移動ユニットにより受信されるブロードキャスト及びマルチキャストフレームの数を含む、請求項１に記載の方法。
【請求項８】
前記第１ネットワークトラフィックデータは、認証要求の記録を含む、請求項１に記載の方法。
【請求項９】
前記第２ネットワークトラフィックデータは、前記アクセスポイントに対する送信メッセージの数を含む、請求項１に記載の方法。
【請求項１０】
前記第２ネットワークトラフィックデータは、前記送信メッセージの行先アドレスを含む、請求項９に記載の方法。
【請求項１１】
前記第２ネットワークトラフィックデータは、前記受信メッセージのソースアドレスを含む、請求項１に記載の方法。
【請求項１２】
前記第２ネットワークトラフィックデータは、前記移動ユニットと前記アクセスポイントとの関連付け要求の記録を含む、請求項１に記載の方法。
【請求項１３】
前記第２ネットワークトラフィックデータは、関連付け解除トランザクションの記録を含む、請求項１に記載の方法。
【請求項１４】
前記第２ネットワークトラフィックデータは、前記アクセスポイントにより送信されたブロードキャスト及びマルチキャストフレームの数を含む、請求項１に記載の方法。
【請求項１５】
前記第２ネットワークトラフィックデータは、認証要求の記録を含む、請求項１に記載の方法。
【請求項１６】
前記コンピュータへの前記第１及び第２のネットワークトラフィックデータの前記通信は、周期的なベースで繰り返される、請求項１に記載の方法。
【請求項１７】
前記コンピュータへの前記第１及び第２のネットワークトラフィックデータの前記通信は、前記コンピュータからのコマンド信号に応答して行われる、請求項１に記載の方法。
【請求項１８】
少なくとも１つのアクセスポイントと通信する少なくとも２つの移動ユニットを有するワイヤレスローカルエリアネットワークの無断使用を検出する方法であって、
第１移動ユニットにおいて、該第１移動ユニットに対する受信メッセージの数を含む第１ネットワークトラフィックデータを累積するステップと、
第２移動ユニットにおいて、該第２移動ユニットに対する受信メッセージの数を含む第２ネットワークトラフィックデータを累積するステップと、
前記第１及び第２のネットワークトラフィックデータをコンピュータへ通信するステッ

プと、
前記第１及び第２のネットワークトラフィックデータを前記コンピュータにおいて相関させ、相関していない第１及び第２のネットワークトラフィックデータを識別すると共に、前記相関していない第１及び第２のネットワークトラフィックデータがしきい値を越えたときにアラーム状態をシグナリングするステップと、を含むことを特徴とする方法。
【請求項１９】
ワイヤレスローカルエリアネットワークの無断使用を検出するシステムであって、
少なくとも１つの移動ユニットと、
少なくとも１つのアクセスポイントと、
少なくとも１つのサーバーコンピュータと、
を具備し、
第１ネットワークトラフィックデータが前記少なくとも１つの移動ユニットにより累積され、前記第１ネットワークトラフィックデータが前記少なくとも１つの移動ユニットに対する受信メッセージの数を含み、
第２ネットワークトラフィックデータが前記少なくとも１つのアクセスポイントにより累積され、前記第２ネットワークトラフィックデータが前記少なくとも１つのアクセスポイントに対する受信メッセージの数を含み、
前記第１及び第２のネットワークトラフィックデータが前記少なくとも１つのサーバーコンピュータへ通信され、前記第１及び第２のネットワークトラフィックデータは、前記少なくとも１つのサーバーコンピュータにより相関させられ、相関していない第１及び第２のネットワークトラフィックデータを識別し、前記相関していない第１及び第２のネットワークトラフィックデータがしきい値を越えたときにアラーム状態がシグナリングされるようにした、ことを特徴とするシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ワイヤレスローカルエリアネットワーク（ＷＬＡＮ）に係る。より詳細には、本発明は、ワイヤレスローカルエリアネットワークへの無断アクセス又はアクセス試みを検出するための方法に係る。
【背景技術】
【０００２】
ＷＬＡＮの大成功で、ＷＬＡＮは、これに攻撃し侵入するための新規な方法を積極的に開発しているハッカー（「ウオッカー(whacker)」として知られている）の格好の標的になっている。新規なＷＬＡＮハッキングツールが、不安を煽る頻度でインターネットに発表されている。多くの産業調査では、ＷＬＡＮの展開を考えているほとんどの会社の最高情報幹部にとってＷＬＡＮのセキュリティが最大の問題であることが示されている。不幸なことに、現代のＷＬＡＮセキュリティ解決策は、欠点があるか又は証明されていないかのいずれかである。
【０００３】
本発明の譲受人が所有する、参考としてここに援用する２０００年3月１７日に出願された出願中の米国特許出願第０９／５２８，６９７号には、ＩＥＥＥ規格８０２．１１のプロトコルに従うシステムが説明されているが、これは、ＲＦポート（「アクセスポート」とも称される）と、セルコントローラとの組合せを使用して、古典的な８０２．１１データ通信システムのアクセスポイントの機能を遂行するものである。下位レベルのＭＡＣ機能は、ＲＦポートにより遂行され、そして関連付け及びローミング機能を含む上位レベルのＭＡＣ機能は、セルコントローラにより遂行される。ここで使用する「アクセスポイント」という語は、前記出願中の特許出願に述べられたように、従来のアクセスポイント、例えば、ＩＥＥＥ規格８０２．１１のプロトコルに従いそして全てのＭＡＣ機能を遂行するもの、並びにセルコントローラで動作するＲＦポートを包含することが意図される。
【０００４】

