(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2008-538470
(P2008-538470A)
(43)公表日　平成20年10月23日(2008.10.23)

| (51)Int.Cl. | | F I | | | テーマコード（参考） |
|---|---|---|---|---|---|
| H04M 3/42 | (2006.01) | H04M | 3/42 | E | 5K030 |
| G06F 13/00 | (2006.01) | G06F | 13/00 | 610Q | 5K201 |
| H04L 12/58 | (2006.01) | H04L | 12/58 | 100F | |

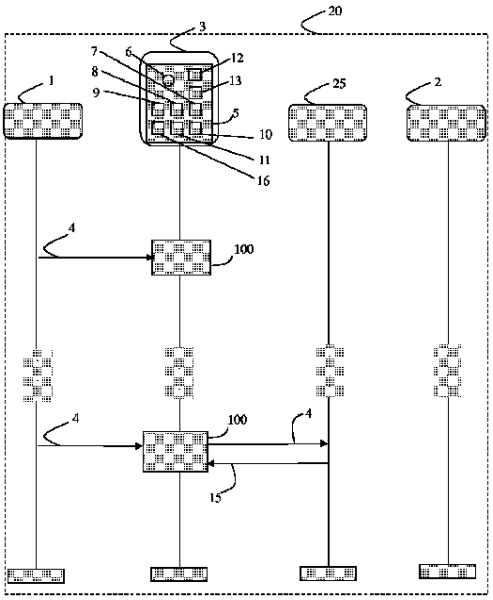
審査請求 未請求　予備審査請求 未請求　（全 20 頁）

(21)出願番号　特願2008-505940 (P2008-505940)
(86)(22)出願日　平成18年4月10日 (2006.4.10)
(85)翻訳文提出日　平成19年12月10日 (2007.12.10)
(86)国際出願番号　PCT/FR2006/050324
(87)国際公開番号　WO2006/108989
(87)国際公開日　平成18年10月19日 (2006.10.19)
(31)優先権主張番号　0503710
(32)優先日　平成17年4月13日 (2005.4.13)
(33)優先権主張国　フランス(FR)

(71)出願人　591034154
フランス　テレコム
フランス国　パリ　７５０１５　プラス　ダルレ　６
(74)代理人　100064908
弁理士　志賀　正武
(74)代理人　100089037
弁理士　渡邊　隆
(74)代理人　100108453
弁理士　村山　靖彦
(74)代理人　100110364
弁理士　実広　信哉
(72)発明者　ベルトラン・マシュー
フランス・２２５６０・プルムール－ボドゥ・リュ・デュ・ブール・３１
最終頁に続く

(54)【発明の名称】未承諾の音声情報の送信に対抗する方法

(57)【要約】
本発明は、送信エンティティから宛先エンティティへのパケット伝送ネットワークにおける未承諾情報の送信に対抗する方法を提供し、前記未承諾情報は、音声タイプの情報であり、且つ、コールセットアップステージを含むコール期間で送信され、前記コールセットアップステージの期間ではコールシグナリングメッセージが前記ネットワークにおいて送信され、その後、進行中のコールステージが続き、この進行中のコールステージの期間では前記未承諾情報が送信されることを特徴とし、且つ、当該方法は、前記コールの期間で未承諾情報を検出するステップを含むことを特徴とする。有利には、本方法は、前記コールの期間で未承諾情報の検出に続いて起動される反応ステップを含む。また、本発明は、未承諾情報の送信に対抗するためのシステムに関する。



【特許請求の範囲】
【請求項１】
送信エンティティ（１）から宛先エンティティ（２）へのパケット伝送ネットワーク（２０）における未承諾情報の送信に対抗する方法であって、
前記未承諾情報は、音声タイプの情報であり、且つ、コールセットアップステージを含むコール期間に送信され、前記コールセットアップステージの期間ではコールシグナリングメッセージが前記ネットワークにおいて送信され、その後、進行中のコールステージが続き、この進行中のコールステージの期間では前記未承諾情報が送信されることを特徴とし、
且つ、当該方法は、
前記コールの期間に未承諾情報を検出するステップ（１００）を含むことを特徴とする方法。
【請求項２】
未承諾情報は、前記送信エンティティから到来する前記コールシグナリングメッセージ（４）と、前記送信エンティティから到来する前のコールに関連するコールコンテキスト（６）を分析することにより検出される請求項１記載の方法。
【請求項３】
未承諾情報は、前記コールセットアップステージにおけるコールに関する多くのコールシグナリングメッセージを或る期間（７，９）にわたってカウントし、前記コールセットアップステージにおけるコールの数を、超えてはならない閾値（８，１０）と比較することにより検出される請求項２記載の方法。
【請求項４】
未承諾情報は、コールの構成における自動化ロジック（１１）を或る期間（１２）にわたって識別することにより検出される請求項２記載の方法。
【請求項５】
未承諾情報は、前記コールがセットアップされた後のステージで送信されたパケットにおける共通特性を認識することにより検出される請求項１記載の方法。
【請求項６】
前記コールの期間で未承諾情報の検出の後に起動される反応ステップを含むことを特徴とする請求項１乃至５の何れか１項記載の方法。
【請求項７】
前記反応は、未承諾情報を送信するものとして識別されたコールをブロック（５１）することにある請求項６記載の方法。
【請求項８】
前記反応は、未承諾情報を送信する前記エンティティ（１）によって単位時間あたりに送信されるコールの数を制限することにある請求項６記載の方法。
【請求項９】
前記反応は、未承諾情報を送信するものとして識別されたコールの全部（４）又は一部（５６）をネットワークエンティティ（５５，５８）にリダイレクトすることにある請求項６記載の方法。
【請求項１０】
前記送信エンティティに関連するユーザーに知られていない未承諾情報を送信しているワームまたはウィルスに感染した前記送信エンティティに関連する端末を浄化するためのサービスを提供するための請求項１記載の方法の使用。
【請求項１１】
未承諾情報の送信に対抗するためのシステムであって、当該システムは、パケット伝送ネットワーク（２０）と、送信エンティティ（１）と、宛先エンティティ（２）と、前記ネットワークにおけるエンティティ（３，３３）とから構成され、当該システムは、前記未承諾情報が音声タイプの情報であると共にコールセットアップステージを含むコール期間で送信され、前記コールセットアップステージの期間でコールシグナリングメッセージ

