

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第4053992号
(P4053992)

(45) 発行日 平成20年2月27日 (2008. 2. 27)

(24) 登録日 平成19年12月14日 (2007. 12. 14)

(51) Int. Cl.	F I
H04 L 12/28 (2006. 01)	H04 L 12/28 3 O O M
H04 Q 7/34 (2006. 01)	H04 Q 7/04 B

請求項の数 21 (全 15 頁)

(21) 出願番号	特願2003-580963 (P2003-580963)	(73) 特許権者	390009531
(86) (22) 出願日	平成14年11月20日 (2002. 11. 20)		インターナショナル・ビジネス・マシーンズ・コーポレーション
(65) 公表番号	特表2005-522073 (P2005-522073A)		I N T E R N A T I O N A L B U S I N E S S M A S C H I N E S C O R P O R A T I O N
(43) 公表日	平成17年7月21日 (2005. 7. 21)		アメリカ合衆国10504 ニューヨーク州アーモンク ニュー オーチャードロード
(86) 国際出願番号	PCT/US2002/033648		
(87) 国際公開番号	W02003/083601	(74) 復代理人	100106699
(87) 国際公開日	平成15年10月9日 (2003. 10. 9)		弁理士 渡部 弘道
審査請求日	平成16年11月18日 (2004. 11. 18)	(74) 復代理人	100077584
(31) 優先権主張番号	10/107, 794		弁理士 守谷 一雄
(32) 優先日	平成14年3月27日 (2002. 3. 27)	(74) 代理人	100086243
(33) 優先権主張国	米国 (US)		弁理士 坂口 博
(31) 優先権主張番号	10/209, 568		
(32) 優先日	平成14年7月30日 (2002. 7. 30)		
(33) 優先権主張国	米国 (US)		

最終頁に続く

(54) 【発明の名称】 ワイヤレス・アクセス・ポイントのための方法、装置、およびプログラム・プロダクト

(57) 【特許請求の範囲】

【請求項 1】

アクセス・ポイントと該アクセス・ポイントを介してネットワークに接続されるワークステーション・コンピュータ・システムと前記ネットワークに接続されるサーバ・コンピュータ・システムとにおける方法であって、

データを通過させて前記ネットワークと交換可能とする前記アクセス・ポイントを前記ワークステーション・コンピュータ・システムが監視するステップと、

前記ワークステーション・コンピュータ・システムが前記アクセス・ポイントに関する情報を前記サーバ・コンピュータ・システムに送信するステップと、

前記サーバ・コンピュータ・システムが不正アクセス・ポイントを識別するステップと

10

、
前記識別した不正アクセス・ポイントを通るトラヒックを監視するステップと、
を備える、方法。

【請求項 2】

前記識別した不正アクセス・ポイントの地理的位置を求めるステップを更に備える、請求項 1 に記載の方法。

【請求項 3】

前記識別した不正アクセス・ポイントを通る監視されたトラヒックにトラヒック・フィルタリングを適用するステップを更に備える、請求項 1 または請求項 2 に記載の方法。

【請求項 4】

20

トラヒック・フィルタリングを適用するステップは、前記識別した不正アクセス・ポイントを介した前記ネットワークへのアクセスを拒否するステップを備える、請求項 3 に記載の方法。

【請求項 5】

前記不正アクセス・ポイントを識別するステップは、監視したアクセス・ポイントの識別子 (identity) を認証済みアクセス・ポイントのデータベースと比較するステップを備える、請求項 1 ないし請求項 4 の 1 項に記載の方法。

【請求項 6】

前記識別した不正アクセス・ポイントに識別されたネットワーク・リソースのアクセスおよび使用の課金を蓄積するステップを更に備える、請求項 1に記載の方法。

10

【請求項 7】

データを通過させてネットワークと交換可能とするアクセス・ポイントを監視するステップと、

不正アクセス・ポイントを識別するステップと、

前記識別した不正アクセス・ポイントを通るトラヒックを監視するステップと、

不正アクセス・ポイントのための製造業者、モデルおよびデフォルト・パスワードを決定することによって前記不正アクセス・ポイントの識別に応答するステップと、

前記デフォルト・パスワードを用いて前記不正アクセス・ポイントをアドレッシングし、それに対するアクセスを得る際に、前記不正アクセス・ポイントを認証済みアクセス・ポイントに再構成するステップと

20

を備える、方法。

【請求項 8】

複数のコンピュータ・デバイスに対してアクセス可能なアクセス・ポイントを検出し、検出したアクセス・ポイントの識別子 (identity) を前記サーバ・コンピュータ・システムに報告するため、前記コンピュータ・デバイスの各々に装備を行うことにより、データを通過させてネットワークと交換可能とするアクセス・ポイントを監視するステップと、

監視したアクセス・ポイントの識別子 (identity) を認証済みアクセス・ポイントのデータベースと比較して不正アクセス・ポイントを識別するステップと、

前記識別した不正アクセス・ポイントを通るトラヒックを監視するステップとを備える方法。

30

【請求項 9】

前記監視するステップは、前記ネットワークにおけるノードに維持されたノード識別接続テーブルに対する最近のエントリについて前記ノードにクエリを行うステップを備える、請求項 8に記載の方法。

【請求項 10】

前記監視するステップは間欠的および周期的に実行される、請求項 8 または請求項 9に記載の方法。

【請求項 11】

前記監視するステップは所定の一定の間隔で実行される、請求項 10に記載の方法。

【請求項 12】

前記監視するステップはランダムな不規則の間隔で実行される、請求項 10に記載の方法。

40

【請求項 13】

データを通過させてネットワークと交換可能とするアクセス・ポイントを監視するステップと、

不正アクセス・ポイントを識別するステップと、

前記識別した不正アクセス・ポイントを通るトラヒックを監視するステップと、

全てが前記識別した不正アクセス・ポイントの検出を報告する複数のコンピュータ・デバイスの位置を比較することにより前記識別した不正アクセス・ポイントの地理的位置を求めるステップを備える、方法。