本発明の譲受人が所有する、参考としてここに援用する２００３年１０月６日に出願された出願中の米国特許出願第１０／６７９，５２４号には、ワイヤレスローカルエリアデータ通信ネットワークに使用するためのシステムであって、移動ユニットがアクセスポイントと通信し、そして送信器により送信された信号を使用して送信器を探索するように構成されたシステムが説明されている。許可された送信器を位置に関連付けるデータベースが維持される。選択された信号がアクセスポイントにおいて検出され、そして信号のソースを探索するのに使用するためにその選択された信号に対応する位置データが記録される。この位置データを使用してソースが探索され、そしてソースの位置がデータベースにおける対応位置と比較される。ソースの位置がデータベースにおける対応位置に一致しない場合にはアラーム信号が発せられる。

【発明の開示】

【発明が解決しようとする課題】

【０００５】

本発明の目的は、ＷＬＡＮへの無断アクセス又はアクセス試みを検出するための改良されたシステム及び方法を提供することである。

【課題を解決するための手段】

【０００６】

本発明によれば、少なくとも１つのアクセスポイントと通信する少なくとも１つの移動ユニットを有するワイヤレスローカルエリアネットワークの無断使用を検出するための方法を提供することである。第１ネットワークトラフィックデータが移動ユニットに累積される。第２ネットワークトラフィックデータがアクセスポイントに対して累積される。第１及び第２のトラフィックデータは、コンピュータへ通信され、そしてコンピュータにおいて相関されて、非相関トラフィックデータを識別する。非相関トラフィックデータがトラフィックデータのスレッシュホールド部分を越えたときにアラーム状態が信号される。

【０００７】

本発明の別の実施形態において、ワイヤレスローカルエリアネットワークの無断使用を検出するためのシステムは、移動ユニットと、アクセスポイントと、サーバーコンピュータとを備え、第１ネットワークトラフィックデータが移動ユニットにより累積され、第２ネットワークトラフィックデータがアクセスポイントにより累積され、そして第１及び第２のトラフィックデータがサーバーコンピュータへ通信される。サーバーコンピュータは、トラフィックデータを相関して、非相関トラフィックデータを識別し、そして前記非相関トラフィックデータがあるスレッシュホールド部分を越えたときにアラーム状態が信号されるようにする。

