(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2012-10402
(P2012-10402A)
(43)公開日　平成24年1月12日(2012.1.12)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/32	(2006.01)	H04L	9/00	675B	5J104
H04M 11/00	(2006.01)	H04M	11/00	303	5K201

審査請求 有　請求項の数 38　ＯＬ　外国語出願　（全 44 頁）

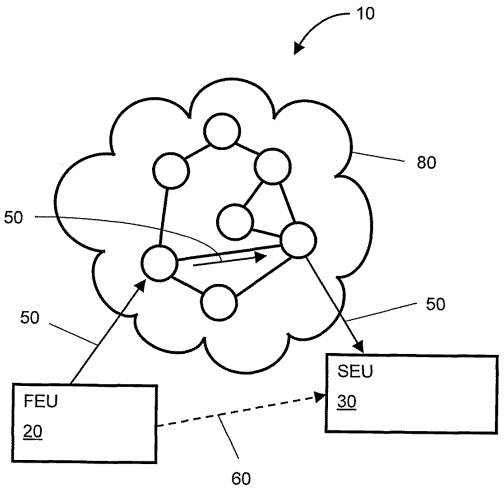
(21)出願番号　特願2011-198587 (P2011-198587)
(22)出願日　平成23年9月12日 (2011.9.12)
(62)分割の表示　特願2006-520034 (P2006-520034)の分割
原出願日　平成16年7月14日 (2004.7.14)
(31)優先権主張番号　60/487,242
(32)優先日　平成15年7月16日 (2003.7.16)
(33)優先権主張国　米国(US)

(71)出願人　506016691
スカイプ・リミテッド
ＳＫＹＰＥ　ＬＩＭＩＴＥＤ
アイルランド２ダブリン、アールスフォート・テラス、アールスフォート・センター、アーサー・コックス・ビルディング
(74)代理人　100101454
弁理士　山田　卓二
(74)代理人　100081422
弁理士　田中　光雄
(74)代理人　100125874
弁理士　川端　純市
(72)発明者　アハティ・ヘインラ
エストニア、エーエー１０１３２タリン、ユヒケンタリ８－５番

最終頁に続く

(54)【発明の名称】ピアツーピア電話システムおよび方法

(57)【要約】
【課題】複数のエンドユーザ装置および１つの通信構造を備え、その通信構造を経由して、通信の目的のために１つ以上のエンドユーザ装置を接続可能なピアツーピア電話システムを提供する。
【解決手段】通信構造（８０）は、１つ以上のエンドユーザ装置（２０、３０）を接続する通信構造内での通信経路のスイッチングに関して、実質的に分散している。１つ以上のエンドユーザ装置（２０、３０）が、構造（８０）へのアクセスを獲得するために１つ以上の認可証明書、すなわち、ユーザ識別証明書（ＵＩＣ）の交換に基づいて、構造（８０）を通るエンドユーザ装置自身の通信経路を確立するように動作する。構造（８０）が、１つ以上のエンドユーザ装置（２０、３０）に対して１つ以上の証明書を発行する管理装置（１００）を含む。
【選択図】図１



【特許請求の範囲】
【請求項１】
複数のエンドユーザ装置装置（２０、３０）および１つの通信構造（８０）を備え、その通信構造を経由して、通信の目的のために１つ以上のエンドユーザ装置（２０、３０）を接続可能なピアツーピア電話システム（１０）であって、
（ａ）上記通信構造（８０）が、上記１つ以上のエンドユーザ装置（２０、３０）を接続する上記通信構造（８０）内での通信経路のスイッチングに関して、実質的に分散していて、
（ｂ）上記１つ以上のエンドユーザ装置（２０、３０）が、上記構造（８０）へのアクセスを獲得するために１つ以上の認可証明書の検証に基づいて、上記構造（８０）を通る上記エンドユーザ装置自体の通信経路を確立するように動作し、
（ｃ）上記構造（８０）が、上記１つ以上のエンドユーザ装置（２０、３０）に対して上記１つ以上の証明書を発行する管理手段（１００）を含む
ことを特徴とするシステム（１０）。
【請求項２】
上記管理手段（１００）が、上記通信構造（８０）にアクセスするためのエンドユーザ装置によるサインアップおよびエンドユーザによる支払いのうち少なくとも一方を管理するように動作することを特徴とする請求項１に記載のシステム（１０）。
【請求項３】
上記管理手段（１００）が１組以上の秘密鍵および公開鍵のペアを生成するように動作し、証明書認証の目的のために、上記管理手段（１００）が、１つ以上の上記秘密鍵を秘匿し、１つ以上の対応する上記公開鍵を上記システム（１０）内で配布するように動作することを特徴とする請求項１または２に記載のシステム（１０）。
【請求項４】
上記管理手段（１００）が、リベスト－シャミール－アデルマン（ＲＳＡ）方式を使用して秘密鍵および公開鍵のペアを生成するように動作することを特徴とする請求項３に記載のシステム（１０）。
【請求項５】
上記構造（８０）が、ピアツーピア通信ネットワーク（１１０）を含み、上記ピアツーピア通信ネットワークを経由して上記複数のエンドユーザ装置（２０、３０）が相互に接続可能であることを特徴とする請求項１～４のいずれか１つに記載のシステム（１０）。
【請求項６】
上記ピアツーピアネットワーク（１１０）が、インタフェースノードおよび記憶ノードの組合せにより実現され、上記記憶ノードが、データベースアクセスの目的のため、１つ以上のスロットの中に構成されることを特徴とする請求項５に記載のシステム（１０）。
【請求項７】
上記管理手段（１００）が、
（ａ）エンドユーザ装置（２０、３０）アカウントデータベースの提供、
（ｂ）上記通信構造（８０）の時間基準の同期の提供、
（ｃ）上記システム（１０）のグローバルに設定可能な設定情報の提供、
（ｄ）上記構造（８０）のブート中のピアの発見の提供、
（ｅ）新規エンドユーザ装置（２０、３０）登録の取り扱い、
（ｆ）所望の動作モードを制御する構造（８０）の動作の監視
のうち１つ以上を実行するように構成されることを特徴とする請求項１～６のいずれか１つに記載のシステム（１０）。
【請求項８】
複数のエンドユーザ装置が、その間の通信を開始する前に、認可証明書を相互に交換するように動作し、上記証明書のうち少なくとも１つが本物であると同定されたとき上記通信が開始されることを特徴とする請求項１～７のうちいずれか１つに記載のシステム（１０）。

【請求項９】
上記構造（８０）が、上記システム（１０）のエンドユーザによる無料試用をサポートするように構成され、そのような無料試用が、許可の発行を繰り返して行うことにより、上記管理手段（１０）の管理下におかれていることを特徴とする請求項１～８のうちいずれか１つに記載のシステム（１０）。
【請求項１０】
上記管理手段（１００）が、１つ以上のエンドユーザ装置（２０、３０）により行使される上記システム（１０）の使用量に実質的に無関係である定額の請求書を、上記１つ以上のエンドユーザ装置に発行するように動作することを特徴とする請求項１～９のいずれか１つに記載のシステム（１０）。
【請求項１１】
ＰＯＴＳおよび／またはＰＳＴＮと同時に動作するように構成されたことを特徴とする請求項１～１０のいずれか１つに記載のシステム（１０）。
【請求項１２】
上記管理手段（１００）が、１つ以上の中央コンピュータサーバにより実現されることを特徴とする請求項１～１１のいずれか１つに記載のシステム（１０）。
【請求項１３】
上記管理手段（１００）が、エンドユーザ装置（２０、３０）による上記システム（１０）への不正アクセスを検出するために、エンドユーザ登録およびシステム（１０）使用データのヒューリスティックな不正検出解析を適用するように動作することを特徴とする請求項１～１２のいずれか１つに記載のシステム（１０）。
【請求項１４】
複数のエンドユーザ装置（２０、３０）および１つの通信構造（８０）を備え、その通信構造（８０）を経由して、通信の目的のために１つ以上のエンドユーザ装置（２０、３０）を接続可能なピアツーピア電話システムを動作させる方法であって、
（ａ）上記１つ以上のエンドユーザ装置（２０、３０）を接続する上記通信構造（８０）内での通信経路のスイッチングに関して実質的に分散しているように、上記通信構造（８０）を構成するステップ、
（ｂ）上記構造（８０）へのアクセスを獲得するために１つ以上の認可証明書の交換に基づいて、上記構造（８０）を通る上記エンドユーザ装置（２０、３０）自体の通信経路を確立するように動作するように、上記１つ以上のエンドユーザ装置（２０、３０）を構成するステップ、
（ｃ）上記１つ以上のエンドユーザ装置（２０、３０）に対して上記１つ以上の証明書を発行する管理手段（１００）を含むように、上記構造を構成するステップ
を含む方法を特徴とする方法。
【請求項１５】
上記管理手段（１００）が、上記通信構造（８０）にアクセスするためのエンドユーザ装置によるサインアップおよびエンドユーザによる支払いのうち少なくとも一方を管理するように動作することを特徴とする請求項１４に記載の方法。
【請求項１６】
上記管理手段（１００）が１組以上の秘密鍵および公開鍵のペアを生成するように動作し、証明書認証の目的のために、上記管理手段（１００）が、１つ以上の上記秘密鍵を秘匿し、１つ以上の対応する上記公開鍵をシステム（１０）内で配布するように動作することを特徴とする請求項１４または１５に記載の方法。
【請求項１７】
上記管理手段（１００）が、リベストーシャミールーアデルマン（ＲＳＡ）方式を使用して秘密鍵および公開鍵のペアを生成するように動作することを特徴とする請求項１６に記載の方法。
【請求項１８】
上記構造（８０）が、ピアツーピア通信ネットワーク（１１０）を含み、上記ピアツー