50

【請求項 14】

ワークステーション・コンピュータ・システムと、

前記ワークステーション・コンピュータ・システムに接続され、前記ワークステーション・コンピュータ・システムとネットワークとの間の通信チャネルを提供するネットワーク・インタフェースと、

前記ワークステーション・コンピュータ・システムにアクセス可能にストアされたプログラムであって、

前記ワークステーション・コンピュータ・システム上で実行されると、前記ワークステーション・コンピュータ・システムと協働して、データを通してネットワークと交換可能とするアクセス・ポイントを監視し、不正アクセス・ポイントの識別を支援し、識別した不正アクセス・ポイントを通るトラヒックを監視するプログラムと、

ワークステーション・コンピュータ・システム上で実行されると、前記ワークステーション・コンピュータ・システムと協働して、前記ネットワーク・インタフェースを介してアクセス可能なアクセス・ポイントを識別するアクセス・ポイント識別プログラムと、

前記ワークステーション・コンピュータ・システム上で実行されると、前記アクセス・ポイント識別プログラムおよび前記ワークステーション・コンピュータ・システムと協働して、前記ネットワーク・インタフェースを介してアクセスされたアクセス・ポイントの識別子 (identity) をサーバ・コンピュータ・システムに報告する報告プログラムとを備える、装置。

【請求項 15】

コンピュータ・システムと、

前記システムに接続され、前記システムとネットワークとの間の通信チャネルを提供するネットワーク・インタフェースと、

前記コンピュータ・システムにアクセス可能にストアされたプログラム命令であって、前記コンピュータ・システム上で実行されると、

前記コンピュータ・システムと協働して、データを通してネットワークと交換可能とするアクセス・ポイントを監視し、

不正アクセス・ポイントの識別を支援し、

識別した不正アクセス・ポイントを通るトラヒックを監視し、

不正アクセス・ポイントのための製造業者、モデルおよびデフォルト・パスワードを決定することによって前記不正アクセス・ポイントの識別に応答し、

前記デフォルト・パスワードを用いて前記不正アクセス・ポイントをアドレッシングし、それに対するアクセスを得る際に、前記アクセス・ポイントを認証済みアクセス・ポイントに再構成するプログラム命令とを備える装置。

【請求項 16】

実行されると、前記識別した不正アクセス・ポイントに識別されたネットワーク・リソースのアクセスおよび使用の課金を蓄積するプログラム命令を更に備える、請求項 15 に記載の装置。

【請求項 17】

アクセス・ポイントとサーバ・コンピュータ・システムが接続されたネットワークに前記アクセス・ポイントを介して接続が可能なコンピュータ・システムであって、

データを通して前記ネットワークと交換可能とするアクセス・ポイントを監視する手段と、

前記サーバ・コンピュータ・システムにおいて不正アクセス・ポイントを識別するために前記アクセス・ポイントに関する情報を送信する手段と、

前記識別された不正アクセス・ポイントを通るトラヒックを監視する手段とを備える、コンピュータ・システム。

【請求項 18】

アクセス・ポイントとサーバ・コンピュータ・システムが接続されたネットワークに前記アクセス・ポイントを介して接続が可能なコンピュータ・システムに、

データを通過させて前記ネットワークと交換可能とするアクセス・ポイントを監視する機能と、

前記サーバ・コンピュータ・システムにおいて不正アクセス・ポイントを識別するために前記アクセス・ポイントに関する情報を送信する機能と、

前記識別された不正アクセス・ポイントを通るトラフィックを監視する機能と
を実現させる、コンピュータ・プログラム。

【請求項 19】

コンピュータ読み取り可能媒体と、

コンピュータ・システムにアクセス可能に前記媒体にストアされたプログラム命令であって、システム上で実行されると有効となり、

データを通過させてネットワークと交換可能とするアクセス・ポイントを監視し、不正アクセス・ポイントを識別し、

前記識別した不正アクセス・ポイントを通るトラフィックを監視し、

不正アクセス・ポイントのための製造業者、モデルおよびデフォルト・パスワードを決定することによって前記不正アクセス・ポイントの識別に応答し、前記デフォルト・パスワードを用いて前記不正アクセス・ポイントをアドレッシングし、それに対するアクセスを得る際に、前記アクセス・ポイントを認証済みアクセス・ポイントに再構成する、プログラム命令と

を備える、プログラム・プロダクト。

【請求項 20】

前記プログラム命令は、有効となって前記識別した不正アクセス・ポイントに識別されたネットワーク・リソースのアクセスおよび使用の課金を蓄積する命令を更に備える、請求項 19 に記載のプログラム・プロダクト。

【請求項 21】

前記プログラム命令は、有効となって監視したアクセス・ポイントの識別子 (identity) を認証済みアクセス・ポイントのデータベースと比較する命令を更に備える、請求項 19 または請求項 20 に記載のプログラム・プロダクト。

【発明の詳細な説明】

【技術分野】

【0001】

以下の記載は、かかる通信ネットワークにおいて用いられるネットワーク・データ通信およびスイッチおよびルータの知識を前提としている。特に、この記載は、ネットワーク動作を層 (layer) に分割するネットワーク・アーキテクチャの I S O モデルに精通していることを前提とする。

【背景技術】

【0002】

以下の記載は、かかる通信ネットワークにおいて用いられるネットワーク・データ通信およびスイッチおよびルータの知識を前提としている。特に、この記載は、ネットワーク動作を層 (layer) に分割するネットワーク・アーキテクチャの I S O モデルに精通していることを前提とする。I S O モデルに基づく典型的なアーキテクチャでは、物理経路または媒体である層 1 (時に、「L 1」とも示す) を信号が通過し、層 2、3、4 等を通して層 7 まで上る。この最後の層は、ネットワークにリンクされたコンピュータ・システム上で実行するアプリケーション・プログラミング層である。この文書において、L 1、L 2 等の言及は、ネットワーク・アーキテクチャの対応する層を示すことを意図している。また、この開示は、かかるネットワーク通信においてパケットおよびフレームとして知られるビット・ストリングの基本的な理解を前提としている。