【０００８】

第１トラフィックデータは、移動ユニットのための送信メッセージの数、送信メッセージの行先アドレス、移動ユニットのための受信メッセージの数、受信メッセージのソースアドレス、移動ユニットとアクセスポイントとの関連付け要求の記録、関連付け解除トランザクションの記録、移動ユニットにより受信されるブロードキャスト及びマルチキャストフレームの数、又は認証要求の記録を含むことができる。第２トラフィックデータは、アクセスポイントに対する送信メッセージの数、送信メッセージの行先アドレス、アクセスポイントに対する受信メッセージの数、受信メッセージのソースアドレス、移動ユニットとアクセスポイントとの関連付け要求の記録、関連付け解除トランザクションの記録、アクセスポイントにより送信されるブロードキャスト及びマルチキャストフレームの数、又は認証要求の記録を含むことができる。トラフィックデータは、周期的な間隔で、或いはコンピュータから送信されたコマンド信号に応答して、コンピュータへ送信することができる。

【０００９】

本発明によれば、プロセッサ及び無線装置を有し、コンピュータと通信するように構成された移動ユニットの改良が提供される。移動ユニットのプロセッサは、コンピュータに接続されたアクセスポイントとの通信を表わすトラフィックデータを累積し、そしてその

累積されたトラフィックデータをコンピュータへ通信するように構成される。

【００１０】

本発明は、更に別の目的と共にこれを良く理解するために、添付図面を参照して以下に詳細に説明し、そしてその範囲は、特許請求の範囲に指摘する。

【発明を実施するための最良の形態】

【００１１】

図１には、サーバー１２がワイヤードネットワーク１４を経て複数のアクセスポイント１６に接続されたワイヤレスローカルエリアネットワーク１０が示されている。このネットワーク１０は、ＩＥＥＥ規格８０２．１１のような規格プロトコルに基づいて動作して、移動ユニット１８とサーバー１２との間にワイヤレスネットワークデータ通信を与えることができる。

【００１２】

本発明は、侵入者２０がシステムを使用し又は使用しようと試みるのを検出するための方法を提供する。この方法によれば、トラフィックデータが移動ユニット１８及びアクセスポイント１６に累積され、アクセスポイントは、ここに援用する前記特許出願に述べられたように、セルコントローラ及びＲＦポートを含むことができる。理想的には、データは、特定のメッセージ及びマネージメント信号に関連し、そして相関することができる。例えば、理想的な状態では、アクセスポイント１６により送信されるメッセージの数は、移動ユニット１８により受信されるメッセージの数に等しくなければならず、又、その逆のことも言える。

【００１３】

本発明の方法による１つの構成では、アクセスポイント１６は、各移動ユニット１８へ送信されて移動ユニット１８により確認されたメッセージの数を表わすトラフィックデータを累積することができる。移動ユニット１８において、受信されて確認されたメッセージの数は、トラフィックデータとして累積される。アクセスポイント１６により累積されたトラフィックデータ及び移動ユニット１８により累積されたトラフィックデータは、周期的に、ワイヤレス及びワイヤードネットワーク１０、１４を経てのデータ通信により、コンピュータ１２へ分析のために送信される。任意の構成では、侵入サーバー２２がコンピュータ１２からトラフィックデータを受信して、その分析を実行する。データを分析するために、アクセスポイント１６により送信されたメッセージを、そのメッセージがアドレスされる移動ユニット１８により受信されて確認されたメッセージと相関させるための試みがなされる。

【００１４】

同様に、移動ユニット１８は、移動ユニット１８によりアクセスポイント１６へ送信されたメッセージを表わすトラフィックデータを累積することができ、そしてアクセスポイント１６は、アクセスポイント１６が受信して確認した各移動ユニット１８からのメッセージを表わすトラフィックデータを累積することができる。このトラフィックデータは、コンピュータ１２又は侵入サーバー２２へ分析のために送信される。

【００１５】

ネットワークを経て送信されそしてネットワークの許可されたエレメントにより受信されるメッセージ間に著しい差があり、例えば、メッセージの１０％以上を相関できない場合には、コンピュータ１２又は侵入サーバー２２が、システムへの侵入が生じたかもしれないことを信号する。これは、侵入者２０が、システムの許可されたユーザとしてそれ自身をマスクする信号を送信し又は確認したことを意味する。この１０％スレッシュホールドは、例示のために与えられたに過ぎず、最も有効なスレッシュホールドは、主として、ワイヤレスネットワークの構成に依存することに注意されたい。本発明のシステム及び方法の別の実施形態では、スレッシュホールドは、固定値でなくてもよく、ノイズ、パケット衝突、等によるトラフィックロスを考慮するように動的に調整されてもよい。