ピア通信ネットワークを経由して上記エンドユーザ装置（２０、３０）が相互に接続可能であることを特徴とする請求項１４～１７のうちいずれか１つに記載の方法。
【請求項１９】
上記ピアツーピアネットワーク（１１０）が、インタフェースノードおよび記憶ノードの組合せにより実現され、上記記憶ノードが、データベースアクセスの目的のため、１つ以上のスロットの中に構成されることを特徴とする請求項１８に記載の方法。
【請求項２０】
上記管理手段（１００）が、
（ａ）エンドユーザ装置（２０、３０）アカウントデータベースの提供、
（ｂ）上記通信構造（８０）の時間基準の同期の提供、
（ｃ）上記システム（１０）のグローバルに設定可能な設定情報の提供、
（ｄ）上記構造（８０）のブート中のピアの発見の提供、
（ｅ）新規エンドユーザ装置（２０、３０）登録の取り扱い、
（ｆ）所望の動作モードを制御する上記構造（８０）の動作の監視
のうち１つ以上を実行するように構成されることを特徴とする請求項１４～１９のいずれか１つに記載の方法。
【請求項２１】
複数のエンドユーザ装置が、その間の通信を開始する前に、認可証明書を相互に交換するように動作し、上記証明書のうち少なくとも１つが本物であると同定されたとき上記通信が開始されることを特徴とする請求項１４～２０のうちいずれか１つに記載の方法。
【請求項２２】
上記構造（８０）が、上記システム（１０）のエンドユーザによる無料試用をサポートするように構成され、そのような無料試用が、許可の発行を繰り返して行うことにより、上記管理手段（１０）の管理下におかれていることを特徴とする請求項１４～２１のうちいずれか１つに記載の方法。
【請求項２３】
上記管理手段（１００）が、上記１つ以上のエンドユーザ装置（２０、３０）により行使される上記システム（１０）の使用量に実質的に無関係である定額の請求書を、１つ以上のエンドユーザ装置に発行するように動作することを特徴とする請求項１４～２２のいずれか１つに記載の方法。
【請求項２４】
上記システム（１０）が、ＰＯＴＳおよび／またはＰＳＴＮと同時に動作するように構成されたことを特徴とする請求項１４～２３０のいずれか１つに記載の方法。
【請求項２５】
上記管理手段（１００）が、１つ以上の中央コンピュータサーバにより実現されることを特徴とする請求項１４～２４のいずれか１つに記載の方法。
【請求項２６】
上記管理手段（１００）が、エンドユーザ装置（２０、３０）による上記システム（１０）への不正アクセスを検出するために、エンドユーザ登録およびシステム（１０）使用データのヒューリスティックな不正検出解析を適用するように動作することを特徴とする請求項１４～２５のいずれか１つに記載の方法。
【請求項２７】
請求項１にかかる上記システム（１０）の少なくとも一部を実現するソフトウェア。
【請求項２８】
請求項１４にかかる上記方法の少なくとも１つのステップを実現する、コンピュータハードウェア上で実行可能なソフトウェア。
【請求項２９】
通信ネットワーク経由でエンドユーザ装置（２０、３０）と通信可能および／またはデータキャリアに格納されることを特徴とする請求項２７または請求項２８に記載のソフトウェア。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は通信システムに関し、例えば、ピアツーピアの原理により動作する分散型の通信システムであるとともに電話システムでもあるシステムに関する。さらに、本発明は、そのような電話システムおよび通信システムの動作方法に関する。
【背景技術】
【０００２】
現在設けられている従来の通信システム、例えば「公衆交換電話網（ＰＳＴＮ）」、携帯電話、およびＩＰ電話（ＶｏＩＰ）は、本来、実質的に集中型のシステムである。それらは、多くの場合、中継線、ローカルメトロリング、および同様な回線分配構造によりユーザにリンクされた中央電話交換機を用いている。さらに最近では、ソフトウェア動作によるエンドユーザ装置が、そのような従来の電話システム、例えば、卓上電話、携帯電話、およびＶｏＩＰ装置を接続するために利用可能になってきている。しかし、電話サービスプロバイダより提供されるほとんどすべての機能を実行するためには、エンドユーザ装置は、当該エンドユーザ装置のために１個以上の所望の機能を実行する中央電話交換機および／または構内電話交換機との通信を強いられる。多くの場合、そのような現在の電話システムにおける２つのエンドユーザ電話機は、２つのエンドユーザ電話機を互いにリンクするシステムの中央電話交換機なしには、互いに直接通信できない。例えば、２者が携帯電話機を使用して通話するとき、その通話は、２つの携帯電話機が無線により１個以上の基地局経由で通信することにより支援され、その２者および各々の携帯電話機が同じ建物内に存在する時でさえ、そのような基地局通信が必要とされる。もう１つの例では、公開のインターネット越しに２者がＶｏＩＰソフトウェアを用いて通話するとき、その通話は、中央サーバ経由で通信するそれらのソフトウェアアプリケーションにより支援され、たとえ２者の間で直接に接続を確立できても、そのようなサーバが必要になる。
【発明の概要】
【発明が解決しようとする課題】
【０００３】
集中型の電話システムの使用により、中央電話交換機への要求は著しく大きくなる。そのような中央電話交換機は広帯域光接続にますます依存するようになり、広帯域光接続としては、最高で１２０個までの光チャネルが３００ＴＨｚのオーダーの光キャリア周波数における５０ＧＨｚの周波数間隔の波長帯域に分散される高密度波長分割多重（ＤＷＤＭ）が使用される。そのような集中型の電話交換機は、極端に高価で、時折の故障による影響を受けやすい複雑な装置になり、そのような故障は、電話交換機を通る通信トラフィックを損なう可能性があり、それにより顧客への保証金の支払いが必要になる可能性がある。さらにそのような中央電話交換機の運用費用は、エンドユーザの数に比例して増大する。
【０００４】
本発明の発明者は、そのような集中型のアプローチが多くの場合に最適ではないと考え、他の代替の電話システムアーキテクチャを実施することによる利点が存在すると考えている。
【０００５】
そのような代替のアーキテクチャの採用から生じる問題を解決するために、本願発明者は本発明を発明した。
【０００６】
本発明の第１の目的は、実質的に分散型の電話ネットワークシステムを提供することである。
【０００７】
本発明の第２の目的は、加入者認証、ネットワークアクセス制御、およびアカウント処理を、より頑健であり、より信頼できる方法で実行できる、そのような分散型の電話シス

テムを提供することである。
【０００８】
本発明の第３の目的は、システムのエンドユーザと接続を確立する役割を他へ移すことにより電話システム内での通信トラフィックの集中を緩和させることができる、分散型の電話システム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の形態では、複数のエンドユーザおよび１つの通信構造を備え、その通信構造を経由して、通信の目的のために複数のエンドユーザを接続することのできるピアツーピア電話システムが提供され、本システムは、
（ａ）上記通信構造が、上記複数のエンドユーザを接続する上記通信構造内での通信経路のスイッチングに関して実質的に分散型であり；
（ｂ）上記複数のエンドユーザが、上記通信構造へアクセスするための認可証明書（authorisation certificate）の検証に基づいて、上記通信構造を通る上記エンドユーザ自身の通信経路を確立するように動作し；
（ｃ）上記通信構造が、上記複数のエンドユーザに対して上記認可証明書を発行する管理手段を含む
ことを特徴とする。
【００１０】
本発明の利点は、本発明の上記目的のうちの少なくとも１つを解決できることにある。
【００１１】
本発明は、集中型ではないアーキテクチャに関連する問題、すなわち、例えば本発明の目的となる課金／請求書作成のための、制御およびユーザ許可の問題を解決する。
【００１２】
好ましくは、このシステムでは、管理手段が、通信構造へアクセスするためのエンドユーザによるサインアップ（登録）およびエンドユーザによる支払いの少なくとも一方を管理するように動作する。
【００１３】
より好ましくは、例えば、システムの無許可の無料使用および／または不正使用を避けようとするために、管理手段は、１組以上の秘密鍵と公開鍵のペアを生成するように動作可能であり、証明書認証の目的で、上記管理手段は、１個以上の上記秘密鍵を秘匿し、１個以上の対応する上記公開鍵をシステム内で配布する。さらにより好ましくは、システムの中で、管理手段は、リベスト－シャミール－アデルマン（ＲＳＡ）方式を使用して秘密鍵と公開鍵のペアを生成するように動作できる。
【００１４】
好ましくは、システム内のネットワークの頑健性を増大させる目的のために、通信構造は、エンドユーザが相互に接続できるピアツーピア通信ネットワークを含む。より好ましくは、ピアツーピアネットワークは、インタフェースノードおよび記憶ノードの組合せにより実現され、上記記憶ノードは、データベースにアクセスする目的のため、１個以上のスロットとして構成される。有益なのは、通信構造が、プロプライエタリなグローバルインデックスピアツーピアネットワーク技術により実現されることである。
【００１５】
好ましくは、このシステムでは、管理手段が以下のうち１個以上を実行するよう構成される。
（ａ）エンドユーザアカウントデータベースの提供；
（ｂ）通信構造の同期時間基準の提供；
（ｃ）システムのグローバルに設定可能な設定；
（ｄ）通信構造のブートストラップ中におけるピアの発見；
（ｅ）新規エンドユーザ登録の取り扱い；
（ｆ）通信構造の所望モードの動作を制御するための通信構造の動作の監視。