【0003】

802.11 規格は、2.4ギガビット帯域幅空間におけるワイヤレス・ローカル・エ

10

20

30

40

50

リア・ネットワークのために電気電子学会（I E E E : Institute of Electrical and Electronics Engineers Inc.）が生成した仕様ファミリである。802.11は、コンピュータおよびその他の電子デバイスを、極めて高速で、わずらわしい配線を用いずに、相互におよびインターネットへと接続するための方法として考えることができる。これは、基本的に、どのようにコードレス電話をその基地局にリンクするかを高速化したものである。802.11により、電子デバイスは、約300フィートの距離を毎秒11メガビットで互いに通信を行うことができ、これは企業における一部の有線ネットワークより速い。

【0004】

802.11を用いたデバイスは、Wi-Fiとしてますます知られるようになっており、比較的安価である。ネットワーク・アクセス・ポイントは、約500ドルで購入することができ、範囲内の全ての802.11装備デバイスの通信を調整し、このアクセス・ポイントをリンクするインターネットおよび／またはイントラネットへのリンクを与える。ラップトップ・コンピュータまたは他のデバイスをネットワークに「プラグ（plug）」インするカードは、100から200ドルである。一部の個人用通信デバイスは、追加のカードを必要とせずに802.11通信に対応可能である。ワイヤレス802.11カードおよびアクセス・ポイントは、コンピュータ供給業者から飛ぶように売られている。人々は、802.11規格の製品との容易な接続性を望み、これを発見した。また、かかるネットワークは、アドホック・ワイヤレス・ネットワーク、場合によってはモバイル・アドホックネットワークすなわちMANETという更に正式な名前で見られる。

【0005】

ワイヤレス速度を適度な価格で提供することは、いつでも／どこでもの通信を好む世界にとって大きな意味を持つ。Wi-Fiは、急速に普及している。大学生は、寮や食堂でネットワークをセットアップしている。サン・フランシスコの一部では、人々は、近所をカバーする802.11ネットワークを構築している。とりわけ、スターバックス社（Starbucks Corp.）、ユナイテッド・エアライン社（United Airlines Inc.）およびホリデイ・イン社（Holiday Inn）は、店舗、空港のラウンジ、およびホテルで、顧客が常時接続状態を望むのに対応して、802.11ネットワークをインストールしている。シナージ・リサーチ・グループ（Synergy Research Group）によると、2000年には、ワイヤレス・ローカル・エリア・ネットワークを用いる人の数は150パーセント増大したことが報告されている。アリゾナ州スコッツデールに本社を置くマーケット・リサーチの会社Cahners In-Stat Groupは、ビジネスにおけるワイヤレス・データのユーザ数は、今日の660万人から、2006年までには3900万人以上に増えると予測している。この傾向を促進するのは、中小企業の全社員のうち約4分の1がモバイル・ワーカー（mobile worker）であり、労働時間のうち少なくとも20パーセントを会社から離れて過ごすという事実である。ワイヤレス電子メールは、彼らの最も重要なニーズであり、このため、常にオンの電子メール機能を有するモバイル・コンピューティング製品は、高い売上げを維持している。2002年初めには、毎日25,000人から50,000人の人々が802.11ネットワークをインストールし管理すると予想された。

【0006】

ワイヤレスの流行が、家庭用ネットワーキング市場にも広がっていくことは避けられないであろう。主な理由は価格である。アクセス・ポイント、ワイヤレス・ネットワークに接続する機器、および、PCとアクセス・ポイントとの間のリンクを形成するネットワーク・インタフェース・カードすなわちNICのコストが下がっている。この低価格が購買者の目を引き、このため家庭用市場は2001年の第4四半期に20パーセント成長した。

【0007】

802.11の後に続く技術が現れつつある。1つは、超広帯域無線技術すなわちUWB（ultra-wide band radio technology）であり、これは、低電力で広スペクトル技術を用いて、極めて高速でデータを転送する。UWBは、おそらく802.11よりも10倍の速度であるが、ここで論じたのと同じ障害のいくつかがある。別のものは、無線周波数

10

20

30

40

50

機能を、システム中央プロセッサおよびネットワーク・プロセッサ等の他の機能を実行するチップ上に直接含ませることである。

【発明の開示】

【発明が解決しようとする課題】

【0008】

そして、問題があり、本当のジレンマを生じさせる。ここでも、情報技術の管理者およびユーザは、使用の容易さとセキュリティの必要性との間で板ばさみになっている。今日のワイヤレスには2つの大きな問題があり、これは将来にまで残ると予想され得る。1つは、何らセキュリティ対策を講じずに実施されることがあまりに多いということである。もう1つは、難しい設定等が不要のセキュリティの選択肢は、顧客がスイッチ・オンした場合、完全に無駄だということである。Gartner Dataquestによると、コンピュータ・ネットワークを用いる全企業のうち約30パーセントは、公式または非公式に、何らかの種類のワイヤレス・ネットワークを有する。更に、企業または隣のカフェがワイヤレス・ネットワークを有する場合、その企業でトラブルが起こる恐れがある。