【００１６】

相関は、システム全体として又は個々のトランシーバとして評価することができる。個

々のトランシーバに基づいて評価を行うべき場合には、トラフィックデータは、受信した各メッセージのソースアドレスと、送信した各メッセージの行先アドレスとを含んでもよい。更に、トラフィックデータは、８０２．１１システムのＢＳＳ　ＩＤのように、データが収集されたトランシーバを識別するパケットにおいてコンピュータ１２又は侵入サーバー２２へ送信される。この情報で、コンピュータ１２又は侵入サーバー２２は、各々の完了したパケット、例えば、確認されたパケットのソース及び行先を相関させることができる。

【００１７】

本発明の方法の変形例において、侵入の試みに使用できるある形式のメッセージに集中して分析を行うことができる。例えば、移動ユニット１８は、その移動ユニット１８により送信される各々の関連付け要求をトラフィックデータとして記録することができる。更に、移動ユニット１８は、認証又は関連付けが各関連付け要求に対して承諾されたかどうかの情報をトラフィックデータに記録することができる。平均的な人間(man-in-the middle type)の侵入を検出するために特に重要なことは、移動ユニット１８が関連付け解除トランザクションを記録できることである。

【００１８】

トラフィックデータを相関させる目的で、各アクセスポイント１６は、移動ユニット１８から受信した関連付け要求に対応するトラフィックデータと、アクセスポイントにより遂行される関連付け又は認証の承諾、及び関連付け解除トランザクションを表わす事象とを記憶しそして送信することができる。本発明によるシステム及び方法の実施形態で収集できる他の事象は、ログインの試み、ログインの失敗、再試み、プローブ要求送信、プローブ要求受信、送信／受信されたマルチキャストフレームの数、送信／受信されたブロードキャストフレームの数、送信／受信されたデータトラフィックの数、等を含むことができる。当業者に明らかなように、本発明の範囲は、これらのデータカテゴリーしか収集しないシステム及び方法に制限されないことに注意されたい。

【００１９】

本発明による方法の更に別の構成では、移動ユニット１８は、侵入者２０がシステムに入るよう試みていることを指示する事象を記録することができる。１つのこのような事象は、侵入者２０がアクセスポイントとして見えるよう試みているブロードキャスト又はマルチキャストメッセージである。これらのメッセージは、トラフィックデータとして記録できる一方、アクセスポイント１６は、認証ブロードキャスト及びマルチキャストメッセージに対応するトラフィックデータを記録する。記録されたデータトラフィックは、相関のためにコンピュータ１２又は侵入サーバー２２へ送信される。

【００２０】

トラフィックデータは、プリセットされた周期的間隔、例えば、１時間ごとに、コンピュータ１２又は侵入サーバー２２へ送信することができる。移動ユニット１８の場合には、移動ユニットがアクセスポイントに関連付けされる間にトラフィックデータを送信することしかできない。この場合には、移動ユニット１８は、関連付けの終りに、トラフィックデータを、関連付け解除機能の一部分として送信することができる。

【００２１】

別の構成では、コンピュータ１２又は侵入サーバー２２からコマンドメッセージを受信した際にトラフィックデータを送信することができる。

【００２２】

別の構成では、侵入サーバー２２は、どの統計学的データを収集すべきかについて移動ユニット１８及び／又はアクセスポイント１６に動的に命令することができる。

【００２３】

更に別の構成では、セキュリティプロトコルを使用して、トラフィックデータをコンピュータ１２又は侵入サーバー２２に送信することができる。好ましい実施形態では、使用するプロトコルは、セキュア・ソケット・レイヤ・プロトコル（ＳＳＬ）でよいが、本発明は、このプロトコルの使用に限定されない。