が前記ネットワークにおいて送信され、その後に進行中のコールステージが続き、この進行中のコールステージの期間で前記未承諾情報が送信されることを特徴としており、
　且つ、前記ネットワークにおけるエンティティは、
　前記コールの期間で未承諾情報を検出するように構成された検出モジュール（５）を備えたことを特徴とするシステム。
【請求項１２】
　前記ネットワークにおけるエンティティ（３，３３）は、前記未承諾情報の検出に続いて反応するように構成された反応モジュール（５０）を備えたことを特徴とする請求項１１記載のシステム。
【請求項１３】
　前記検出モジュール（５）は、前記送信エンティティから到来する前のコールに関するコールコンテキスト（６）と前記コールシグナリングメッセージを分析することを特徴とする請求項１１記載のシステム。
【請求項１４】
　パケット伝送ネットワークのエンティティ（３，３３）のメモリにインストールされるように構成されたコンピュータプログラムであって、当該プログラムは、送信エンティティによって送信されたコールに関するコールコンテキストを処理するための命令と、前記コールセットアップステージでコールシグナリングメッセージを分析するための命令と、未承諾情報を送信するものとしてコールを識別するための命令とを含むことを特徴とするコンピュータプログラム。
【請求項１５】
　前記パケット伝送ネットワークのエンティティ（３，３３）のメモリにインストールされるように構成されたコンピュータプログラムであって、当該プログラムは、前記送信エンティティから到来すると共に未承諾情報を送信するものとして識別されるコールに作用するための命令を含むことを特徴とする請求項１４記載のコンピュータプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
　本発明は、遠隔通信(telecommunication)に関する。更に詳しくは、本発明は、ＶｏＩＰ(Voice over IP)としても知られているＩＰ技術の分野における未承諾情報(unsolicited information)の送信に対抗(combat)する技術に関する。
【背景技術】
【０００２】
　現今、ユーザーに対して未承諾情報を送りつける慣行が増加している。通常はコマーシャルの類の電子メッセージ又は電子メールメッセージを、それを要求してもいないユーザーに送信することが問題である場合、その送信の慣行はスパム(spam)と呼ばれている。スパムは紛れもない厄介物(plague)であり、ビジネスに対する生産性の著しい損失の原因として考えられる。この慣行は、また、インスタントメッセージの分野でも増加しており、この分野では、（“spam on instant messaging”から）スピム(spim)として知られる。同じ慣行が、ＶｏＩＰ技術の分野でも同様に起こる可能性があり、この分野では、（“spam over Internet telephony”から）スピット(spit)として知られる。従って、この慣行は、インターネット電話のアプリケーションのユーザーに影響を及ぼす。ＩＰ電話(IP telephony)は、急速に成長している音声通信電話であり、単音声(single voice)及びデータのネットワーク上でマルチメディア通信を提供するためのＩＰデータネットワークを使用する。
【０００３】
　ＶｏＩＰデータネットワークにおける未承諾情報またはスピットの送信は深刻な問題を引き起こす。ユーザーが未承諾情報を受信することはさておき、スピットは、ユーザーに関連する音声メールボックスの飽和の原因となり、最悪の場合には、大量のメッセージの送信に続いてネットワーク機器が利用不能になる。ネットワーク機器を利用不能にするス

ピットの送信は、サービス拒絶攻撃(denial of service attack)として知られている。
【０００４】
スピットは、スピットを送信するワームまたはウィルスに感染した端末から、その端末のユーザーが気づくことなく、故意あるいは意図せずに送信される。
【０００５】
従って、未承諾情報を受信することからユーザーを保護し、ネットワークの有効性を妨害する過負荷からインターネットサービスプロバイダーまたはオペレータのネットワークを保護するために、スピットに対抗(combat)することが要請されている。
【０００６】
現在、スピットに対抗するネットワークレベルの解決策は存在しない。スピットは、ＶｏＩＰインフラにおいてのみ可能性がある。この新興のインフラは、開発が始まったばかりであり、現在のところはほとんどユーザーがいない。従ってほとんどスピットの事例は報告されていない。これらの事例に固有の問題は差し当たり比較的大したことはないので、ほとんど研究がなされておらず、解決策の提案は極めて少ない。
【０００７】
スパムに対抗するために使用される技法は直接的には適用できない。スパムに対抗するために現在広く使用されている技法のひとつの例は、メールが送信された後、それが受信される前に、メッセージングサーバーまたはクライアント端末上でフィルターを使用することにより、望まない電子メールをブロックすることである。フィルターはキーワードを認識することができ、そしてさらに高機能なフィルターは、トレーニングステージの後に、電子メールの一部がスパムである確率をその電子メールが含むキーワードに基いて計算することができる。どのようなタイプのフィルターが使用されようとも、キーワードの認識に基づくその技法は、音声メッセージに適用することは困難である。さらには、その技法はネットワークにおけるメールの巡回を阻止できない。
【発明の開示】
【発明が解決しようとする課題】
【０００８】
本発明の目的は、ＶｏＩＰ遠隔通信ネットワークにおける未承諾の音声情報を検出する方法を提案することである。本発明の他の目的は、スピットの検出に続く反応ステップを含む方法を提案することである。本発明の更なる目的は、スピットのソースとして識別されたエンティティに関する情報を収集するための手段を提供すると共に、そのエンティティに関連する端末が、その端末のユーザーに気づかれていないスピットを送信しているワームまたはウィルスに感染していることを検証する浄化サービス(a decontamination service)を提供するための技術的手段を提供することである。
【課題を解決するための手段】
【０００９】
本発明の第１の態様は、送信エンティティから宛先エンティティへのパケット伝送ネットワークにおける未承諾情報の送信に対抗する方法であって、前記未承諾情報は、音声タイプの情報であり、且つ、コールセットアップステージを含むコール期間に送信され、前記コールセットアップステージの期間ではコールシグナリングメッセージが前記ネットワークにおいて送信され、その後、進行中のコールステージが続き、この進行中のコールステージの期間では前記未承諾情報が送信されることを特徴とし、且つ、当該方法は、前記コールの期間に未承諾情報を検出するステップを含むことを特徴とする。
【００１０】
未承諾情報を検出するステップは反応に先行して行われる。本検出方法の利点は、それがコールセットアップステージにおいて、故にネットワークにおいて未承諾情報が巡回して目的のエンティティに到達する前に、使用されることにある。
【００１１】
有利には、未承諾情報は、前記送信エンティティから到来する前記コールシグナリングメッセージと、前記送信エンティティから到来する前のコールに関連するコールコンテキ

ストを分析することにより検出される。

【００１２】

前記コールシグナリングメッセージを分析することは、コールセットアップステージにおけるコールに関連する情報、例えば、前記コールのソースである送信エンティティに関する情報の収拾を可能にする。この分析は、ネットワークにおいて達成され、次のような多くの利点を有する。

・スピットのソースである悪意のあるユーザーを識別し、その場所を特定することができる。

・端末のユーザーに知られていないスピットを送信するウィルスまたはワームに感染したその端末を識別し、その場所を特定することができる。

・検出がネットワークにおいて達成されるので、このスピットの検出は、ユーザーまたはユーザーの端末に特有の構成を条件としない。

・もし、オペレータがスピットのソースであるユーザーに関する情報を合法的に開示する必要があるのであれば、ネットワークのオペレータは、このような情報を取得する。

【００１３】

第１の実施では、未承諾情報は、前記コールセットアップステージにおけるコールに関する多くのコールシグナリングメッセージを或る期間にわたってカウントし、前記コールセットアップステージにおけるコールの数を、超えてはならない閾値と比較することにより検出される。