【0009】

ワイヤレスは非常に広く開かれているので、実際、新しい科学技術者のオリンピック・スポーツを生んだ。戦争ドライブ (war driving) である。このゲームは、いくつかの潜在的ターゲットを発見することができるかを見るものである。プレイするのに必要なのは、ラップトップ・コンピュータ、ワイヤレスPCカード、およびいくつかのソフトウェアだけである。戦争ドライブは、技術出版物および技術ウェブ・サイトにおいて広く論じられてきており、定期的に行われている。退屈したティーンエージャーおよび技術マニアの新しい趣味は、ワイヤレス・アクセス・ポイントを捜し求めて、アンテナとラップトップ・コンピュータにひもで結びつけたGPSとを持ってドライブして回ることである。ほとんどの人は、悪意からネットワークに攻撃するのではなく、ネットワークおよびそれに含まれるファイルにアクセスすることを慎重に避けるが、全ての人がそう礼儀正しいわけではない。

【0010】

戦争ドライブで用いられる人気のあるツールの1つ、NetStumblerは、アクセス・ポイントの名前、暗号化が可能か、および多数の他の情報ビットを教えてくれる。また、NetStumblerは、企業に接続された非公式で不正のアクセス・ポイントを識別しようとする管理者にとっても利用できるツールである。あるユーザは、シリコン・バレーでハイウェイ101を短時間ドライブする間に20のアクセス・ポイントを見つけた。別のユーザは、ロンドンの金融街を移動し、空のプリングルス (Pringles) ポテト・チップ缶から作ったアンテナを用いて、30分でほぼ60のアクセス・ポイントを見つけることができた。Kismetは、NetStumblerと同じ機能の多くを含む、Linux用ワイヤレス・ネットワーク・スニファ (sniffer) である。AirSnortは、暗号鍵を回復しようとするLinuxベースのツールである。これらおよび多くのツールは、インターネットで自由に入手可能である。

【0011】

企業は、メイン・インターネット・ゲートウェイの保護について用心深いはずであるが、企業の周辺は、ワイヤレスに拡大している。何人のユーザが、VPNまたは他のリモート・アクセス手段を介して内部ネットワークにアクセスするか？ それらのユーザのうち何人が家庭にワイヤレス・ネットワークを有するか？ それらは安全か？ そうでない場合、どんなにメイン・インターネット・ゲートウェイが安全であるかに関わらず、内部ネットワークは傷つきやすい。802.11およびUWBが安全に作られ、安全と証明されるまで、賢いネットワーク管理人は心配し続けることになる。特に、その認証を得ていない従業員がサービスの良いコンピュータ用品店に行き、ワイヤレス・アクセス・ポイントを買い、それを職場に持っていき、電源を入れて雇用者のイントラネットに接続するような場合がある。

【0012】

今日のアクセス・ノードまたはポイントは、一般に層2で機能し、層3アドレッシングの知識を持たないが、それらが接続するエッジ・ルータは、層3アドレッシングの全知識を有することを注記しておくのは重要である。技術が進歩するにつれて、アクセス・ポイントに組み込まれる機能はいっそう多くなっている。例えば、元来これらは、完全に無電源製品であったIBM8228等の過度に単純化した「有線コンセントレータ(wiring concentrators)」であった。今日、これらのアクセス・ポイントは、通常、ワイヤレスであれ有線であれ、層2の全知識、または媒体アクセス制御(MAC:Medium Access Control)、それらに接続されるデバイスのアドレスを有する層2スイッチである。

【0013】

将来、低コストのネットワーク・プロセッサ(文献において別個に記載したような)の出現により、これらのアクセス・ポイントは、特にそれらに接続されるエンド・ステーションのIPアドレスを知ることに関して、完全に層3対応になるであろう。むしろ、今日、エッジ・ルータは、すでにそれに直接接続されているエンド・デバイスのIPアドレスのこの知識を有する。今日、全てのエッジ・ノードおよびいくつかのアクセス・ノードは、シンプル・ネットワーク管理プロトコル(SNMP:Simple Network Management Protocol)として既知のメッセージング・プロトコルを用いて、ネットワークを介して、ネットワーク管理コンソールに接続する機能を有する。将来、全てのアクセス・ノードはこの機能を有するであろう。

【課題を解決するための手段】

【0014】

本発明は、1つの目的として、ネットワーク管理者またはマネージャが、非公式または不正のアクセス・ポイントの存在を識別することを可能とし、これによってネットワークのセキュリティ向上を支援する。更に別の目的は、不正のアクセス・ポイントの地理的な位置を決定することを可能とすることである。また、本発明は、1つの目的として、ネットワーク管理者またはマネージャが、非公式または不正のアクセス・ポイントのアクティビティを制御することを可能とする。また、本発明は、1つの目的として、ネットワーク管理者またはマネージャが、非公式または不正のアクセス・ポイントの制御を自動化することを可能とし、これによってネットワークの操作性の向上を支援する。また、本発明は、1つの目的として、ネットワーク管理者またはマネージャが、非公式または不正のアクセス・ポイントを介してネットワークと交換したアクティビティの決算または請求を制御することを可能とし、これによってネットワークの金融セキュリティの向上を支援する。

【0015】

これらの目的は、データを通過させてネットワークと交換可能とするアクセス・ポイントを監視し、不正のアクセス・ポイントを識別し、アクセス・ポイントを介したあるアクティビティを制御する方法、装置、およびプログラム・プロダクトによって達成される。

【0016】

本発明の目的のあるものはすでに述べ、他のものは、添付図面と関連付けた場合に、説明が進むにつれて明らかになる。

【発明を実施するための最良の形態】

【0017】

本発明について、本発明の好適な実施形態を示す添付図面を参照して、以下で更に十分に説明するが、後に続く説明の最初に、当業者は、本発明の良好な結果を達成しながら、ここに記載する本発明を変更可能であることは理解されよう。従って、以下の説明は、本発明の限定としてではなく、当業者を対象とする幅広い教示の開示として理解されるものとする。

【0018】

先に簡単に述べたように、802.11規格の普及に伴う問題は、ネットワークを管理する責任を担う情報技術(IT)企業が知らないうちに、誰かが、ネットワークに対するワイヤレス・アクセス・ポイントを容易にセットアップすることができることである。これが問題である理由は、かかるアクセス・ポイントは、恐らく(そして通常は)誤って構