【００１６】
好ましくは、このシステムでは、複数のエンドユーザは、それらの相互の通信を開始する前に、相互にそれらの認可証明書を交換するように動作可能であり、このとき、上記認可証明書のうち少なくとも１つが本物であると同定される。
【００１７】
好ましくは、例えば、実際面で本システムの採用を支援するために、通信構造は、エンドユーザによるシステムの無料試用をサポートするよう構成され、そのような無料試用は、許可の発行を繰り返して行うことにより、管理手段の管理下におかれている。
【００１８】
好ましくは、管理手段は、１つ以上のエンドユーザにより行使されるシステムの使用量に実質的に無関係である定額の請求書を、上記１つ以上のエンドユーザに発行するように動作できる。
【００１９】
好ましくは、使用中の既存の装置における本システムの使用を促進するために、本システムは、ＰＯＴＳおよび／またはＰＳＴＮと同時に動作するように構成されてもよい。「ＰＯＴＳ」および「ＰＳＴＮ」は、各々、従来のアナログ電話サービスおよび公衆交換電話網に対応する略語である。
【００２０】
好ましくは、管理手段は、１個以上の中央コンピュータサーバにより実現される。そのような実施例は、システムが公開のインターネットに関連して構成される時に特に有用である。代替として、管理手段は、実質的に分散型で実現されてもよい。
【００２１】
好ましくは、管理手段は、エンドユーザによるシステムへの不正なアクセスを検出するために、エンドユーザ登録およびシステム使用データのヒューリスティックな不正検出解析を利用するように動作できる。
【００２２】
本発明の第２の形態では、複数のエンドユーザおよび１つの通信構造を備え、その通信構造を経由して、通信の目的のために複数のエンドユーザを接続することのできるピアツーピア電話システムを動作させる方法が提供され、本方法は、
（ａ）上記複数ののエンドユーザを接続する上記通信構造内での通信経路のスイッチングに関して実質的に分散型であるように上記通信構造を構成するステップ；
（ｂ）上記通信構造へアクセスするための認可証明書の検証に基づいて、上記通信構造を通る上記エンドユーザ自身の通信経路を確立するように動作可能であるように、上記複数のエンドユーザを構成するステップ；
（ｃ）上記複数のエンドユーザに対して上記認可証明書を発行する管理手段を含むように上記通信構造を構成するステップ
を含むことを特徴とする。
【００２３】
本システムを利用することにより、本発明の目的の少なくとも１つを解決できるので、本方法は有利である。
【００２４】
好ましくは、この方法では、管理手段が、通信構造へアクセスするためのエンドユーザによるサインアップおよびエンドユーザによる支払いの少なくとも一方を管理するように動作できる。
【００２５】
好ましくは、この方法では、管理手段が、１組以上の秘密鍵と公開鍵のペアを生成するように動作可能であり、上記管理手段は、証明書認証の目的のため、１個以上の上記秘密鍵を秘匿し、システム内で、１個以上の対応する上記公開鍵を配布するように動作可能である。
【００２６】

好ましくは、この方法では、管理手段は、リベスト－シャミール－アデルマン（ＲＳＡ）方式を使用して秘密鍵と公開鍵のペアを生成するように動作可能である。しかし、本方法では、秘密鍵と公開鍵を生成する他のアプローチを使用してもよい。

【００２７】

好ましくは、この方法では、上記通信構造が、エンドユーザが相互に接続できるピアツーピア通信ネットワークを含む。さらに好ましくは、ピアツーピアネットワークが、インタフェースノードおよび記憶ノードの組合せにより実現され、上記記憶ノードは、データベースへアクセスする目的のため、１個以上のスロットとして構成される。

【００２８】

好ましくは、この方法では、管理手段が以下のうち１個以上を実行するように構成される。

（ａ）エンドユーザアカウントデータベースの提供；

（ｂ）通信構造の同期時間基準の提供；

（ｃ）システムのグローバルに設定可能な設定；

（ｄ）通信構造のブートストラップ中におけるピアの発見；

（ｅ）新規エンドユーザ登録の取り扱い；

（ｆ）通信構造の所望モードの動作を制御するための通信構造の動作の監視。

【００２９】

好ましくは、この方法では、複数のエンドユーザは、それらの相互の通信を開始する前に、相互にそれらの認可証明書を交換するように動作可能であり、このとき、上記認可証明書のうち少なくとも１つが本物であると同定される。

【００３０】

好ましくは、本方法の実施では、本システムの採用を促進するために、通信構造は、エンドユーザによるシステムの無料試用をサポートするよう構成され、そのような無料試用は、許可の発行を繰り返して行うことにより、管理手段の管理下におかれている。

【００３１】

好ましくは、この方法では、管理手段は、１つ以上のエンドユーザにより行使されるシステムの使用量に実質的に無関係である定額の請求書を、上記１つ以上のエンドユーザに発行するように動作できる。

【００３２】

好ましくは、本方法の実施では、既存の電話インフラストラクチャが存在する場所での本システムの使用を促進するために、本システムが、ＰＯＴＳおよび／またはＰＳＴＮと同時に動作するように構成されてもよい。「ＰＯＴＳ」および「ＰＳＴＮ」は、各々、従来のアナログ電話サービスおよび公衆交換電話網に対応する略語である。

【００３３】

好ましくは、この方法では、管理手段は、１個以上の中央コンピュータサーバにより実現される。

【００３４】

好ましくは、この方法を実施する時にシステムの不正使用を避けるために、管理手段は、エンドユーザによるシステムへの不正なアクセスを検出するために、エンドユーザ登録およびシステムの使用データのヒューリスティックな不正検出解析を利用するように動作できる。

【００３５】

本発明の第３の形態では、本発明の第１の形態にかかる電話システムの少なくとも一部を実施するように動作できるソフトウェアが提供される。

【００３６】

本発明の第４の形態では、本発明の第２の形態にかかる方法の少なくとも一部を実行するように動作できるソフトウェアが提供される。

【００３７】

本発明の範囲から離れることなく本発明の構成要件が任意の方法で組み合わされてもよ

いことは理解されるであろう。
【図面の簡単な説明】
【００３８】
【図１】本発明にかかる電話システムの概略図
【図２】図１のシステムのピアツーピア構造の概略図
【発明を実施するための形態】
【００３９】
以下、添付の図面を例示としてのみ参照して、発明の実施の形態を説明する。
【００４０】
本発明にかかる電話システムは実質的には分散した構造を有し、この構造は、ピアツーピア通信ネットワークにより接続された複数のエンドユーザからなる空間的に分散したアレーを含む。この構造内には、通信ネットワークの使用に関する加入者のサインアップおよび支払いなどのある特定のネットワーク管理機能を実行する１個以上の管理ノード装置を除き、実質的には、いかなる形式の集中型の電話交換機も除去されている。分散型の構造では、ほとんどの通常の機能、例えば電話をかける機能は、完全にエンドユーザ装置により取り扱われ、ここで、エンドユーザ装置は、実質的に互いに直接通信するか、光メトロリングまたは公開のインターネット上の分散型リレーノードなどの何らかの形式のローカル電話交換機を経由して通信するように動作できる。
【００４１】
本発明にかかるシステム、すなわち、図１において概して参照番号１０により示されるシステムでは、システム１０の第２のエンドユーザ（ＳＥＵ）３０にメッセージを送ることを所望するシステム１０の第１のエンドユーザ（ＦＥＵ）２０は、以下のような通信方法を採用する。
（ａ）第１のエンドユーザ２０は第２のエンドユーザ３０の位置を特定する。この位置決めは、例えば、後で説明する「グローバルインデックス」（Global Index：ＧＩ）と呼ばれるプロプライエタリなピアツーピア技術を用いた、および／または、ノード検索機能を提供するように構成された最新の「分散ハッシュテーブル」技術を用いた、ピアツーピア技術により実行される。
（ｂ）第１エンドユーザ２０は、第２のエンドユーザ３０のアドレス情報と、第１のエンドユーザ２０から第２のエンドユーザ３０へ接続するために使用される１個以上の通信経路５０、６０に関する詳細情報とを受信する。
（ｃ）次に、第１のエンドユーザ１０が、所定のプロトコルに従って、第２のエンドユーザ３０へ１個以上の通信経路５０、６０を確立する。
【００４２】
ＧＩピアツーピア技術では、分散型の通信ネットワーク経由で相互接続された複数の参加ノードからなるネットワークが提供される。参加ノードは、インタフェースノードまたは記憶ノードのどちらかであるように割り当てられる。好ましくは、例えばインタフェースノードが記憶ノードよりも１００倍多いというように、記憶ノードの数がインタフェースノードの数よりも著しく少なくなるように構成される。さらに、記憶ノードにはデータレコードを格納する役割があり、一方、インタフェースノードには、クエリーを処理して記憶ノードに要求を送信する役割があり、記憶ノードからは、このクエリーに応答してデータレコードが送信される。さらに、インタフェースノードには、格納するデータレコードを受信する役割と、データレコードを収容して格納するための１個以上の適切な記憶ノード群を決定する役割がある。複数の記憶ノードは、スロットとして知られる複数のグループとして構成され、このとき、与えられた記憶ノードと特定のスロットとの関連付けは、記憶ノードの各々に保持されたアドレスデータに依存する。ＧＩ技術は、本特許出願とほぼ同時期の特許出願に記載され、ＧＩ技術特許出願の内容は、本発明の電話システムを説明する目的で参照によりここに組み入れられている。
【００４３】
システム１０では、加入者の認証、アクセス制御、およびアカウント処理に多大な要求

がある。システム１０の主要なシステム機能は、システム１０の１以上のエンドユーザがそのような機能に対して支払いをしたときか、そのような機能へアクセスする許可を受けたときにのみ使用できる。最新の従来型の電話システムでは、１個以上の主要なシステム機能へのエンドユーザによるアクセスは、システムの中央電話局により集中型の制御で検査される。対照的に、本システム１０では、アクセスは、公開鍵暗号法を使用してエンドユーザの装置により検査される。そのような暗号法では、加入者とも呼ばれる各エンドユーザは、エンドユーザの装置により作成された暗号鍵ペアと関係づけられる。加入者のサインアップまたは支払いに際して、システム１０の中央電話局が加入者にデジタル証明書を発行する。そのような証明書はユーザ識別証明書（ＵＩＣ）とも呼ばれる。それにより中央電話局が、この鍵ペアの所有者が許可を受けた加入者であることを証明する。

【００４４】

上記の方法のステップ（ｃ）で、第１のエンドユーザ２０が他の加入者装置、すなわち第２のエンドユーザ３０と通信する時、第１のエンドユーザ２０は、加入者である証明として、証明書、つまり上記のＵＩＣを提供する。システム１０では、エンドユーザ装置が、そのような加入者である証明のない相互通信を拒否するように構成されている。さらに、公開鍵暗号法を使用することで、証明書（ＵＩＣ）を発行する役割をもつシステム１０の上記中央電話局と通信する必要なしに、システム１０の各エンドユーザ装置が、互いの証明書（ＵＩＣ）を検証するように構成される。このように、システム１０は、エンドユーザ２０、３０間の通信経路を確立する時に、システム１０の中央電話局との通信を必要とせず、エンドユーザ２０、３０により分散型の方式で機能する。