【００１４】

通常の電話コールをするのと同様に、マルチメディアコールをすることは、ダイアリング、リンギング、ピックアップ、会話、或いは音声メールボックスにメッセージを預けることを含む複数のステップを含む。前記ステップは時間を要する。分析モードは、この遅延を技術的に考慮することに対応し、もし、送信エンティティが同時または短期間に複数のコールを送信するのであれば、コールの送信は自動化されている。実際には、一つの送信エンティティが二つの連続したコールを宛先エンティティに送信することはあり得るが、同じ宛先エンティティに５個または１０個の連続したコールを送信することは稀である。

【００１５】

他の実施では、未承諾情報は、コールの構成における自動化ロジックを或る期間にわたって識別することにより検出される。

【００１６】

この実施の利点は、コールをなすために使用されるアドレスのリストの自動スキャンを検出するためのネットワークにおける技術的手段を提供することである。

【００１７】

有利には、本方法は、前記コールの期間で未承諾情報の前記検出の後に起動される反応ステップを含む。

【００１８】

前記反応は、例えば、未承諾情報を送信するものとして識別された前記コールをブロックすることにある。

【００１９】

これに代えて、又はこれに加えて、前記反応は、未承諾情報を送信する前記エンティティによって単位時間あたりに送信されるコールの数を制限することにある。

【００２０】

これに代えて、又はこれに加えて、前記反応は、未承諾情報を送信するものとして識別された前記コールの全部又は一部をネットワークエンティティにリダイレクトすることにある。

【００２１】

上記反応ステップの利点は多く、ネットワークオペレータの顧客であるユーザーと、ネットワークオペレータ自身との両者に対して有益であり、次のようである。

・スピットはネットワークで巡回しない。
・ユーザーは、未承諾の広告メッセージに煩わされない。
・ユーザーの音声メールボックスは、未承諾メッセージによって溢れない。
・オペレータは、そのネットワーク機器の可用性を改善する。
・オペレータは、その顧客をスピットから保護し、これによりそのブランドイメージを強化する。
・最後に、さらに一般的には、本発明は、スピットからなる障害を低減することによりＶｏＩＰ技術の拡大および伝播に寄与する。

【００２２】
本方法は、有利には、前記送信エンティティに関連するユーザーに知られていない未承諾情報を送信しているワームまたはウィルスに感染した前記送信エンティティに関連する端末を浄化するためのサービスを提供することができる。

【００２３】
本発明は、また、未承諾情報の送信に対抗するためのシステムにあり、当該システムは、パケット伝送ネットワークと、送信エンティティと、宛先エンティティと、前記ネットワークにおけるエンティティとから構成され、当該システムは、前記未承諾情報が音声タイプの情報であると共にコールセットアップステージを含むコール期間で送信され、前記コールセットアップステージの期間でコールシグナリングメッセージが前記ネットワークにおいて送信され、その後に進行中のコールステージが続き、この進行中のコールステージの期間で前記未承諾情報が送信されることを特徴としており、且つ、前記ネットワークにおけるエンティティは、
前記コールの期間で前記未承諾情報を検出するように構成された検出モジュールを備えたことを特徴とする。

【００２４】
本システムは、有利には、前記未承諾情報の次の検出に続いて反応するように構成された反応モジュールを備える。

【００２５】
本発明は、さらに、ＩＰ伝送ネットワークの第１のエンティティのメモリにインストールされるように構成されたコンピュータプログラムにあり、当該プログラムは、送信エンティティによって送信されたコールに関するコールコンテキストを処理するための命令と、前記コールセットアップステージにおけるコールシグナリングメッセージを分析するための命令と、未承諾情報を送信するものとして前記コールを識別するための命令とを含むことを特徴とする。

【００２６】
本発明のコンピュータプログラムは、有利には、前記送信エンティティから到来すると共に未承諾情報を送信するものとして識別されるコールに作用するための命令を含む。

【発明を実施するための最良の形態】

【００２７】
本発明の多くの詳細と利点は、添付の図面を参照して一つの特定の実施例の記述を読めばより良く理解され、それは非限定的な例により提供され、その例における図は次のようである。
図１は、ＶｏＩＰコールセットアップの期間で交換されるＳＩＰシグナリングメッセージを分析する複数のモードに基づくスピット検出方法を示す。
図２は、複数の反応モードに基づくと共にスピットの検出に続く反応方法を示す。
図３は、スピット検出及び反応方法がＳＩＰベースのＶｏＩＰネットワークに配置されたアプリケーションサービスにおいて実施される本発明の第１構成に対応するアーキテクチャを示す。
図４は、スピット検出及び反応方法がネットワークにおけるアプリケーションプローブにおいて実施される本発明の第２構成に対応するアーキテクチャを示す。

【００２８】

ＶｏＩＰ技術を管理する基準は、例えば、限定的には、ＩＴＵ－Ｔ(International Telecommunications Union-Telecommunications standardization)からのＨ．３２３プロトコルと、ＩＥＴＦ(Internet Engineering Task Force)の主導で開始されたＳＩＰ(Session Initiation Protocol)を含み、ここで、前者のＨ．３２３プロトコルについてはhttp://www.ietf.org/rfc/rfc3261.txtを参照され、後者のＳＩＰについてはhttp://www.ietf.orgを参照されたい。シグナリングプロトコルＳＩＰは、ＯＳＩ(Open System Interconnection model)のアプリケーションレイヤ（レイヤ７）に属する。それは、他のプロトコル、例えば、限定的には、実時間でマルチメディアデータを伝送するためのＲＴＰ(Real Time Protocol)と、シグナリングを転送するためのＴＣＰ(Transmission Control Protocol)に依存し、ＲＴＰ(Real Time Protocol)についてはhttp://www.ietf.org/rfc/rfc1890.txtを参照されたい。ＩＰ電話、より正確にはそのシグナリング伝送部は、また、“ピアツーピア(peer to peer)”（Ｐ２Ｐ）の概念を用いて達成され、それは、クライアントのみの役割またはサーバーのみの役割を果たさないが、これら両方の様式で動作するエレメントを有するタイプの通信プロトコルを言い、一つの同じ時間ではネットワークの他のノードのクライアント及びサーバーの両方である。

【００２９】

ＳＩＰは、クライアント／サーバーモードに基づくマルチメディアコールを処理(manage)し、即ち、ＳＩＰダイアログの期間で交換されるメッセージは問い合わせ(enquiries)または応答(responses)である。ＳＩＰメッセージは、進行中のコールに関する情報、例えば、限定的にはコールの識別子と、“ＦＲＯＭ”と呼ばれるメッセージのフィールドにおけるメッセージを送信するエンティティに関する情報と、“ＴＯ”と呼ばれるメッセージのフィールドにおける宛先エンティティに関する情報とを含む。問い合わせに対する応答は、その問い合わせのものと同じように埋められたフィールドを含み、具体的には、コール識別子と、“ＦＲＯＭ”フィールドと、“ＴＯ”フィールドを含む。ＳＩＰ応答は、具体的には、問い合わせがどの程度処理されたかを示す応答ステートコードを含む。このステートコードは、エラーメッセージまたはサクセスメッセージとしてＳＩＰ問い合わせに応答して受信されるメッセージを識別する。ＳＩＰダイアログの期間で、問い合わせを送信しても応答を受信しない送信エンティティによって起動されるマルチメディアコールは、ＴＣＰによって実施されるＴＣＰタイムアウト機構によって終了され、ＳＩＰはその機構に依存し、即ち、タイムアウトは、タイマー装置として、問い合わせサービスを送信するときに送信エンティティに設定されるタイムアウトは、タイマー装置として機能し、上記問い合わせに対して応答がない場合にタイムアウトが満了すれば、前記コールは終了される。