【００２４】

図２は、本発明の方法を実施するのに使用できる移動ユニット１８のブロック図である。移動ユニットは、データパケットを送信及び受信するための無線装置２４と、ＩＥＥＥ規格８０２．１１のようなデータ通信プロトコルに基づいて無線装置を制御するためのプロセッサ３０とを備えている。移動ユニットは、リードオンリメモリ３４及びランダムアクセスメモリ３２を備え、これは、プロセッサ３０を含むマイクロコンピュータの一部分でもよいし、デジタル信号プロセッサの一部分でもよい。リードオンリメモリ３４は、プロセッサ３０を操作するためのプログラム命令を含み、これらの命令は、ランダムアクセスメモリ３２にトラフィックデータを累積するための命令を含む。又、プロセッサ３０は、ポータブルコンピュータ、電話、又はパーソナルデジタルアシスタントのようなホストシステム２８にもインターフェイスされる。

【００２５】

以上、本発明の好ましい実施形態を説明したが、当業者であれば、本発明の精神から逸脱せずに更に別の変更や修正がなされ得ることが明らかであり、そしてこのような変更や修正は、全て、本発明のシンの範囲内に包含されるものとする。

【図面の簡単な説明】

【００２６】

【図１】本発明の方法を実施するワイヤレスローカルエリアネットワークを示すブロック図である。

【図２】本発明による改良された移動ユニットの実施形態を示すブロック図である。

【図１】

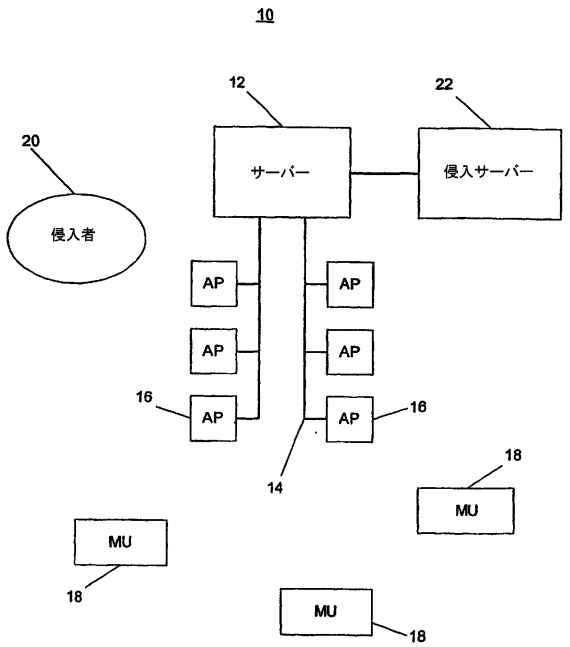

FIG. 1

【図２】

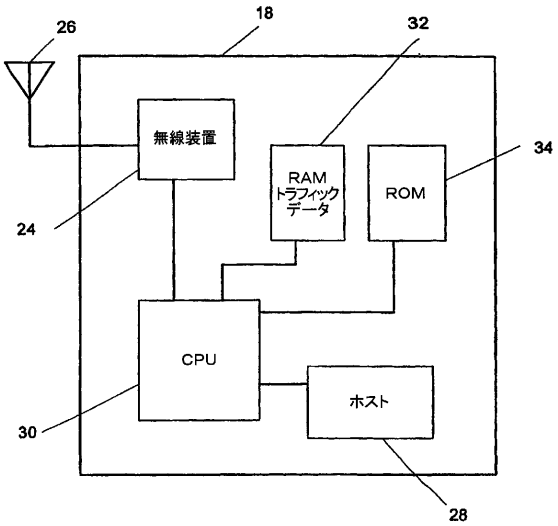

FIG. 2

フロントページの続き

(72)発明者　ワン　ファイアン　エイミー
アメリカ合衆国　ニューヨーク州　１１７８８　ホーポーグ　デヴォンシャー　ロード　９０８

審査官　田畑　利幸

(56)参考文献　米国特許出願公開第２００３／０１４２６４１（ＵＳ，Ａ１）
特開２００２－２４７６５４（ＪＰ，Ａ）
特開２００４－０１５３６８（ＪＰ，Ａ）
国際公開第０３／０８３６０１（WO，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04W　24/00
H04L　12/22
H04W　12/12
H04W　84/12