【００４５】

システムの加入者装置、例えば第１のエンドユーザ２０が、受信者、例えば第２のエンドユーザ３０の位置を特定すると、それに続いて相互に通信する必要がある。そのような通信は、好ましくは直接経路によって行われ、例えば図１に示された経路６０に沿って行われる。しかし、例えば空間的な分離および／または地形のために、そのような直接経路が常に技術的に実現可能であるわけではない。例えば、第１のエンドユーザ２０から第２のエンドユーザ３０まで公開のインターネットを経由した通信が望まれる時、第２のエンドユーザ３０が、システム１０のローカルネットワークの外側からアクセス不可能なプライベートアドレスを持つと、そのような通信は実現不可能である。直接通信が実現不可能な場合には、システム１０は、ピアツーピア構造８０内の１個以上のピアノードを経由する通信をルーティングして、第１のエンドユーザ２０と第２のエンドユーザ３０とが相互に通信するのを支援する。これらの１個以上のピアノードは、好ましくは加入者装置により実現され、それらの加入者装置は、第１のエンドユーザ２０および第２のエンドユーザ３０の間の通話に関わる第１のエンドユーザ２０および第２のエンドユーザ３０に必ずしも属す必要はない。したがって、例えば直接接続が実現不可能なシナリオでは、加入者は直接アクセス可能なもう１つの装置と通信し、このもう１つの装置が最終的な受信者装置と直接通信する。

【００４６】

次に、システム１０のアーキテクチャ形態をさらに詳細に説明する。ピアツーピア構造８０は、図２に示されているように２つの区分、つまり、一方の中央サーバ（ＣＳ）１００と、もう一方のピアツーピアネットワーク（Ｐ２ＰＮ）１１０とに再分割される。

【００４７】

中央サーバ１００は、好ましくは、構造８０の提供事業者により運用される。これらのサーバ１００は、以下のタスクのうちの１個以上を実行するように構成される。

（ｉ）エンドユーザのアカウント処理の詳細を記録するエンドユーザアカウントデータベースの提供；

（ii）構造８０用の同期時間基準の提供；

（iii）システム１０用のグローバルに設定可能な設定の提供；

（iv）構造８０のブートストラップ中におけるピアの発見および新たなエンドユーザの登録の取り扱い；

（ｖ）システム１０の提供事業者のみに知られている秘密暗号鍵を使用した、システム１０に関する重要な情報への電子的署名、例えば、上に説明したようなエンドユーザの識別情報や、例えば、上記のユーザ識別証明書（ＵＩＣ）への署名；

（vi）提供事業者のインフラストラクチャ、賃借したインフラストラクチャ、およびアウトソーシングしたインフラストラクチャのうちの１つ以上による追加サービスの提供；

（vii）中央サーバ１００およびネットワーク１１０の所望の動作モードを保証するための、それらの動作の監視。

【００４８】

上記の（vi）で述べた追加サービスは以下のうち１個以上に関連する。

（１）「公衆交換電話網」（ＰＳＴＮ）および／または「従来のアナログ電話回線サービス」（ＰＯＴＳ）接続から“Ｖｏｉｃｅ ｏｖｅｒ Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ”（ＶｏＩＰ）トラフィックの終端装置への接続、および逆の接続。例えばＰＯＴＳから提供事業者のシステムへの接続。

（２）「インスタントメッセージ」（ＩＭ）から「ショートメッセージサービス」（ＳＭＳ）への接続の取り扱い。

（３）中央サーバ１００内に含まれるバックエンドサーバと接続可能な、エンドユーザ会議、ボイスメール、および同様な活動の取り扱い。

【００４９】

ピアツーピアネットワーク１１０は、好ましくは、システム１０の提供事業者により提供されるソフトウェアを内部で実行するように構成されたエンドユーザコンピュータ装置を含む。ネットワーク１１０はまた、好ましくは、システム１０の提供事業者によりカスタマイズされた、所定バージョンの上記ＧＩプロトコルに基づく。ネットワーク１１０は、以下のうち１個以上を好ましくは含む機能を実行するように動作できる。

（ａ）エンドユーザの仲間リストの管理；

（ｂ）エンドユーザの嗜好情報、例えば仲間のオンライン／オフライン通知の取り扱い；

（ｃ）ノード識別情報（ＩＤ）、ユーザ名、エンドユーザプロファイルデータのうちの１個以上によるエンドユーザ識別情報の提供；

（ｄ）基本的統計情報、例えば、システム１０内で現在アクティブに通信しているエンドユーザの数の維持；

（ｅ）ネットワーク１１０を通る通信をサポートするアドホックなプロキシとして機能するネットワーク１１０内のランダムピアノードを経由した、ファイアウォールおよび／または“Ｎｅｔｗｏｒｋ Ａｄｄｒｅｓｓ Ｔｒａｎｓｌａｔｉｏｎ”（ＮＡＴ）の通過の維持。

【００５０】

ピアツーピアネットワーク１１０に関する上記（ｃ）において、ユーザ名が、システム１０内で「電話番号」として有効に使用できる。さらに、エンドユーザプロファイルデータは、エンドユーザから提供されると、データレコードに関連したものとなる。そのようなデータレコードは、実際の名前（例えば、ロジャー・スミス、アニー・ハンセン）、空間的な位置（例えば、米国のワシントン、デンマークのコペンハーゲン）、生年月日、および電子メールアドレスのうちの１個以上を含む。

【００５１】

本願発明者は、システム１０の動作が、例えば、システム内での公開鍵暗号の使用により提供されるセキュリティに依存することを理解している。システム１０の開発に際して、本願発明者はさらに、ピアツーピアＩＭ／ＶｏＩＰシステムが、１個以上の中央サーバに依存するＰＯＴＳまたは任意の同等の電話システムよりも本質的にセキュアでないと考えている。ここで、「ＩＭ」、「ＶｏＩＰ」、および「ＰＯＴＳ」は、各々「インスタントメッセージ」、“Ｖｏｉｃｅ ｏｖｅｒ Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ”、および「従来のアナログ電話回線サービス」の略語である。システム１０では、本願発明者は、システム１０内で大部分の基本的なセキュリティ要求を満たすために、最新のリベス

トーシャミールーアデルマン（ＲＳＡ）公開鍵暗号および関連する電子署名を使用するように構成した。しかし、システム１０では他のタイプの公開鍵暗号を使用してもよいことは理解されるであろう。

【００５２】

あるエンドユーザ、例えばエンドユーザ２０、３０のうちの１つが中央サーバ１００における登録を求めたとき、そのエンドユーザは、ＲＳＡ暗号鍵のペア、つまり、相補的な秘密鍵及び公開鍵を含み、公開鍵からの秘密鍵の導出及びその逆が不可能な鍵のペアの生成を行う。エンドユーザの公開鍵は、エンドユーザに提供されたユーザ識別証明書（ＵＩＣ）に現れ、一方、秘密鍵はエンドユーザの機器にローカルに格納される。

【００５３】

通信を開始する前、第１のエンドユーザ２０から第２のエンドユーザ３０への呼のセットアップ中において、また、同様にインスタントメッセージ（ＩＭ）の送信中において、各エンドユーザは、適正であることを他方に示すために、ユーザ識別証明書（ＵＩＣ）を提示し、または、システム１０が受理するように設定されていれば一時的識別番号（ＴＩＮ）を提示する。各エンドユーザは、ユーザ名を持っているときには、ＵＩＣを示す。ＵＩＣが、エンドユーザ２０、３０のうちの第１のエンドユーザから第２のエンドユーザに提示されると、第２のエンドユーザは、第１のエンドユーザにより提供された署名を検証する。そのような検証は中央サーバへの接続を要求しない。さらに第２のエンドユーザは、第１のユーザの公開鍵に関するチャレンジデータパケットを発行することにより、第１のエンドユーザが対応する秘密鍵を持つことを検証し、第１のエンドユーザがそれを復号できることを検査する。以上の動作の完了後、第１のエンドユーザは、第１のエンドユーザが保持していると主張するところのユーザ名を合法的に持つことを安全に信じることができる。

【００５４】

システム１０の中で通話する時、限定的な試行期間にわたる許可が与えられているのでない限り、通話により支払いが請求されるので、追加の検査が必要になる。システム１０では、セキュアな方法で通話時間および通話回数を監視するのが難しく、この点で、本願発明者は、システム１０内の課金／請求書作成の基礎として、時間ベースの加入を使用することが有利であると理解している。したがって、そのような時間ベースの加入を実現するために、ユーザ識別証明書（ＵＩＣ）の権限が検査され、上記の例ではエンドユーザ２０、３０のいずれも満了前の加入権付きのユーザ識別証明書（ＵＩＣ）を持たない場合には、試用通話でない通話をピアツーピアネットワーク１１０を介して行うことはできない。言い換えると、１つ以上のエンドユーザ２０、３０が有効な加入権または試用権をもつと、ピアツーピアネットワーク経由で通話が行われる。

【００５５】

加入権が期限切れにならないように維持するためには、システム１０のエンドユーザは、例えば次の月／年の料金を支払うことにより、ユーザ識別証明書（ＵＩＣ）を定期的に更新しなければならない。他の支払期間が可能であること、または支払い以外の他の基準に基づいてＵＩＣが延長可能であることは理解されるであろう。更新の支払いを受けたとき、中央サーバ１００は、以前のエンドユーザの名前に応答して新しいＵＩＣを発行するように動作し、新しいＵＩＣは新しい加入権の期限の詳細に関連付けられる。クレジット／デビットカードの課金／請求書作成が、システム１０の１つ以上のエンドユーザにより許可された時、課金／請求書作成は、関連するエンドユーザによる介入の必要なく、中央サーバ１００により自動的に実行されてもよい。

【００５６】

したがって、システム１０では、通話の好ましい支払い方法は、システム１０で無制限に通話する権利をユーザに与える月々の定額加入または年間定額加入である。そのような通話をする時には中央電話交換機のリソースは実質的に利用されず、通話はシステム１０の提供事業者に運用費用を発生させないので、そのような課金／請求書作成の構成は、業務上の観点からはシステム１０にとって許容できるものである。対照的に、ＰＯＴＳ／Ｐ