10

20

30

40

50

成され、このため、ネットワークへのアクセスおよびそこに存在するデータを世界中に与えてしまうからである。

【0019】

かかるアクセス・ポイントが確立されると、ネットワークにクエリを行うことによって、それらがあるか、またはそれらがどのように構成されているかを判定することは難しい場合がある。これは、展開するアクセス・ポイントの具体的なタイプおよびネットワーク洗練度によって異なる可能性がある。これについては、以下で更に十分に説明する。単純なアクセス・ポイントに対する現在の解決策は、ノートブックまたはパーソナル・デジタル・アシスタント（PDA: personal digital assistant）等のモバイル・コンピューティング・デバイス上でNet Stumbler（または同様のソフトウェア）を用い、信号強度測定を用いていつユーザがアクセス・ポイントに近づいているかまたは離れているかを決定し、インデクスに手動で参照を行ってアクセス・ポイントが不正の「非公式なもの」であるかを判定することである。これには、ある人が不正のアクセス・ポイントを発見するために定期的に設備全体を調べる必要がある。

【0020】

本発明は、ユーザがあちこち調べることを必要とせずに、不正のアクセス・ポイントを迅速に突き止めるためのいくつかの方法を提供する。

【0021】

ここで具体的に図面を参照すると、図1はネットワーク10を示し、これは、サーバ・コンピュータ・システム11、ワイヤレスまたは有線とすることができる複数の認証済みアクセス・ポイント12、および、複数のワークステーション・コンピュータ・システム14を有する。各ワークステーション・コンピュータ・システム14は、ワイヤレス接続を介して、または、恐らくは有線接続、または双方を介して、ネットワークに結合されている。設備の大きさおよび範囲に応じて、管理されるネットワークには、複数種類のシステムおよび複数種類の接続が混在する場合がある。ワークステーションは、ノートブック・コンピュータ・システム、パーソナル・デジタル・アシスタント・システム、高度機能電話、デスクトップまたはミニタワー・システム、またはアクセス・ポイントを介してネットワーク10にアクセスすることができる他のデバイスとすることができる。

【0022】

ネットワーク10に対するアクセスは、認証済みのワイヤレス・アクセス・ポイント15を介して、および、例示したネットワークでは、不正のまたは非公式ワイヤレス・アクセス・ポイント16を介して行われる場合がある。非公式アクセス・ポイント16は、情報技術管理の知識も許可もなく行動する個人またはグループによって確立された可能性がある。本発明のいくつかの目的に従って、非公式アクセス・ポイント16の検出および位置付けは、達成されるべき目標である。

【0023】

本発明によれば、ワークステーション14のうち複数または全てでなくても、少なくとも1つに、ネットワークに対するワイヤレスすなわち無線周波数接続のための設備を備える。また、これまたはこれらのワークステーションは、Net Stumbler等の監視ソフトウェアをインストールしており、これはシステムが通信を行うことができる全てのワイヤレス・アクセス・ポイントに関する情報を検出し収集することができる。更に、本発明によれば、システム（複数のシステム）は、監視プログラムが収集した情報をネットワーク10およびサーバ・コンピュータ・システム11に送信することができる報告ソフトウェアもインストールしている。図2は、ここで論じている本発明の態様に従ってワークステーション14上にインストールされたソフトウェアの機能を概略的に示す。

【0024】

最小の数の監視および報告ソフトウェアを用いることが望ましい場合、この数を、稠密集合（dense set）として数学的に知られるものまで減らすことができる。すなわち、非公式アクセス・ポイントが位置する可能性がある全地点に十分に近いシステム集合であり、少なくとも1つのシステムが非公式なものを検出する。小さいビルまたは領域では、単

10

20

30

40

50

一のシステムで稠密集合を提供することができる。もっと大きい領域では、図1に示すような複数のシステムがいっそう望ましい。

【0025】

本発明では、ワークステーションが検出したアクセス・ポイントに関する収集された情報は、信号強度に関する情報を含むことが考えられる。また、本発明では、監視ソフトウェアは、連続的とは異なり、周期的に実行可能であることも考えられる。このため、ソフトウェアは、1時間に1度または1日に1度、通常の就業時間中に実行して、ワークステーションの他の使用に過剰な負担をかけないようにすることができる。監視ソフトウェアの実行には、ネットワーク・インタフェース・カード（NIC：network interface card）またはワイヤレス・インタフェースを異なるモードに一時的にセットして情報を収集し、次いでインタフェースをリセットして通常の動作が継続するようにする必要がある。これは、ユーザの全員でなくても、ほとんどが気づかないように、十分に素早く実行可能である。また、信号強度測定を適切に校正可能とするため、監視には、検知されたアクセス・ポイントのアクティビティの初期チェックが含まれる場合がある。

10

【0026】

単一のワークステーションを用いて監視を行うことにより、2つのデータ・ポイントを提供する。すなわち、非公式アクセス・ポイントがあるか否か、および非公式アクセス・ポイントの信号強度である。この説明では、後に、多数の監視ステーションを用いることの潜在的な利点について説明する。

【0027】

20

監視が行われて情報が収集されると、情報はネットワークを介してサーバ11に報告される。送信される情報は、暗号化されるか、または不適切なアクセスに対して他の方法で保護することができる。サーバ・システムは、報告された情報を受信するソフトウェアをインストールしており、認証済みのアクセス・ポイントのリストを維持し、報告された情報をリストと比較する。サーバ・システムは、これによって、図1のポイント16等、監視ワークステーションの1つの通信範囲内にある非公式または不正のアクセス・ポイントを識別する。また、サーバ・システムは、報告された信号強度に関する情報をストアする。