【００３０】

ＳＩＰベースのマルチメディアコールに含まれる送信及び宛先エンティティは、ユーザーと端末を識別するＵＲＬ ＳＩＰアドレス(Uniform Resource Locator Session Initiation Protocol address)と呼ばれるアドレスによって指定され、それは、“user_information@domain”という形をとり、ここで、“user_information”は、ネームまたは電話番号に対応し、“domain”は、ドメインネーム又はＩＰアドレスに対応する。ＶｏＩＰコールにおいて、ユーザーは、通常の電話コールでの場合と同様に、コールしている、又はコールされたパーティである。端末は、ＶｏＩＰ端末であり、例えば、ＰＤＡ(Personal digital assistant)、ＰＣ(Personal Computer)、またはＩＰ電話である。

【００３１】

ＶｏＩＰコールは、ＩＰパケット伝送ネットワークを使用する。従って、ネットワークは、送信エンティティが宛先エンティティに送信する情報に対応するデータとコールシグナリングメッセージの両方を伝送する。通常の電話コールと同様に、ＶｏＩＰコールは、種々のステージを通じて進行し、例えば、限定的には、送信エンティティがコンタクトを希望していることを宛先エンティティが通知されていないにもかかわらず、送信エンティティが、コンタクトを希望する宛先エンティティのＵＲＬ ＳＩＰアドレスを供給する期間であるコールセットアップステージを通じて進行する。このステージでは、コールシグ

ナリングメッセージは、コールに必要なリソースを予約し、宛先エンティティがビジーまたはフリーであるかどうかを判定するために、ネットワークにおいて巡回する。コールがセットアップされた後のステージにおいて、宛先エンティティは何れかとコンタクトがとられ、何故ならば、コールが通知されたときにピックアップされるためであり、または、宛先エンティティと関連する音声メールボックスが活性化され、宛先エンティティがピックアップされたように振る舞うためである。コールがセットアップされた後のステージにおいて、送信エンティティと宛先エンティティとの間でセットアップされた会話に関連するデータのパケットはネットワークを巡回する。

【００３２】

図１を参照すれば、ＶｏＩＰ(Voice over IP)タイプのＩＰネットワーク２０は、ＶｏＩＰコールセットアップに関与する。送信エンティティ１は、宛先エンティティ２へのＶｏＩＰコールを起動する。送信及び宛先エンティティは、ネットワーク２０の不可欠な部分を形成すると考えられる。検出モジュール５は、第１ネットワークエンティティ３にインストールされ、またはネットワーク２０の第１エンティティ３と対話するリモートマシンにインストールされる。検出モジュール５は、第１ネットワークエンティティ３のメモリに格納されたプログラムであり、それは本発明の検出方法を実行するための命令を含んでいる。検出モジュール５は、マルチメディアコールに参加するために送信エンティティ１によって宛先エンティティ２に送信されるインビテーション(invitation)に対応するＳＩＰコールシグナリングメッセージINVITE ４の第１ネットワークエンティティ３による受信に続いて、ＶｏＩＰコールセットアップステージにおいて起動される。メッセージは、“FROM”フィールドにおける送信エンティティ１に関する情報と、“TO”フィールドにおける宛先エンティティ２に関する情報とを含む。ステップ１００において、検出モジュールの活性化に続いて、メッセージ４のフィールドが分析される。この分析は、送信エンティティ１から受信される先行のメッセージに関する情報を含む第１ネットワークエンティティ３によって処理(manage)されるコールコンテキスト６を使用する。この分析は、現在のメッセージをスピットであるものとして、またはスピットでないものとして識別し、以下に説明する４つの異なるモードで達成される。検出モジュール５は、少なくとも、次の４つの分析モードのうちの一つを実施する。

【００３３】

第１のモードでは、分析は次のように達成される。検出モジュール５は、送信エンティティ１から到来するＳＩＰコールシグナリングメッセージINVITE ４をカウントする。もし、検出モジュール５で規定された第１期間(time period)７について、送信エンティティ１から受信されたＳＩＰコールシグナリングメッセージINVITE ４の数が、検出モジュール５に規定された第１閾値８を超えれば、送信エンティティ１からのコールの送信が自動化されたと考えられ、且つ、送信エンティティ１から到来するメッセージがスピットとして処理されると考えられる。自動化されたコール送信は、任意的には、スピットを送信することに相当し、なぜなら、実際には、幾つかのエンティティは、メッセージの送信を自動化することが許可されるからである。上記エンティティは、同時に複数のコールを送信することが許可されたエンティティのホワイトリストと呼ばれるリストにリストアップされる。上記エンティティは、例えば、大量の警報(bulk alert)または情報メッセージを送信した政府系機関である。ホワイトリストにリストアップされたエンティティによるメッセージの大量送信はスピットとして処理されない。この第１の実施では、ネットワークエンティティ３によって処理(manage)されるコールコンテキストは、送信エンティティ１によって送信される各コールについてのタイムスタンプとコール識別子を含む。

【００３４】

第２のモードでは、分析は次のように達成される。検出モジュール５は、検出モジュール５に規定された第２期間９の間に送信エンティティ１から宛先エンティティ２への連続的なコールをカウントする。もし、コールの数が、検出モジュール５に規定された第２閾値１０を超えれば、送信エンティティからのコールの送信が自動化され、それ故に送信エンティティに関連する端末から到来するメッセージがスピットとして処理され得ると考え

られる。この第２のモードでは、第１ネットワークエンティティ３によって処理されるコールコンテキストは、少なくとも、送信エンティティ１によって送信される各コールについて宛先エンティティ２のＩＤ(identity)と、コールタイムスタンプと、コール識別子とを含む。

【００３５】

第３のモードでは、分析は次のように達成される。検出モジュール５は、宛先モジュール５に規定された第３期間１２の間に送信エンティティ１によって送信されるＶｏＩＰコールの宛先アドレスを構成するようにして自動化ロジック１１の使用を検出する。自動化ロジックの使用は、例えば、ＳＩＰコールシグナリングメッセージINVITE ４の“TO”フィールドで指定されるコールされたユーザー識別子におけるシーケンシャルロジックの使用に相当し、それは、ユーザーネームのアルファベット式のディレクトリをスキャンすることにより選択されることができる。他の種類の自動化ロジックは、極めて多くのコールにわたる一定のコール継続期間(a constant call duration)を検出することにより検出される。この第３のモードでは、第１ネットワークエンティティ３によって処理されるコールコンテキストは、少なくとも、送信エンティティ１によって送信される各コールについて宛先エンティティ２のＵＲＬ ＳＩＰアドレスと、コールタイムスタンプと、コール識別子とを含む。