ＳＴＮを発信元または宛先とする通話は、実際の１分毎の運用コストを発生させ、それ故、システム１０では、本発明にかかる通話から別々および区別して適切に課金される。

【００５７】

ピアツーピア構造８０が上記のＧＩプロトコルにより実現されると、図１に示されていない他のエンドユーザを含む図１のエンドユーザ２０、３０、中央サーバ１００、およびピアツーピアネットワーク１１０は、有効に参加するノードである。そのような構成では、各エンドユーザは、その身元に関する情報をＧＩ記憶ノードに定期的に送信することにより、または、システム１０が一時的識別番号（ＴＩＮ）を受理する構成である時は、一時的識別番号（ＴＩＮ）をＧＩ記憶ノードに定期的に送信することにより、そのエンドユーザの存在についてＧＩ記憶ノードに通知する。１個以上のエンドユーザが、例えば電話帳問い合わせに類似したＧＩクエリーを行う時、記憶ノードは、そのようなクエリーに応答したデータパケットとして、格納されたユーザ識別証明書（ＵＩＣ）または一時的識別番号（ＴＩＮ）を送信して応答する。

【００５８】

ＵＩＣの場合、ＧＩ記憶ノードにより送り出された対応するデータパケットはエンドユーザに受信され、エンドユーザはそのエンドユーザの秘密鍵によりデータパケットに署名し、それにより、クエリーを出した１個以上のエンドユーザが、対応する公開鍵を使用して、例えば問い合わせに応答して受信されたデータパケットの真正性を検証できる。このような構成は、誰もユーザ識別証明書（ＵＩＣ）のエンドユーザのディレクトリのエントリを偽造できないことを実質的に保証できるので有利である。そのようなアプローチの理論的根拠は、ユーザ識別証明書（ＵＩＣ）を所有する参加ノードが、例えばその存在の通知を行うとき、そのＵＩＣに対応する秘密鍵の署名付きのデータパケットを１個以上の記憶ノードに送信し、必要ならば他の参加ノードにも送信するように動作できるということにある。１個以上の記憶ノードから受信し、次のリリースのためにそこに格納される署名付きのＵＩＣは、対応する公開鍵を使用することにより、クエリーを出した側の参加ノードによって検証される。そのような構成により、ＵＩＣの改ざんおよび偽造を回避できる。

【００５９】

システム１０には、さらに無料試用機能が設けられ、そのような機能は、新しいエンドユーザをシステム１０に惹きつける目的で商業的に有利である。好ましくは、そのような無料試用機能は、X_1日の無料期間であり、または、その代替もしくは追加としてのX_2回の無料通話である。そのような無料試用期間および無料試用通話のために、中央サーバ１００は各無料通話に明示的な許可を与える必要がある。好ましくは、与えられるか要求される全ての許可は、例えば後で説明するヒューリスティックな不正行為検出目的のために、システム１０のデータベース内に記録されている。エンドユーザが、割り当てられた無料期間および／または無料通話回数を使い切ってしまうと、中央サーバ１００から許可が与えられず、エンドユーザがなおもシステム１０内で通話することを望むならば、続いてエンドユーザに支払い要求が来る。

【００６０】

システム１０は、従来型の電話システム、例えば、インターネットを実現できる従来型の電話システムの中で、またはそれと組み合わせて同時に動作させることができる。

【００６１】

上記の無料試用許可スキームは、本願発明者が、システム１０に関してのみ意図していることである。システム１０に関連して行われる従来型の支払いによる加入者通話の場合は、通常の従来型の加入制度が適用され、通話毎の許可は要求も記録もされない。ＰＳＴＮ通話の場合、無料試用スキームは、潜在的にはシステム１０に関連して提供可能であるものの実施されない。

【００６２】

システム１０で受信された無料通話許可要求の各々に関し、中央サーバ１００は、通話に関する以下のパラメータのうち少なくとも１つを記録するように動作できる。

（ａ）ユーザ名または一時的識別番号（ＴＩＮ）の形式の発呼側エンドユーザの識別情報；
（ｂ）発呼側エンドユーザのコンピュータ識別情報（ＩＤ）；
（ｃ）発呼側エンドユーザのインターネットプロトコル（ＩＰ）アドレス；
（ｄ）ユーザ名またはＴＩＮの形式の被呼側エンドユーザの識別情報；
（ｅ）被呼側エンドユーザのコンピュータＩＤ
（ｆ）被呼側エンドユーザのＩＰアドレス
（ｇ）通話日時
（ｈ）その通話に許可が与えられたか否か

【００６３】

したがって、システム１０では、「試用ユーザ」の明示的なステータスが提供されず、好ましくは、ただ単に、エンドユーザが定められた開始日Ｄから何回かの無料通話をすることのみが必要である。任意のエンドユーザの最初の無料通話がX_1日前よりも最近である場合（またはエンドユーザがシステム１０内で無料通話オプション権をまだ行使していない場合）、そのエンドユーザには、無料通話をする権利が与えられる。代わりに、システム１０は、Ｘ日間にわたる無料通話期間ではなく、Ｘ回の無料通話からなる無料試行期間を許容するように設定にできる。

【００６４】

システム１０のソフトウェアのハッキングされたバージョンを用いると、不正エンドユーザが、システム１０で用いている無料試用許可要求および許可検査対策を省略できるようになる。しかし、発呼側エンドユーザ許可検査および被呼側エンドユーザ許可検査の両方を実施するシステム１０では、そのようなハッキングを行っても、不正なエンドユーザは、他の不正なエンドユーザと無料で通話することしかできず、言い換えると、海賊版の不正なエンドユーザソフトウェアは、システム１０上で使用される時、とても限られた利益を提供することしかできない。多くの場合、システム１０のそのような限られた不正使用が行われたとしても、システム１０の提供事業者に対する著しい経済的損失は生じない。

【００６５】

システム１０の主な不正行為の機会としては、ハッカーがユーザ名およびコンピュータＩＤを偽装しようとし、新規無料試用を繰り返して始める場合があることを本願発明者は理解している。そのような主な不正行為の機会では、ハッカーは、システム１０に互換性のあるソフトウェアにおいて全てのローカルシェアウエアタイプの検査を省略する必要がある。そのような不正行為に対抗するため、中央サーバ１００は、繰り返しの不正行為パターンを同定するヒューリスティックな不正行為検出を実行するようにプログラムされる。例えば中央サーバ１００は、無料通話の提供をＺ回要求し、次に、同じＩＰアドレスと新規のコンピュータＩＤで同じ人に通話する新規の無料通話許可を引き続き要求するエンドユーザを、不正なエンドユーザとして検出するように動作できる。システム１０内での無料通話の明示的な許可が中央サーバ１００から要求されるので、システム１０内で実行されているそのようなヒューリスティックな不正行為検出ソフトウェエアへ入力するための重要な情報がシステム１０内では利用可能である。しかし、そのようなヒューリスティックな不正行為検出を行っても、システム１０内で発生する全てのハッキングのケースを検出できるわけではない。

【００６６】

上に説明した発明の実施の形態は、本発明の範囲から離れることなく変更可能であることは理解されるであろう。

【００６７】

前述のように、システム１０は、一時的識別番号（ＴＩＮ）の使用をサポートできるとして説明した。しかし、システム１０は、その中でＴＩＮが利用されないように変更できるので、無料試用目的で、ユーザ名と、そのユーザ名に関連付けられた時間制限付きの実質的に費用のかからない権限に対応するユーザ識別証明書（ＵＩＣ）とが使用される。必

要とされるならば、システム１０は、前に説明したような無料試用がエンドユーザに提供されないように構成されてもよく、代わりに、無料試用の他の構成、例えば最初払った加入費用の払い戻しなどが利用できる。

【００６８】

システム１０は、好ましくは、少なくとも部分的には、コンピュータハードウェア上で実行可能なソフトウェアを使用して実現される。そのようなソフトウェアは、インターネットなどの通信ネットワークを経由しておよび／またはユーザに提供されるＣＤＲＯＭ等の適切なデータキャリア上に格納されたソフトウェアにより、ユーザに配布できる。

【００６９】

電話システム１０に関する発明の実施の形態の上記の説明では、本発明が一般的に通信システムに関連し、それ故、用語「電話」はそのように解釈すべきであることは理解されるであろう。具体的に、当該システムと共に実施可能な他の形式の通信としては、テレビ電話、電話会議、およびテキスト・メッセージを含む。

【００７０】

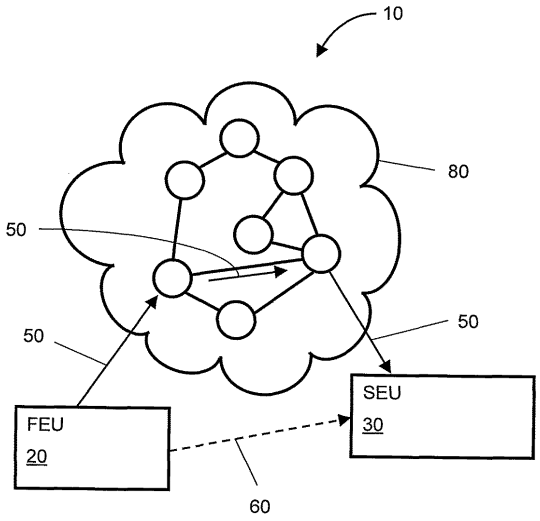
以上の説明では、「含む」「備える」「持つ」「である」「組み入れる」「包含する」は、排他的ではないように解釈されるよう意図していて、開示されていない他の要素が存在する可能性もある。

【符号の説明】

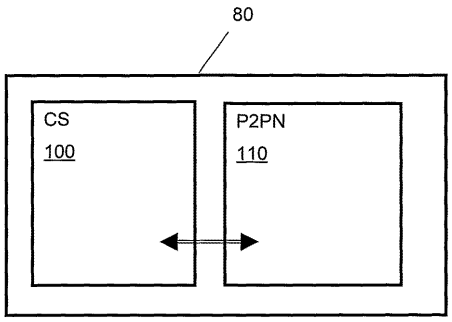
【００７１】

１０　システム
２０　第１のエンドユーザ
３０　第２のエンドユーザ
５０　通信経路
６０　通信経路
８０　通信構造
１００　管理手段（中央サーバ）
１１０　ピアツーピアネットワーク