【0028】

責任を担うIT企業は、各ワークステーション14の位置を知っており、または、図1のポイント15および16等の報告されたアクセス・ポイントの信号強度を分析することによって、その位置を求めることができる（ワークステーションがモバイルである場合）。この情報から、および非公式アクセス・ポイントの検出の報告された信号強度から、非公式アクセス・ポイントの位置を決定することができる。図3は、本発明のいくつかの態様に従ってサーバ・システム11上にインストールされたソフトウェアの機能を概略的に示す。

30

【0029】

本発明では、ネットワークに特に接続されていないワイヤレス・アクセス・ポイントを監視対象の領域中に分散させて設ける等の取り組みによって、説明する動作を改善可能であると考えられる。かかるダミー・アクセス・ポイントは、相対信号強度に関する追加情報を提供し、認証済みアクセス・ポイントからいくぶん離れて位置するポイントを突き止めるのに役立てることができる。更に、固定またはモバイルのワークステーションの通常分布からいくぶん離れている可能性のある領域を監視する目的のため、ワークステーションとして非アクティブである監視ステーションを、同様に、監視対象の領域中に分散させることができる。監視ステーションおよびアクセス・ポイントについて、情報を選択的に収集し、分析のための追加データ・ポイントを与えることができる。かかる他のクライアントに関する情報は、監視または報告することができ、サーバ・システムは、かかる情報を用いて、監視システムならびに非公式および認証済みのアクセス・ポイントを位置付ける場合もあり、または位置付けない場合もある。

40

【0030】

50

ワークステーションおよびサーバ・システムの協働により、本発明が実施する方法では、データを通過させてネットワークと交換可能とするアクセス・ポイントの監視が行われ、不正アクセス・ポイントを識別し、識別された不正アクセス・ポイントの位置を求める。この前に、複数のコンピュータ・デバイスに対してアクセス可能なアクセス・ポイントを検出し、検出したアクセス・ポイントの識別子 (identity) をサーバ・コンピュータ・システムに報告するため、デバイスの各々に装備を行う。監視は、アクセス・ポイントの可用性を間欠的および周期的に決定することを含み、所定の一定の間隔でまたはランダムな不規則な間隔で監視を行うことによって、アクセス・ポイントの可用性を間欠的および周期的に決定することができる。不正アクセス・ポイントの識別は、監視したアクセス・ポイントの識別子 (identity) を認証済みアクセス・ポイントのデータベースと比較することによって行われる。識別した不正アクセス・ポイントの位置の決定は、識別した不正アクセス・ポイントの検出を報告した複数のコンピュータ・デバイスの位置を比較することによって行われる。

10

【0031】

ここで、この考察において、アクセス・ポイントに関する情報は本質的に受動的に得られる。かかる情報の受動的獲得は、以下で説明するようにアクセス・ポイントを再構成することが望ましい場合、困難を生じる恐れがある。受動的に得られる情報には、MACアドレス、信号強度、およびアクセス・ポイントについての少なくとも何らかの構成データが含まれるが、アクセス・ポイントに対する制御を確立するのに必要な場合があるIPアドレスは含まない。

20

【0032】

本発明では、非公式アクセス・ポイントとして識別されるアクセス・ポイントを更に識別可能なステップ・シーケンスが考えられる。「聞いている (listening)」クライアントは、アクセス・ポイントを介したトラフィックの監視を続け、パケット・ストリームを監視して、アクセス・ポイントに接続するクライアントのIPアドレスを求めるか、またはDHCPが行われるのを見る。このように収集した情報をサーバに供給し、アクセス・ポイントが実際に企業のイントラネット内にあるか否かを判定するために十分な情報をサーバに与える。アクセス・ポイントが企業のイントラネット内にある場合、サーバは、接続したクライアントにメッセージを送信して、このクライアントに、アクセス・ポイントのIPアドレスを決定するためのアクティブな手段を用いるように指示する。これは、質問技法によって行われ、特別なICMPパケットをMACアドレスに向けたアクセス・ポイントに送信するが、サブネットに同報通信する。アクセス・ポイントは、そのIPアドレスによって応答し、これは次いでサーバに送信される。

30

【0033】

ここに記載した機能に適切なソフトウェアは、図7に示すディスク等のコンピュータ読み取り可能媒体を用いてユーザに分配することができ、これに含ませることができるソフトウェアは、ワークステーション・システムまたはサーバ・システム上で実行されると、ソフトウェアがインストールされているシステムのタイプに応じて適宜、図2および3に示すシーケンスをシステムに実行させる。

【0034】

40

図4に、本発明の他の態様による例示的なアクセス・ポイントを示す。アクセス・ポイントは、全体として20で示す。アクセス・ポイント20は、ネットワーク10におけるノードであり、有線接続またはインタフェース21を介していくつかの他の要素に、および、おそらくワイヤレス接続またはインタフェース22を介して他に接続されている。アクセス・ポイント20は、内部に接続テーブル24を格納している。2つのレベルのインタフェース21、22間に介在させてネットワークにテーブルを格納することができる。

【0035】

業界のコンサルタントは、ネットワーク・プロセッサ（ここでは「NP」とも呼ぶ）を、以下の機能のうち1つ以上を実行可能なプログラム可能通信集積回路として規定している。

50

パケット分類—アドレスまたはプロトコル等、既知の特徴に基づいてパケットを識別すること。

パケット変更—IP、ATM、または他のプロトコルに適合するようにパケットを変更すること（例えばIP用のヘッダ内でタイム・トゥ・ライブ（time-to-live）・フィールドを更新すること）。

キュー／ポリシ管理—特定用途のためのパケットのキューイング（queuing）デキューイング（de-queuing）、およびスケジューリングの設計戦略を反映させること。

パケット転送—スイッチ・ファブリック（switchfabric）上でデータを送信および受信すること、ならびにパケットを適切なアドレスに転送またはルーティングすること。