【００３６】

第４のモードでは、分析は次のように達成される。検出モジュール５は、存在しない宛先エンティティをコールする試みに続いて、ネットワーク２０のＶｏＩＰルーティングエレメント２５から到来すると共に第１ネットワークエンティティ３によって受信されるエラーメッセージ１５の数を、検出モジュール５に規定された第４期間１３の間にカウントする。このような環境の下で、ＳＩＰコールシグナリングメッセージINVITE ４のフィールド“TO”は埋められるが、ここで現れる情報は、ネットワーク２０に存在するどのエンティティにも対応しない。従って、第４の分析モードは、ステートコードがエラーに対応するところの多くのメッセージをカウントし、もし、その数が検出モジュールに規定された第３閾値１６を超えれば、送信エンティティからのコールの送信が自動化されたと考えられ、従ってそのエンティティから到来するメッセージがスピットとして処理されると考えられることにある。この第４のモードでは、第１ネットワークエンティティ３によって処理されるコールコンテキストは、少なくとも、フェイルする送信エンティティ１によって送信される各コールについてのコールタイムスタンプとコール識別子とを含む。

【００３７】

第１、第２、第３および第４の期間は異なり、または同一であり得る。同様に、第１、第２および第３の閾値は異なり、または同一であり得る。

【００３８】

上述の４つの検出モードは独立である。それらは、補完的に使用されてもよい（即ち、一つのモードが単独で使用され、あるいはそれ以上のモードが組み合わされて使用される）。

【００３９】

コールシグナリングの分析を用いて、本検出方法は、ウィルスまたはワームが端末に感染しているために故意または意図せずにスピットを送信しているエンティティを識別するための技術的手段を提供し、上記端末は、上記エンティティに関連したものであると共に、上記端末のユーザーに知られずにスピットを送信しているものである。スピットを送信しているエンティティを識別する情報は、上記エンティティに関連するユーザーが故意にスピットを送信していることを証明すれば、その後の可能性な合法的なアクションを容易化し、または、そのエンティティに関連する端末がワームまたはウィルスに感染していれば、浄化サービスが提供されることを可能にする。

【００４０】

図２を参照すると、スピット反応モジュール５０は、ネットワーク２０の第２ネットワークエンティティ３３において実施される。或いは、反応モジュール５０は、ネットワー

ク２０の第２ネットワークエンティティ３３と情報をやり取りするリモートマシンにおいて実施される。反応モジュール５０は、第２ネットワークエンティティ３３のメモリに格納されたプログラムであり、それは、本発明の反応方法を実行するための命令を含む。反応モジュール５０は、図１を参照して説明されるように、検出モジュール５によるスピットの検出に続いて起動される。本発明の検出モジュール５及び反応モジュール５０は、本発明との関連で説明されるもの以外のモジュールまたはエンティティによるスピットの検出が反応モジュールを起動することができるという意味において独立である。一つの特定の実施において、モジュール５０及び５は、同一のネットワークエンティティにおいて実施される。

【００４１】

１または２以上の反応モードは、反応モジュール５０の起動に続いて、ステップ２００において実施される。反応モジュール５０は、次の反応モードのうちの少なくともひとつを実施する。

【００４２】

第１の反応モードでは、送信エンティティ１によって起動されると共に検出モジュールによってスピットのソースとして識別されたコールはブロック（５１）される。送信エンティティから受信されるＳＩＰコールシグナリングメッセージINVITEは、ネットワーク２０によってルーティングされない。第１の実施では、反応モジュール５０は、情報メッセージ５２を送信エンティティ１に送信して、宛先エンティティ２とコンタクトすることは不可能であることを通知する。第２の実施では、反応モジュール５０は、送信エンティティ１に何も送信しない。このような環境の下で、コールは、ＴＣＰタイムアウト機構によってステップ５３で終了される。

【００４３】

第２の反応モードでは、送信エンティティ１が単位時間あたりに送信が許可されるコールの数は、反応モジュール５０に規定された値５４に制限される。値５４は、一時的または恒久的に設定されるパラメータセットであり得る。送信エンティティ１によって起動されるコールの数が値５４に到達すると、送信エンティティ１によって起動される新たなコールは他の反応モードのうちの一つによって処理される。

【００４４】

第３の反応モードでは、送信エンティティ１によって起動されるコールは、コール処理オートマトン(call processing automaton)を実行し或いはこの種の問題を処理するための専用のＶｏＩＰサポートサービスにそのコールをルーティングするネットワーク２０のネットワークエンティティ５５にリダイレクトされることができる。上記オートマトンまたは上記サービスは、限定的例によれば、

・コール構成における問題を送信エンティティ１に示し、
・送信端末に関連端末の不審な動作を通知すると共に、その問題を解決するためのサポートサービスに接続されることを提案し、
・これがエラーであると考えるのであれば苦情(compliant)を提起することを送信エンティティに提案し、
・送信エンティティ１に関連するユーザーとの関係を保持しながら、スピットが終了されることを可能にする任意の他の通信動作を開始する。

【００４５】

第４の反応モードでは、検出モジュール５０によって識別されるスピットに関連するイベント５６は、ネットワーク２０におけるコール管理オペレーションに関与するネットワークエンティティ５８にルーティングされる。ネットワークエンティティ５８は、ネットワーク２０の情報システム（ＳＩ）、ＳＡＶ(after-scales service)またはＶｏＩＰサポートサービスをホスト(host)することができる。イベント５６をネットワークエンティティ５８にルーティングすることは、さらに多くの包括的なアクションが予想されることを意味し、加えて、受け渡された各コールに関する同一のオペレーションを繰り返すことを意味する。