【図１】



【図２】



【手続補正書】
【提出日】平成23年10月3日(2011.10.3)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】０００２
【補正方法】変更
【補正の内容】
【０００２】
現在設けられている従来の通信システム、例えば「公衆交換電話網（ＰＳＴＮ）」、携帯電話、及びＩＰ電話（ＶｏＩＰ）は、本来、実質的に集中型のシステムである。それらは、多くの場合、中継線、ローカルメトロリング、及び同様な回線分配構造によりユーザにリンクされた中央電話交換機を用いている。さらに最近では、ソフトウェア動作によるエンドユーザ装置が、そのような従来の電話システム、例えば、卓上電話、携帯電話、及びＶｏＩＰ装置を接続するために利用可能になってきている。しかし、電話サービスプロバイダより提供されるほとんどすべての機能を実行するためには、エンドユーザ装置は、当該エンドユーザ装置のために１個以上の所望の機能を実行する中央電話交換機及び／又は構内電話交換機との通信を強いられる。多くの場合、そのような現在の電話システムにおける２つのエンドユーザ電話機は、２つのエンドユーザ電話機を互いにリンクするシステムの中央電話交換機なしには、互いに直接通信できない。例えば、２者が携帯電話機を使用して通話するとき、その通話は、２つの携帯電話機が無線により１個以上の基地局経由で通信することにより支援され、その２者及び各々の携帯電話機が同じ建物内に存在する時でさえ、そのような基地局通信が必要とされる。もう１つの例では、公開のインターネット越しに２者がＶｏＩＰソフトウェアを用いて通話するとき、その通話は、中央サーバ経由で通信するそれらのソフトウェアアプリケーションにより支援され、たとえ２者の間で直接に接続を確立できても、そのようなサーバが必要になる。

【特許文献１】米国特許第７，４８０，６５８号
【特許文献２】国際出願の国際公開第ＷＯ０２／０６５３２９号
【特許文献３】欧州特許出願ＥＰ１，６４９，３８７号
【手続補正２】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
ＶｏＩＰピアツーピアシステムを備えたピアツーピアシステムであって、上記ＶｏＩＰピアツーピアシステムは、
複数の許可されたエンドユーザ装置を相互接続してＶｏＩＰ通信経路を介するＶｏＩＰ呼を支援する、実質的に分散型のピアツーピア通信構造を含み、上記複数の許可されたエンドユーザ装置は許可された発呼側エンドユーザ装置及び許可された被呼側エンドユーザ装置を含み、
上記ピアツーピア通信構造は、上記複数の許可されたエンドユーザ装置のそれぞれに各ユーザ名を関連付けることにより、許可されたエンドユーザの識別を行い、上記ユーザ名は上記ピアツーピア通信構造における電話番号として使用可能であり、
上記ピアツーピア通信構造は管理ノードを含み、上記管理ノードは、上記複数の許可されたエンドユーザ装置のそれぞれに認可証明書を発行して上記ピアツーピア通信構造における許可されたアクセスの証明を支援することにより、上記ピアツーピア通信構造の無許可の不正な使用を回避するように構成され、
上記複数の許可されたエンドユーザ装置は、許可されたアクセスの証明が存在しない場合、上記ピアツーピア通信構造を介するＶｏＩＰ呼を受理することを拒否するように構成され、
上記許可された発呼側エンドユーザ装置は、上記許可された被呼側エンドユーザ装置のアドレスに関する情報を受信し、ＶｏＩＰ呼の開始前に、上記許可された被呼側エンドユーザ装置によって提供された認可証明書を検証するように構成され、上記認可証明書を検証することによりピアツーピア通信構造へのアクセスを可能にし、上記ＶｏＩＰ通信経路を介する上記許可された被呼側エンドユーザ装置への呼を確立し、
上記許可された発呼側エンドユーザ装置は、上記認可証明書を発行する責務を有する上記管理ノードと通信する必要なしに、上記許可された被呼側エンドユーザ装置からの認可証明書を検証して上記ＶｏＩＰ呼を確立するように構成されたピアツーピアシステム。
【請求項２】
上記管理ノードは、証明書認証の目的で、１組以上の秘密鍵と公開鍵のペアを生成し、１つ以上の上記秘密鍵を秘匿し、１つ以上の対応する上記公開鍵を上記ピアツーピア通信構造内で配布するように構成された請求項１に記載のピアツーピアシステム。
【請求項３】
上記管理ノードは、リベストーシャミールーアデルマン（ＲＳＡ）方式を用いて秘密鍵及び公開鍵のペアを生成するように構成された請求項２に記載のピアツーピアシステム。
【請求項４】
上記管理ノードは、
（ａ）エンドユーザ装置アカウントデータベースの提供、
（ｂ）上記ピアツーピア通信構造の同期時間基準の提供、
（ｃ）上記ピアツーピアシステムのグローバルに設定可能な設定情報の提供、
（ｄ）上記ピアツーピア通信構造のブート中のピアの発見、
（ｅ）新規エンドユーザ登録の取り扱い、及び、
（ｆ）上記ピアツーピア通信構造の所望の動作モードを制御するための上記ピアツーピア通信構造の動作の監視、

のうちの少なくとも１つを実行するように構成された請求項１記載のピアツーピアシステム。
【請求項５】
ＰＯＴＳ及び／又はＰＳＴＮと同時に動作するように構成された請求項１に記載のピアツーピアシステム。
【請求項６】
上記管理ノードは１つ以上のコンピュータサーバにより実現された請求項１に記載のピアツーピアシステム。
【請求項７】
上記管理ノードは、エンドユーザによる上記ピアツーピア通信構造への不正アクセスを検出するために、エンドユーザ登録及びシステム使用量データのヒューリスティックな不正検出解析を適用するように構成された請求項１記載のピアツーピアシステム。
【請求項８】
ピアツーピア通信構造において呼を確立する方法において、上記方法は、
ＶｏＩＰピアツーピアシステムへのアクセスを管理することを含み、
上記ＶｏＩＰピアツーピアシステムは、
複数の許可されたエンドユーザ装置を相互接続してＶｏＩＰ通信経路を介するＶｏＩＰ呼を支援する、実質的に分散型のピアツーピア通信構造を含み、上記複数の許可されたエンドユーザ装置は許可された発呼側エンドユーザ装置及び許可された被呼側エンドユーザ装置を含み、
上記ピアツーピア通信構造は、上記複数の許可されたエンドユーザ装置のそれぞれに各ユーザ名を関連付けることにより、許可されたエンドユーザの識別を行い、上記ユーザ名は上記ピアツーピア通信構造における電話番号として使用可能であり、
上記ピアツーピア通信構造は管理ノードを含み、上記管理ノードは、上記複数の許可されたエンドユーザ装置のそれぞれに認可証明書を発行して上記ピアツーピア通信構造における許可されたアクセスの証明を支援することにより、上記ピアツーピア通信構造の無許可の不正な使用を回避するように構成され、
上記複数の許可されたエンドユーザ装置は、許可されたアクセスの証明が存在しない場合、上記ピアツーピア通信構造を介するＶｏＩＰ呼を受理することを拒否するように構成され、
上記方法は、
上記許可された発呼側エンドユーザ装置において、上記管理ノードから少なくとも１つの認可証明書を受信することと、
上記許可された発呼側エンドユーザ装置において、上記許可された被呼側エンドユーザ装置のアドレスに関する情報を受信することと、
上記許可された発呼側エンドユーザ装置において、呼の開始前に、上記許可された被呼側エンドユーザ装置によって提供された認可証明書を検証し、上記認可証明書を検証することによりＶｏＩＰピアツーピア通信構造へのアクセスを可能にすることと、
上記許可された被呼側エンドユーザ装置によって提供された認可証明書を検証することに基づいて、上記ピアツーピア通信構造におけるＶｏＩＰ通信経路を介する上記許可された被呼側エンドユーザ装置へのＶｏＩＰ呼を確立することとを含む方法。
【請求項９】
上記管理ノードは、証明書認証の目的で、１組以上の秘密鍵と公開鍵のペアを生成し、１つ以上の上記秘密鍵を秘匿１つ以上の対応する上記公開鍵を許可されたエンドユーザ装置に配布するように構成された請求項８記載の方法。
【請求項１０】
上記管理ノードは、リベスト－シャミール－アデルマン（ＲＳＡ）方式を用いて秘密鍵及び公開鍵のペアを生成するように構成された請求項９記載の方法。
【請求項１１】
上記管理ノードは、