【0036】

10

この規定は、初期のNPの基本的な特徴を正確に記述したものであるが、NPの完全な潜在的な機能および利点は、まだ実現されていない。ネットワーク・プロセッサは、以前はソフトウェアにおいて処理したネットワークング・タスクをハードウェアにおいて実行可能とすることによって、広範囲の用途において、帯域幅を増し、レイテンシの問題を解決することができる。更に、NPは、並列分散処理およびパイプライン処理設計等のアーキテクチャによって、速度向上を与えることができる。これらの機能は、効率的なサーチ・エンジンを可能とし、スループットを増大させ、複雑なタスクを素早く実行することができる。

【0037】

20

ネットワーク・プロセッサは、PCにとってのCPUと同じように、ネットワークにとって基本的なネットワーク構築ブロックになると予想される。NPが提供する典型的な機能は、実時間処理、セキュリティ、ストアおよび転送、スイッチ・ファブリック接続性、ならびにIPパケット処理および学習機能である。NPはISO層2ないし5を対象とし、ネットワークに固有のタスクを最適化するように設計されている。

【0038】

プロセッサ・モデルNPは、多数の汎用プロセッサおよび特殊化論理を組み込んでいる。供給業者は、この設計に合わせて、適時の費用対効果の大きい方法で変化に対応することができる、スケーラブルで柔軟な解決策を提供する。プロセッサ・モデルNPは、より低いレベルの統合で分散処理を可能とし、スループット、柔軟性、および制御を向上させる。プログラム可能であることによって、新たなASIC設計を必要とすることなく、新しいプロトコルおよび技術に容易に移行することができる。プロセッサ・モデルNPにより、ネットワーク機器のベンダは、払い戻し不可能な技術的コストの低下および市場までの時間の改善から利益を得る。

30

【0039】

従来のネットワーク動作によれば、ネットワーク10のノードは、通信を確立することができる他のノードのアドレスを含む接続テーブルを維持する。かかるテーブルを維持するノードの特徴に応じて、テーブルは、ルーティングまたは信頼できる隣接テーブルと称することができる。かかるテーブルは、検出された接続性の同報通信通知に基づいて、周期的にリフレッシュされる。本発明は、かかるルーティングまたは信頼できる隣接テーブルおよびインテリジェント・ノードが上述のような処理を実行する機能を利用する。

40

【0040】

これを背景として、考察している本発明の態様では、周期的またはランダムに、中央サイトのネットワーク管理コンソールが、SNMPまたはいっそう洗練された技法を用いて、ワイヤレス・アクセスまたはワイヤレス・エッジ・ノードに質問可能であることが考えられる。この質問の目的は、層3ルーティング・テーブルに対する最新の追加を判定し、サーバ・アクセスの拒否等、異常なアクティビティについて、最新のエン트리およびそれらのトラヒック・フローを監視することである。あるいは、質問が層2デバイスのものである場合、最も最近のエン트리および上述のように監視したトラヒックについて、「信頼できる隣接テーブル」に質問する。

【0041】

50

即座のアクションが望ましい場合、SNMPおよび他の技法によって、層2または層3のフィルタ・テーブル（適宜）は、すぐに、ネットワークに対するアクセスを拒否するようセットすることができる。侵入者を把握する試みが望ましい場合、上述の信号強度技法を用いて、非公式アクセス・ポイントの位置を決定することができる。侵入者を「止める（stall）」ために、フィルタリング・テーブルを層2または層3ケースにセットして、非公式アクセス・ポイントと交換されるトラヒックを安全なサーバにルーティングすることができ、これは侵入者にネットワークにアクセスを得ていると感じさせる一連のスクリプトによってプログラムすることができる。

【0042】

管理プログラムおよびアクセス・ポイントの機能に応じて、多くの環境において、識別した「非公式」アクセス・ポイントの製造業者を識別することが可能となる。製造業者を識別することで、適切に構成したテーブルから、かかるアクセス・ポイントのデフォルト構成およびパスワードにアクセスすることが可能となる。デフォルト・パスワードを有し、ネットワーク上に「ポイントを確立する」職員によって代替的なインストールが行われないと仮定すると、管理システム・ソフトウェアは、アクセス・ポイントのセキュリティ機構にアクセスし、アクセス・ポイントをルーティングおよび信頼できる隣接テーブルの再構成以上に再構成することができる。更に具体的には、アクセス・ポイントを、認められた公式のアクセス・ポイントに変換することができ、従来のネットワーク管理制御を適用する。これらの管理制御は、アクセスに課金する等の金融制御、および、システム管理決定パスワードの設定等のセキュリティ制御を含むことができる。

【0043】

本発明の重要な特徴は、このため、エッジ・ルータのルーティング・テーブルまたはアクセス・ポイントの信頼できる隣接テーブルに質問し、これらのテーブルにランダムまたは決定的な方法で質問して新しいエントリがあるか判定し、これらの新しいエントリからのトラヒック・フローを監視してそれらがサービス拒否等のネットワークとの問題を有するかを決定し、ルーティングおよび信頼できる隣接テーブルによって、侵入者のトラヒックをフィルタリングし、テーブルへの適切なエントリによってそれらを遮断するか、またはそれらのフローを安全なサーバにルーティングしてイベント・シーケンスを初期化して侵入者を把握する。それらのステップは、図5に例示するようなものである。

【0044】

更に、本発明の他の目標と共に、アクセス・ポイントの識別子（identity）は、再構成されると、課金を割り当てるポートのレジスタに追加され、使用およびアクセスの課金はそのポート識別子（identity）に対して蓄積される。図6に、関連ステップを示す。

【0045】

ここで再び、上述したように、サーバ11等のシステム上で実行しながらこれらのステップを実施するのに有用なプログラムは、図7に示すディスク等、適切なコンピュータ読み取り可能媒体上に書き込むことによって分配することができる。

【0046】

図面および明細書において、本発明の好適な実施形態について述べ、特定の用語を用いたが、このように与えた記載は、限定の目的でなく、一般的かつ記述的な意味でのみ専門用語を用いる。