【００４６】
・例えば、送信エンティティは、コール制限カテゴリ(call restriction category)に配置され、即ち、緊急サービス、ＳＡＶサービス、またはＶｏＩＰサービスのみをコールすることが許可され、またはローカルコールのみを行うことが許可される。
【００４７】
・例えば、送信エンティティは、ネットワークオペレータがプロデュースすることが合法的に必要とされる証拠(proof)を提供する目的で、監視(surveillance)付きで配置される。監視は、例えば、コール期間のような通信パラメータと、送信されるコールをログ(logging)することにある。
【００４８】
・例えば、送信エンティティに関連するユーザーのコーディネート(coordinates)は、スピットを構成する疑いのあるコールを要約すると共にユーザーをコール制限カテゴリーに配置する前に解決策を提案することが可能なサービスへの接続を提案するメールをユーザーに送信するために回復(recover)される。
【００４９】
有利には、反応モジュール５０は、多かれ少なかれスパムと関連するユーザープロファイルを追跡し、取得してスピットに特有な日付統計値(date statistics)まで保持するために拡張され、これは、同一のカテゴリーに属するクライアントユーザーのセットに同一処理が適用されることを可能にする共通カテゴリ内の同等のプロファイルと共にスピットの送信ユーザーを一緒にグループ化するためのユーザープロファイルの進化(evolution)に依存する。これは、スピットを送信したユーザーのリストが定義され、そのリストがブラックリストとして知られ、または振る舞いがこれまで正常であったユーザーが今はスピットを送信していることを示すように、変更された振る舞いの検出とコールの相関関係を可能とする。このような環境の下で、ユーザーの端末は、ウィルスまたはワームに感染し、ユーザーに知られないスピットを送信しているかもしれない。従って、端末が感染していることを検出し、その端末を浄化するためのサービスを提供することが可能である。全く同じように、政府機関のような、同時的なコールを送信することが許可された人物のホワイトリストが存在し得る。このような環境の下では、スピット検出カウンターは、有利には、コールをブロックすることを決断する前にホワイトリストと関連付けられることができる。
【００５０】
本発明の第１の実施では、図３に示されるように、スピット検出及び反応モジュールは、付加価値のあるサービス又は高機能なサービスの形態でＳＩＰアプリケーションサーバーにおいて実施される。図３を参照すると、ＳＩＰに基づくＶｏＩＰネットワークアーキテクチャが開示され、それぞれアプリケーションサービス６０ａおよび６０ｂにおけるスピット反応モジュール５０とスピット検出モジュール５を統合している。この実施は、有利には、スピットを検出すると共に、ネットワークルーティングエレメントを用いてネットワークオペレータによって開発されたＶｏＩＰネットワークアーキテクチャとの関連で反応するために使用される。上記ルーティングエレメントは、それぞれ、ＳＩＰ代理サービス（しばしば、“ＳＩＰプロキシ”と称される）６１ａ及び６１ｂであることができ、それに対して、送信しているサーバー、または宛先エンティティ、またはＳＩＰクライアント６２ａ及び６２ｂがそれぞれ接続される。
【００５１】
上記ＳＩＰプロキシサーバーは、ＳＩＰネットワークにおけるコールをルーティングする。本発明は、ＳＩＰベースのアーキテクチャで示され、Ｈ．３２３プロトコルに基づくアーキテクチャに等しく適合し、なぜなら、上記プロトコルは、同じ機能コンポーネント、例えば、限定的には、Ｈ．３２３アクセスコントローラ（“ゲートキーパー(gatekeepers)”）を使用し、それはネットワークエレメントであり、その役割は、送信エンティティと宛先エンティティとの間のコールを設定することと、ＳＩＰベースのアーキテクチャのルーティングエレメントと同様にルーティングを設定することである。

【００５２】
ＳＩＰコールは、それぞれ、ＳＩＰプロキシサーバー６１ａ及び６１ｂを介して二つのＳＩＰクライアント６２ａ及び６２ｂの間で設定され、それは、ＶｏＩＰネットワークにおけるコールをルーティングすることに関与する。アーキテクチャは、ユーザーの現在位置を提供するためのＳＩＰロケーションサーバー６３ａ及び６３ｂと、データベースにドメイン６５または６６のクライアントを登録するためのＳＩＰ登録サーバー６４ａおよび６４ｂを包含する。ＳＩＰプロキシサーバー６１ａおよび６１ｂは、ＳＩＰクライアントが、異なるＳＩＰプロキシサーバー６１ａ及び６１ｂに接続されれば、矢印６７で示されるように、相互に通信する必要がある。これは、コールが、異なるドメイン６５，６６に属する二つのＳＩＰクライアント６２ａおよび６２ｂの間で設定されれば当てはまる。

【００５３】
上記アプリケーションサーバーは、図３に示されるように、ＳＩＰプロキシサーバーの近くに配置されることができる。他のＶｏＩＰアーキテクチャの実施では、もし、付加価値のサービスロジックを実施すること、または負荷分散を提供することについて問題であれば、複数のアプリケーションサーバーが一つのＳＩＰプロキシサーバーに接続されることができ、または一つのアプリケーションサーバーが複数のＳＩＰプロキシサーバーに接続されることができる。上記アプリケーションサーバーは、全てのコールシグナリングパラメータをアクセスし、それらを修正し、コールをリダイレクトし、そして、他のモジュールと情報のやり取りを行うことができる。従って、ＳＩＰアーキテクチャ上で付加価値のサービスを実施することが容易である。付加価値のサービスを提供するために、アプリケーションサーバーで実行されるソフトウェアモジュールは上記アーキテクチャに付加される。

【００５４】
種々のオプションが、付加価値のサービスをＶｏＩＰアーキテクチャに統合するために利用可能である。即ち、
・ＣＰＬ(call processing language)標準が、ＳＩＰプロキシサーバー上で付加価値サービスを統合するために使用される。
・インターフェイスが、アプリケーションサーバー上での付加価値サービスを開発するために規定される。即ち、http://www.parlay.org/specs/index.asp参照のような、ＯＳＡ(Open Service Access)アーキテクチャに基づくと共にＥＴＳＩ(European Telecommunications Standards Institute)によって規定される標準によってカバーされるＯＳＡ／パーレイインターフェイスは、サービスが、標準化されたインターフェイスによってネットワーク機能を使用することを可能にし、また、http://www.parlay.org/specs/index.asp参照のＥＴＳＩによって規定された標準によってカバーされるＯＳＡ／パーレイＸインターフェイスは、ｗｅｂサービスに基いており、重要な利点を提供する。即ち、それは、遠隔通信ネットワークの知識を免除する傾向を有し、且つ、実行プラットフォームの独立性を提供する工業標準である。

【００５５】
ここに述べられる本発明は、どのインターフェイスが使用されても適合し、ＳＩＰプロキシサーバー上のＣＰＬ、アプリケーションサーバーのレベルでのＯＳＡ／パーレイＸまたはＯＳＡ／パーレイに適合する。実際、上述したようなスピット検出および反応モジュールを実施するアーキテクチャに統合されるソフトウェアモジュールを備えれば十分である。上述のモジュールの統合は、アプリケーションサーバー上にインストールされた付加価値サービスを介して達成され、または、さらに一般的にはサービスの開発を可能にするコンポーネントを介して達成される。また、それは、例えばＣＰＬを用いて、ＳＩＰプロキシサーバーに直接的に統合されることができる。

【００５６】
本発明は、マルチメディアサービスを支援すると共に標準化されたインターフェイスを提供する任意のタイプのアーキテクチャに適合する。例えば、本発明の他の実施において、本発明によるアプリケーションサーバーは、３ＧＰＰ(Third Generation Partnership

Project)に由来する標準、ＩＭＳ(Internet Protocol Multimedia Subsystem)タイプのアーキテクチャに組み込まれることができ、http://www.3gpp.orgを参照されたい。