（ａ）エンドユーザ装置アカウントデータベースの提供、
（ｂ）上記ピアツーピア通信構造の同期時間基準の提供、
（ｃ）上記ピアツーピア通信構造のグローバルに設定可能な設定情報の提供、
（ｄ）上記ピアツーピア通信構造のブート中のピアの発見、
（ｅ）新規エンドユーザ登録の取り扱い、及び、
（ｆ）上記ピアツーピア通信構造の所望の動作モードを制御するための上記ピアツーピア通信構造の動作の監視、
のうちの少なくとも１つを実行するように構成された請求項８記載の方法。
【請求項１２】
上記ピアツーピア通信構造はＰＯＴＳ及び／又はＰＳＴＮと同時に動作するように構成された請求項８に記載の方法。
【請求項１３】
上記管理ノードは１つ以上の中央コンピュータサーバにより実現された請求項８に記載の方法。
【請求項１４】
上記管理ノードは、エンドユーザによる上記ピアツーピア通信構造への不正アクセスを検出するために、エンドユーザ登録及びシステム使用量データのヒューリスティックな不正検出解析を適用するように構成された請求項８に記載の方法。
【請求項１５】
非一時的なコンピュータ可読記憶媒体上に具現されたコンピュータプログラムにおいて、上記コンピュータプログラムは、少なくとも１つのコンピュータプロセッサによって実行されるコンピュータコードであって、ＶｏＩＰピアツーピアシステムにおいてＶｏＩＰ通信を支援することにより上記ＶｏＩＰピアツーピアシステムにおいて呼を確立するコンピュータコードを含み、
上記ＶｏＩＰピアツーピアシステムは、
複数の許可されたエンドユーザ装置を相互接続してＶｏＩＰ通信経路を介するＶｏＩＰ呼を支援する、実質的に分散型のピアツーピア通信構造を含み、上記複数の許可されたエンドユーザ装置は許可された発呼側エンドユーザ装置及び許可された被呼側エンドユーザ装置を含み、
上記ピアツーピア通信構造は、上記複数の許可されたエンドユーザ装置のそれぞれに各ユーザ名を関連付けることにより、許可されたエンドユーザの識別を行い、上記ユーザ名は上記ピアツーピア通信構造における電話番号として使用可能であり、
上記ピアツーピア通信構造は管理ノードを含み、上記管理ノードは、上記複数の許可されたエンドユーザ装置のそれぞれに認可証明書を発行して上記ピアツーピア通信構造における許可されたアクセスの証明を支援することにより、上記ピアツーピア通信構造の無許可の不正な使用を回避するように構成され、
上記複数の許可されたエンドユーザ装置は、許可されたアクセスの証明が存在しない場合、上記ピアツーピア通信構造を介するＶｏＩＰ呼を受理することを拒否するように構成され、
上記許可された発呼側エンドユーザ装置は、上記許可された被呼側エンドユーザ装置のアドレスに関する情報を受信し、呼の開始前に、上記許可された被呼側エンドユーザ装置によって提供された認可証明書を検証するように構成され、上記認可証明書を検証することにより上記ピアツーピアシステムへのアクセスを可能にし、上記許可された被呼側エンドユーザ装置への通信経路を介する呼を確立し、
上記許可された発呼側エンドユーザ装置は、上記認可証明書を発行する責務を有する上記管理ノードと通信する必要なしに、上記許可された被呼側エンドユーザ装置からの認可証明書を検証して上記ＶｏＩＰ呼を確立するように構成されたコンピュータプログラム。
【請求項１６】
非一時的なコンピュータ可読記憶媒体上に具現されたコンピュータプログラムにおいて、上記コンピュータプログラムは、少なくとも１つのコンピュータプロセッサによって実

行されてＶｏＩＰピアツーピアシステムにおいてＶｏＩＰ呼を確立するコンピュータコードを含み、
上記ＶｏＩＰピアツーピアシステムは、
複数の許可されたエンドユーザ装置を相互接続してＶｏＩＰ通信経路を介するＶｏＩＰ呼を支援する、実質的に分散型のピアツーピア通信構造を含み、上記複数の許可されたエンドユーザ装置は許可された発呼側エンドユーザ装置及び許可された被呼側エンドユーザ装置を含み、
上記ピアツーピア通信構造は、上記複数の許可されたエンドユーザ装置のそれぞれに各ユーザ名を関連付けることにより、許可されたエンドユーザの識別を行い、上記ユーザ名は上記ピアツーピア通信構造における電話番号として使用可能であり、
上記ピアツーピア通信構造は管理ノードを含み、上記管理ノードは、上記複数の許可されたエンドユーザ装置のそれぞれに認可証明書を発行して上記ピアツーピア通信構造における許可されたアクセスの証明を支援することにより、上記ピアツーピア通信構造の無許可の不正な使用を回避するように構成され、
上記複数の許可されたエンドユーザ装置は、許可されたアクセスの証明が存在しない場合、上記ピアツーピア通信構造を介するＶｏＩＰ呼を受理することを拒否するように構成され、
上記少なくとも１つのコンピュータプロセッサによって実行されるコンピュータコードは、
上記許可された発呼側エンドユーザ装置において、管理ノードから少なくとも１つの認可証明書を受信することと、
上記許可された発呼側エンドユーザ装置において、上記許可された被呼側エンドユーザ装置のアドレスに関する情報を受信することと、
上記許可された発呼側エンドユーザ装置において、上記ＶｏＩＰ呼の開始前に、上記許可された被呼側エンドユーザ装置によって提供された認可証明書を検証し、上記認可証明書を検証することにより上記ＶｏＩＰピアツーピアシステムへのアクセスを可能にすることとと、
を支援することにより、上記ＶｏＩＰピアツーピアシステムにおいて上記ＶｏＩＰ呼を確立し、
上記許可された発呼側エンドユーザ装置は、上記認可証明書を発行する責務を有する上記管理ノードと通信する必要なしに、上記許可された被呼側エンドユーザ装置からの認可証明書を検証して上記ＶｏＩＰ呼を確立するように構成されたコンピュータプログラム。
【請求項１７】
上記ＶｏＩＰ通信経路は呼のための通信経路である請求項１記載のピアツーピアシステム。
【請求項１８】
（ａ）エンドユーザの嗜好情報の取り扱いと、
（ｂ）ノード識別情報（ＩＤ）、ユーザ名、及びエンドユーザプロファイルデータのうちの１つ以上によるエンドユーザ識別情報の提供と、
（ｃ）基本的統計情報の維持と、
（ｄ）通信の通過をサポートするアドホックプロキシとして機能するネットワーク内のランダムピアノードを経由するファイアウォール及び／又はＮＡＴ（Network Address Translation）トラバーサルの維持と、のうちの少なくとも１つの機能を実行するように構成された請求項１記載のピアツーピアシステム。
【請求項１９】
ユーザ名の形式によるエンドユーザの識別情報が電話番号として使用され、上記ピアツーピア通信構造を介する呼が確立され、
上記呼は、電話呼、テレビ電話、及び電話会議のうちの１つであり、
上記ＶｏＩＰ通信経路はテキストメッセージングのために確立される請求項１記載のピアツーピアシステム。

【請求項２０】
実質的に分散型のピアツーピア通信構造を用いるＶｏＩＰピアツーピアシステムを備えたピアツーピアシステムであって、
上記ピアツーピア通信構造は、複数の許可されたエンドユーザ装置を相互接続してＶｏＩＰ通信経路を介するＶｏＩＰ呼を支援するように構成され、上記複数の許可されたエンドユーザ装置は許可された発呼側エンドユーザ装置及び許可された被呼側エンドユーザ装置を含み、
上記ピアツーピア通信構造は、上記複数の許可されたエンドユーザ装置のそれぞれに各ユーザ名を関連付けることにより、許可されたエンドユーザの識別を支援するように構成され、上記ユーザ名は上記ピアツーピア通信構造における電話番号として使用可能であり、
上記ピアツーピア通信構造は管理ノードを含み、上記管理ノードは、上記複数の許可されたエンドユーザ装置のそれぞれに認可証明書を発行して上記ピアツーピア通信構造における許可されたアクセスの証明を支援することにより、上記ピアツーピア通信構造の無許可の不正な使用を回避するように構成され、
上記複数の許可されたエンドユーザ装置は、許可されたアクセスの証明が存在しない場合、上記ピアツーピア通信構造を介するＶｏＩＰ呼を受理することを拒否するように構成され、
上記許可された発呼側エンドユーザ装置は、上記許可された被呼側エンドユーザ装置のアドレスに関する情報を受信し、呼の開始前に、上記許可された被呼側エンドユーザ装置によって提供された認可証明書を検証するように構成され、上記認可証明書を検証することにより上記ピアツーピア通信構造へのアクセスを可能にし、上記ＶｏＩＰ通信経路を介する上記許可された被呼側エンドユーザ装置へのＶｏＩＰ呼を確立し、
上記許可された発呼側エンドユーザ装置は、上記認可証明書を発行する責務を有する上記管理ノードと通信する必要なしに、上記許可された被呼側エンドユーザ装置からの認可証明書を検証して上記ＶｏＩＰ呼を確立するように構成されたピアツーピアシステム。
【請求項２１】
上記管理ノードは、証明書認証の目的で、１組以上の秘密鍵と公開鍵のペアを生成し、１つ以上の上記秘密鍵を秘匿し、１つ以上の対応する上記公開鍵を上記ピアツーピア通信構造内で配布するように構成された請求項２０記載のピアツーピアシステム。
【請求項２２】
上記管理ノードは、リベスト－シャミール－アデルマン（ＲＳＡ）方式を用いて秘密鍵及び公開鍵のペアを生成するように構成された請求項２１記載のピアツーピアシステム。
【請求項２３】
上記管理ノードは、
（ａ）エンドユーザ装置アカウントデータベースの提供、
（ｂ）上記ピアツーピア通信構造の同期時間基準の提供、
（ｃ）上記ピアツーピアシステムのグローバルに設定可能な設定情報の提供、
（ｄ）上記ピアツーピア通信構造のブート中のピアの発見、
（ｅ）新規エンドユーザ登録の取り扱い、及び、
（ｆ）上記ピアツーピア通信構造の所望の動作モードを制御するための上記ピアツーピア通信構造の動作の監視、
のうちの少なくとも１つを実行するように構成された請求項２０記載のピアツーピアシステム。
【請求項２４】
ＰＯＴＳ及び／又はＰＳＴＮと同時に動作するように構成された請求項２０記載のピアツーピアシステム。
【請求項２５】
上記管理ノードは１つ以上のコンピュータサーバにより実現された請求項２０記載のピアツーピアシステム。