【図面の簡単な説明】

【0047】

【図1】設備内にインストールされたネットワークの概略図であり、ワークステーション・コンピュータ・システムおよびサーバ・コンピュータ・システムを含み、これに不正のアクセス・ポイントが接続されている。

【図2】図1のネットワークにおいて実行されるステップを示す簡略化フローチャートである。

【図3】図1のネットワークにおいて実行されるステップを示す簡略化フローチャートである。

10

20

30

40

50

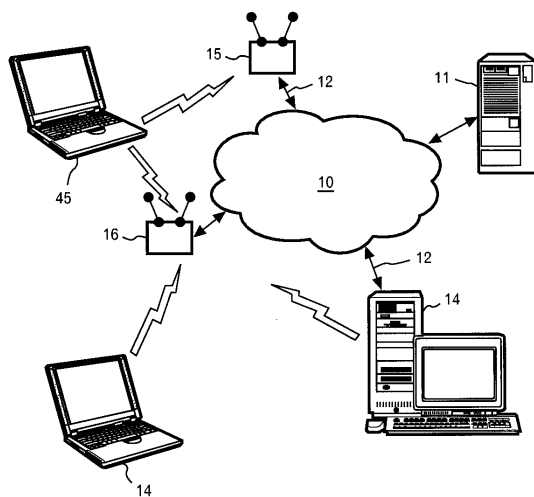
【図４】図１に示すネットワークにおいて機能可能であるようなワイヤレス・アクセス・ポイントの概略図であり、ネットワーク・プロセッサを組み込んでいる。

【図５】図１のネットワークにおいて実行されるステップを示す簡略化フローチャートである。

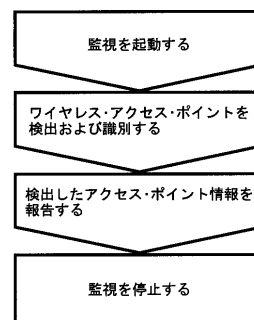
【図６】図１のネットワークにおいて実行されるステップを示す簡略化フローチャートである。

【図７】図１のシステムの適切な１つで実行して図２、３、５、６のステップを実施する場合に有効なプログラムを有するコンピュータ読み取り可能媒体の図である。

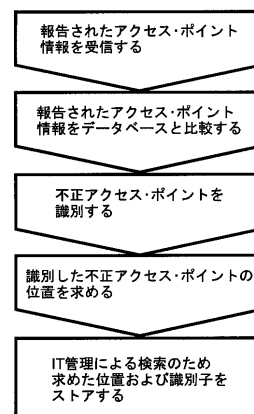
【図１】



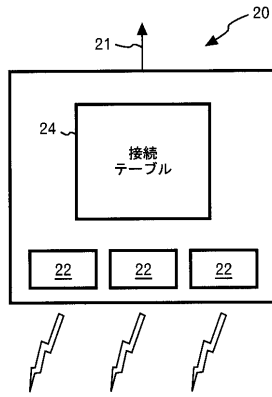
【図２】



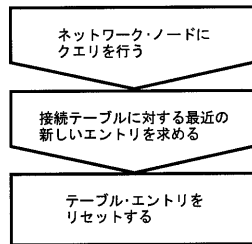
【図３】



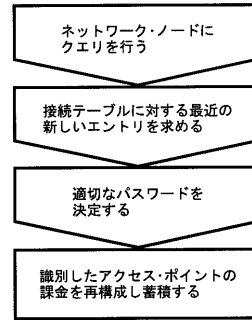
【図 4】



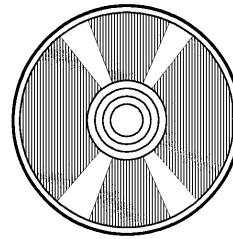
【図 5】



【図 6】



【図 7】



フロントページの続き

- (31)優先権主張番号 10/208,281
(32)優先日 平成14年7月30日(2002.7.30)
(33)優先権主張国 米国(US)
(31)優先権主張番号 10/208,277
(32)優先日 平成14年7月30日(2002.7.30)
(33)優先権主張国 米国(US)
- (74)代理人 100091568
弁理士 市位 嘉宏
(74)代理人 100108501
弁理士 上野 剛史
- (72)発明者 チャレナー、デイヴィッド、シー
アメリカ合衆国 2 7 6 1 5 ノースカロライナ州ローリー ハンティング・リッジ・ロード 7 1
3
(72)発明者 カンプ、ギャリー、エム
アメリカ合衆国 2 7 5 2 3 ノースカロライナ州アペックス ダイアル・ドライブ 2 4 0 2
(72)発明者 ノエル、フランシス、イー、ジュニア
アメリカ合衆国 2 7 7 0 7 ノースカロライナ州ダラム スワスマア・ロード 4 0 2 1
(72)発明者 サフォード、デイヴィッド、アール
アメリカ合衆国 1 0 5 0 9 ニューヨーク州ブルースター インディアン・ヒル・ロード 4 1
(72)発明者 シャーレス、ダグラス、エル
アメリカ合衆国 1 0 5 4 9 ニューヨーク州マウント・キスコ 私書箱 4 1
(72)発明者 ファン・ドールン、レーンデルト、ピー
アメリカ合衆国 1 0 5 9 5 ニューヨーク州ヴァルハラ シーダー・ストリート 2 1

審査官 矢頭 尚之

- (56)参考文献 特開 2 0 0 1 - 0 2 5 0 6 7 (JP, A)
特開平 1 1 - 2 8 9 3 2 8 (JP, A)
特開 2 0 0 2 - 7 2 3 4 (JP, A)
国際公開第 0 2 / 7 5 3 3 9 (WO, A1)
特開 2 0 0 3 - 2 7 4 4 5 4 (JP, A)

(58)調査した分野(Int.Cl., DB名)

H04L 12/28
H04Q 7/34
G06F 13/00