【００５７】

本発明のこの第２の実施では、図４に示されるように、スピット検出モジュール５および反応モジュール５０は、それぞれ、ネットワークに配置されたアプリケーションプローブ７０－１および７０－２において実施される。アプリケーションプローブは、各ストリームをリアルタイムに識別するインターネットサービスプロバイダーまたは遠隔通信オペレータのネットワークに配置された機器であり、アプリケーションレベルまで上記ストリームを分析し、そして、透過的に、すなわち、端末またはユーザーが、ストリームが分析されたことを知ることなしに、データストリームの全パケットを取り押さえる(intercept)。アプリケーションプローブは、それらのアクションが、ストリームに作用することなくそのストリームが通過することをワッチングすることに制限されれば、受動的なものである。受動的プローブは、ストリームをリアルタイムに分析することができ、それを引き続いて分析することを目的としてファイルに前記ストリームに関するデータを格納することができる。データは、例えば、限定的には、交換される多数のデータアイテム、設定される多数の接続(connection)、ストリームのタイプである。データのその後の分析は、ネットワークの機能を理解し、ユーザーの振る舞いを分析し、ユーザーをカテゴリーに分類するために使用されることができる。受動的プローブは、有利には、反応がスピットの検出の後に続いて行われない場合に使用される。しかしながら、もし、受動的プローブが、スピットを送信する疑いのある端末のアドレスのようなデータを外部エンティティに転送(export)することができれば、その外部エンティティは、延期された反応機構(deferred reaction mechanisms)を使用することができ、例えば、スピットを送信する疑いのある端末によって送信された全コールを音声サーバーにルーティングすることにある。アプリケーションプローブは、等しくストリームに作用することができる。このような環境の下で、それらは、アクティブアプリケーションプローブと称される。限定的な例によれば、もし、ＩＰ技術がＰ２Ｐ技術において実施されれば、アクティブアプリケーションプローブはＰＳＰストリームに作用することができる。これは、もし、ＰＳＰプロトコルがＶｏＩＰ機能を提供すれば、本発明に関係する。ＳＩＰのような、標準プロトコルに基づくＶｏＩＰネットワークでは、マルチメディアセッションは二つのストリームから構成され、一つのストリームは、全てのＳＩＰシグナリングメッセージに対応し、もう一つのストリームは、ＲＴＰ(Real Time Protocol)によって伝達されるデータに対応する。そして、アクティブアプリケーションサーバーによって識別されたＳＩＰシグナリングは、ＳＩＰプロキシサーバーまたはアプリケーションサーバーにインストールされた上述のようなスピット検出モジュールにおける場合と同様にスピットを検出する目的で分析されることができ、コールシグナリングフィールドは、格納されたコールコンテキストの機能として分析され、そして、そのコールはスピットであるものとして、またはスピットではないものとして識別される。また、アクティブアプリケーションプローブは、特に、スピットプロキシまたはアプリケーションサーバーにインストールされた上述のようなスピット反応モジュールにおける場合と同様に、それらがスピットとして処理されれば、前記ストリームに作用することができ、即ち、何もせずにコールの通過を許可することにより、或いは、コール処理オートマトンを実行し又はこのタイプの問題に専用のサポートサービスに前記ストリームをルーティングするＶｏＩＰネットワークエンティティにそれらコールをリダイレクトすることによって、それらをブロッキングし、または、コーリングユニットによって単位時間あたりに送信されることができるコールの数を制限し、または、コール制限カテゴリーにコーリングエンティティを配置するような更に多くの全包含するオペレーションを構想することを可能にするイベントをフィードバックする。本発明の他の実施では、アクティブアプリケーションプローブによって識別されたＲＴＰストリームは、有利には、スピットを検出するために分析されることができる。ＲＴＰストリームからスピットを検出することは、同一のデータアイテムがネットワークにおいて複数回にわたって巡回していることを示す異なるＲＴＰパケットの、データに対応する、パケットのペイロードにお

ける共通特性を認識することにより達成される。例えば、共通特性の認識は、ＲＴＰデータパケットにおける同一のシグネチャー(signature)または同一のデータパケットサイズを識別し、同一サイズのデータアイテムがネットワークにおいて巡回していることを示すことにある（この例は、本発明を限定するものではない）。相関(correlation)は、データの転送についてのＲＴＰセッションの開始とＳＩＰシグナリングとの間で達成される。そして、前記ＳＩＰシグナリングによって提供される情報は、上述の反応モジュールにおける場合と同様にスピットの検出に対してプローブが反応することを可能にする。

【００５８】

アクティブアプリケーションプローブは、図４に示すように、ＶｏＩＰネットワークにおいて異なる場所に配置されることができる。前記プローブ７０－１および７０－２は、ＳＩＰクライアント６２ａとＳＩＰプロキシサーバー６１ａとの間、または、二つのＳＩＰプロキシサーバー６１ａおよび６１ｂの間に組み込まれる。

【００５９】

本発明のこの実施例は、スピット検出と反応モジュールをアクティブアプリケーションプローブに付与する。

【００６０】

本発明のこの実施例は多くの利点を有する。それは、例えばＳＩＰまたはＨ．３２３、ピアツーピア技術を用いたＶｏＩＰコールなど、種々のプロトコルに基づくオペレータのＶｏＩＰアーキテクチャにおいて、伝送中のＶｏＩＰコールの検出を可能にする。

【図面の簡単な説明】

【００６１】

【図１】ＶｏＩＰコールセットアップの期間で交換されるＳＩＰシグナリングメッセージを分析する複数のモードに基づくスピット検出方法を示す図である。

【図２】複数の反応モードに基づくと共にスピットの検出に続く反応方法を示す図である。

【図３】スピット検出及び反応方法が、ＳＩＰベースのＶｏＩＰネットワークに配置されたアプリケーションサービスにおいて実施されるところの本発明の第１構成に対応するアーキテクチャを示す図である。

【図４】スピット検出及び反応方法が、ネットワークにおけるアプリケーションプローブにおいて実施されるところの本発明の第２構成に対応するアーキテクチャを示す図である。

【符号の説明】

【００６２】

１　送信エンティティ
２　宛先エンティティ
３　第１ネットワークエンティティ
４　ＳＩＰコールシグナリングメッセージINVITE
５　検出モジュール
１５　エラーメッセージ
２０　ＩＰネットワーク
２５　ＶｏＩＰルーティングエレメント

【図１】

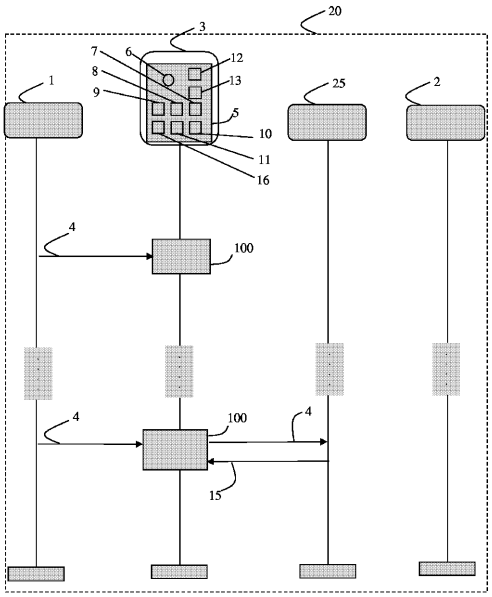



Fig. 1

【図２】

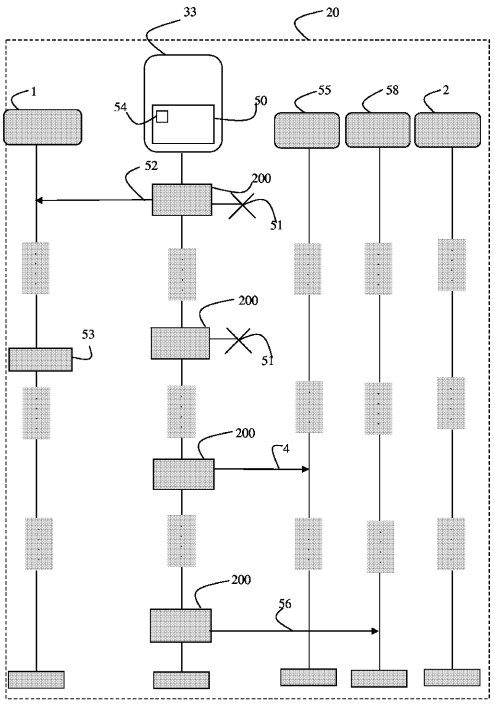



Fig. 2

【図３】

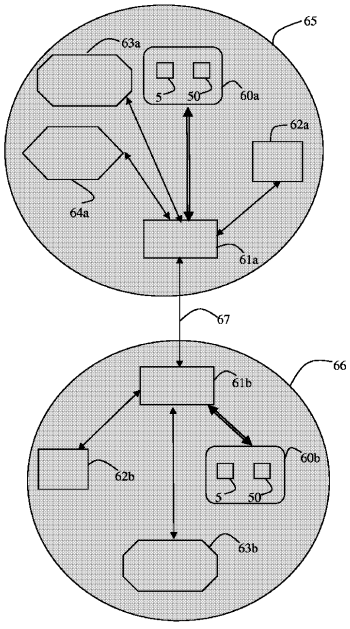



Fig. 3

【図４】

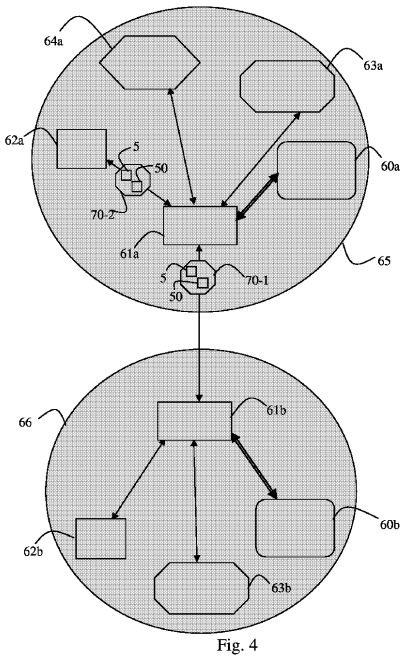



Fig. 4

【国際調査報告】

# INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2006/050324

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L H04M

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, PAJ, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X<br>A | US 2004/203432 A1 (PATIL BASAVARAJ ET AL)<br>14 October 2004 (2004-10-14)<br>abstract<br><br>paragraphs [0006] - [0013]<br>paragraphs [0030] - [0047]<br>paragraphs [0048] - [0053]<br>paragraphs [0054] - [0057]<br>claim 1<br>figure 2 | 1,5,11,<br>12,14,15<br>2-4,<br>6-10,13 |
| A | US 2003/083078 A1 (ALLISON RICK L ET AL)<br>1 May 2003 (2003-05-01)<br>the whole document | 1-15 |

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 22 September 2006 | 28/09/2006 |
| Name and mailing address of the ISA/<br>European Patent Office, P.B. 5818 Patentlaan 2<br>NL – 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,<br>Fax: (+31-70) 340-3016 | Authorized officer<br>Pereira, Mafalda |

Form PCT/ISA/210 (second sheet) (April 2005)

## INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR2006/050324

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| US 2004203432 A1 | 14-10-2004 | AU 2003253224 A1 | 19-04-2004 |
| | | EP 1543691 A1 | 22-06-2005 |
| | | WO 2004030386 A1 | 08-04-2004 |
| US 2003083078 A1 | 01-05-2003 | EP 1374606 A1 | 02-01-2004 |
| | | WO 02071774 A1 | 12-09-2002 |

Form PCT/ISA/210 (patent family annex) (April 2005)

# RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2006/050324

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. H04L29/00

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
H04L H04M

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela estréalisable, termes de recherche utilisés)
EPO-Internal, PAJ, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

| Catégorie* | Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents | no. des revendications visées |
|---|---|---|
| X<br>A | US 2004/203432 A1 (PATIL BASAVARAJ ET AL)<br>14 octobre 2004 (2004-10-14)<br>abrégé<br><br>alinéas [0006] - [0013]<br>alinéas [0030] - [0047]<br>alinéas [0048] - [0053]<br>alinéas [0054] - [0057]<br>revendication 1<br>figure 2 | 1,5,11,<br>12,14,15<br>2-4,<br>6-10,13 |
| A | US 2003/083078 A1 (ALLISON RICK L ET AL)<br>1 mai 2003 (2003-05-01)<br>le document en entier | 1-15 |

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

| Date à laquelle la recherche internationale a été effectivement achevée | Date d'expédition du présent rapport de recherche internationale |
|---|---|
| 22 septembre 2006 | 28/09/2006 |

| Nom et adresse postale de l'administration chargée de la recherche internationale | Fonctionnaire autorisé |
|---|---|
| Office Européen des Brevets, P.B. 5818 Patentlaan 2<br>NL – 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,<br>Fax: (+31-70) 340-3016 | Pereira, Mafalda |

Formulaire PCT/ISA/210 (deuxième feuille) (avril 2005)

## RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2006/050324

| Document brevet cité au rapport de recherche | Date de publication | Membre(s) de la famille de brevet(s) | Date de publication |
|---|---|---|---|
| US 2004203432 A1 | 14-10-2004 | AU 2003253224 A1 | 19-04-2004 |
| | | EP 1543691 A1 | 22-06-2005 |
| | | WO 2004030386 A1 | 08-04-2004 |
| US 2003083078 A1 | 01-05-2003 | EP 1374606 A1 | 02-01-2004 |
| | | WO 02071774 A1 | 12-09-2002 |

Formulaire PCT/ISA/210 (annexe familles de brevets) (avril 2005)

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IS,IT,LT,LU,LV,MC,NL,PL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,LY,MA,MD,MG,MK,MN,MW,MX,MZ,NA,NG,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,SM,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,YU,ZA,ZM,ZW

(72)発明者 イヴォン・グルハン
フランス・２２３００・ラニヨン・アヴニュ・ドゥ・ロレーヌ・４２
(72)発明者 クエンティン・ルディエル
フランス・２２５６０・プルムール－ボドゥ・アレー・アウェル・フォー・３

Ｆターム(参考) 5K030 GA14 HB01 JA10 LB01 LC13
5K201 AA07 BC25 CA02 CB04 CC02 CC03 CD09 DC02 EA05 ED02
FA05