【請求項２６】
上記管理ノードは、エンドユーザによる上記ピアツーピア通信構造への不正アクセスを検出するために、エンドユーザ登録及びシステム使用量データのヒューリスティックな不正検出解析を適用するように構成された請求項２０記載のピアツーピアシステム。
【請求項２７】
非一時的なコンピュータ可読記憶媒体上に具現されたコンピュータプログラムにおいて、上記コンピュータプログラムは、少なくとも１つのコンピュータプロセッサによって実行されるコンピュータコードであって、許可された発呼側エンドユーザ装置及び許可された被呼側エンドユーザ装置を含むＶｏＩＰピアツーピアシステムにおいてＶｏＩＰ通信を管理することにより上記ＶｏＩＰピアツーピアシステムにおいて呼を確立するコンピュータコードを含み、
上記ＶｏＩＰピアツーピアシステムは、
複数の許可されたエンドユーザ装置を相互接続してＶｏＩＰ通信経路を介するＶｏＩＰ呼を支援する、実質的に分散型のピアツーピア通信構造を含み、上記複数の許可されたエンドユーザ装置は上記許可された発呼側エンドユーザ装置及び上記許可された被呼側エンドユーザ装置を含み、
上記ピアツーピア通信構造は、上記複数の許可されたエンドユーザ装置のそれぞれに各ユーザ名を関連付けることにより、許可されたエンドユーザの識別を行い、上記ユーザ名は上記ピアツーピア通信構造における電話番号として使用可能であり、
上記ピアツーピア通信構造は管理ノードを含み、上記管理ノードは、上記複数の許可されたエンドユーザ装置のそれぞれに認可証明書を発行して上記ピアツーピア通信構造における許可されたアクセスの証明を支援することにより、上記ピアツーピア通信構造の無許可の不正な使用を回避するように構成され、
上記複数の許可されたエンドユーザ装置は、許可されたアクセスの証明が存在しない場合、上記ピアツーピア通信構造を介するＶｏＩＰ呼を受理することを拒否するように構成され、
上記許可された発呼側エンドユーザ装置は、上記許可された被呼側エンドユーザ装置のアドレスに関する情報を受信し、呼の開始前に、上記許可された被呼側エンドユーザ装置によって提供された認可証明書を検証するように構成され、上記認可証明書を検証することにより上記ピアツーピアシステムへのアクセスを可能にし、上記ＶｏＩＰ通信経路を介する上記許可された被呼側エンドユーザ装置への呼を確立し、
上記許可された発呼側エンドユーザ装置は、上記認可証明書を発行する責務を有する上記管理ノードと通信する必要なしに、上記許可された被呼側エンドユーザ装置からの認可証明書を検証して上記ＶｏＩＰ呼を確立するように構成されたコンピュータプログラム。
【請求項２８】
上記ＶｏＩＰ通信経路は呼のための通信経路である請求項２０記載のピアツーピアシステム。
【請求項２９】
（ａ）エンドユーザの嗜好情報の取り扱いと、
（ｂ）ノード識別情報（ＩＤ）、ユーザ名、及びエンドユーザプロファイルデータのうちの１つ以上によるエンドユーザ識別情報の提供と、
（ｃ）基本的統計情報の維持と、
（ｄ）通信の通過をサポートするアドホックプロキシとして機能するネットワーク内のランダムピアノードを経由するファイアウォール及び／又はＮＡＴ（Network Address Translation）トラバーサルの維持と、のうちの少なくとも１つの機能を実行するように構成された請求項２０記載のピアツーピアシステム。
【請求項３０】
ユーザ名の形式によるエンドユーザの識別情報が電話番号として使用され、上記ピアツーピア通信構造を介する呼が確立され、
上記呼は、電話呼、テレビ電話、及び電話会議のうちの１つであり、

上記ＶｏＩＰ通信経路はテキストメッセージングのために確立される請求項２０記載のピアツーピアシステム。

【請求項３１】

ピアツーピア通信構造において呼を確立する方法において、上記方法は、

ＶｏＩＰピアツーピアシステムへのアクセスを支援することを含み、

上記ＶｏＩＰピアツーピアシステムは、

複数の許可されたエンドユーザ装置を相互接続してＶｏＩＰ通信経路を介するＶｏＩＰ呼を支援する、実質的に分散型のピアツーピア通信構造を含み、上記複数の許可されたエンドユーザ装置は許可された発呼側エンドユーザ装置及び許可された被呼側エンドユーザ装置を含み、

上記ピアツーピア通信構造は、上記複数の許可されたエンドユーザ装置のそれぞれに各ユーザ名を関連付けることにより、許可されたエンドユーザの識別を行い、上記ユーザ名は上記ピアツーピア通信構造における電話番号として使用可能であり、

上記ピアツーピア通信構造は管理ノードを含み、上記管理ノードは、上記複数の許可されたエンドユーザ装置のそれぞれに認可証明書を発行して上記ピアツーピア通信構造における許可されたアクセスの証明を支援することにより、上記ピアツーピア通信構造の無許可の不正な使用を回避するように構成され、

上記複数の許可されたエンドユーザ装置は、許可されたアクセスの証明が存在しない場合、上記ピアツーピア通信構造を介するＶｏＩＰ呼を受理することを拒否するように構成され、

上記方法は、

上記許可された発呼側エンドユーザ装置において、上記管理ノードから少なくとも１つの認可証明書を受信することと、

上記許可された発呼側エンドユーザ装置において、上記許可された被呼側エンドユーザ装置のアドレスに関する情報を受信することと、

上記許可された発呼側エンドユーザ装置において、呼の開始前に、上記許可された被呼側エンドユーザ装置によって提供された認可証明書を検証し、上記認可証明書を検証することによりＶｏＩＰピアツーピア通信構造へのアクセスを可能にすることと、

上記許可された被呼側エンドユーザ装置によって提供された認可証明書を検証することに基づいて、上記ピアツーピア通信構造におけるＶｏＩＰ通信経路を介する上記許可された被呼側エンドユーザ装置への呼を確立することとを含み、

上記許可された発呼側エンドユーザ装置は、上記認可証明書を発行する責務を有する上記管理ノードと通信する必要なしに、上記許可された被呼側エンドユーザ装置からの認可証明書を検証して上記ＶｏＩＰ呼を確立するように構成された方法。

【請求項３２】

上記管理ノードは、証明書認証の目的で、１組以上の秘密鍵と公開鍵のペアを生成し、１つ以上の上記秘密鍵を秘匿１つ以上の対応する上記公開鍵を許可されたエンドユーザ装置に配布するように構成された請求項３１記載の方法。

【請求項３３】

上記管理ノードは、リベストーシャミールーアデルマン（ＲＳＡ）方式を用いて秘密鍵及び公開鍵のペアを生成するように構成された請求項３２記載の方法。

【請求項３４】

上記管理ノードは、

（ａ）エンドユーザ装置アカウントデータベースの提供、

（ｂ）上記ピアツーピア通信構造の同期時間基準の提供、

（ｃ）上記ピアツーピア通信構造のグローバルに設定可能な設定情報の提供、

（ｄ）上記ピアツーピア通信構造のブート中のピアの発見、

（ｅ）新規エンドユーザ登録の取り扱い、及び、

（ｆ）上記ピアツーピア通信構造の所望の動作モードを制御するための上記ピアツーピア通信構造の動作の監視、

のうちの少なくとも１つを実行するように構成された請求項３１記載の方法。
【請求項３５】
上記ピアツーピア通信構造はＰＯＴＳ及び／又はＰＳＴＮと同時に動作するように構成された請求項３１記載の方法。
【請求項３６】
上記管理ノードは１つ以上の中央コンピュータサーバにより実現された請求項３１記載の方法。
【請求項３７】
上記管理ノードは、エンドユーザによる上記ピアツーピア通信構造への不正アクセスを検出するために、エンドユーザ登録及びシステム使用量データのヒューリスティックな不正検出解析を適用するように構成された請求項３１記載の方法。
【請求項３８】
非一時的なコンピュータ可読記憶媒体上に具現されたコンピュータプログラムにおいて、上記コンピュータプログラムは、少なくとも１つのコンピュータプロセッサによって実行されてＶｏＩＰピアツーピアシステムにおいてＶｏＩＰ呼を確立するコンピュータコードを含み、
上記ＶｏＩＰピアツーピアシステムは、
複数の許可されたエンドユーザ装置を相互接続してＶｏＩＰ通信経路を介するＶｏＩＰ呼を支援する、実質的に分散型のピアツーピア通信構造を含み、上記複数の許可されたエンドユーザ装置は許可された発呼側エンドユーザ装置及び許可された被呼側エンドユーザ装置を含み、
上記ピアツーピア通信構造は、上記複数の許可されたエンドユーザ装置のそれぞれに各ユーザ名を関連付けることにより、許可されたエンドユーザの識別を行い、上記ユーザ名は上記ピアツーピア通信構造における電話番号として使用可能であり、
上記ピアツーピア通信構造は管理ノードを含み、上記管理ノードは、上記複数の許可されたエンドユーザ装置のそれぞれに認可証明書を発行して上記ピアツーピア通信構造における許可されたアクセスの証明を支援することにより、上記ピアツーピア通信構造の無許可の不正な使用を回避するように構成され、
上記複数の許可されたエンドユーザ装置は、許可されたアクセスの証明が存在しない場合、上記ピアツーピア通信構造を介するＶｏＩＰ呼を受理することを拒否するように構成され、
上記コンピュータプログラムは、上記少なくとも１つのコンピュータプロセッサによって実行されるコンピュータコードであって、
上記許可された発呼側エンドユーザ装置において、上記管理ノードから少なくとも１つの認可証明書を受信することと、
上記許可された発呼側エンドユーザ装置において、上記許可された被呼側エンドユーザ装置のアドレスに関する情報を受信することと、
上記許可された発呼側エンドユーザ装置において、呼の開始前に、上記許可された被呼側エンドユーザ装置によって提供された認可証明書を検証し、上記認可証明書を検証することにより上記ＶｏＩＰピアツーピアシステムへのアクセスを可能にすることと、
上記許可された被呼側エンドユーザ装置によって提供された認可証明書を検証することに基づいて、上記ピアツーピアシステムにおけるＶｏＩＰ通信経路を介する上記許可された被呼側エンドユーザ装置へのＶｏＩＰ呼を確立することと、
を含むコンピュータコードを含み、
上記許可された発呼側エンドユーザ装置は、上記認可証明書を発行する責務を有する上記管理ノードと通信する必要なしに、上記許可された被呼側エンドユーザ装置からの認可証明書を検証して上記ＶｏＩＰ呼を確立するように構成されたコンピュータプログラム。

フロントページの続き

(72)発明者　プリイト・カセサル
エストニア、エーエー１３８１１タリン、マハトラ２５－５７番

Ｆターム(参考) 5J104 AA07 AA16 AA32 EA02 EA04 EA19 GA03 JA21 KA02 NA02
NA37 NA38 PA07
5K201 AA08 BD06 CA02 FA07

【外国語明細書】
WO 2005/009019 PCT/IB2004/002282

PEER-TO-PEER TELEPHONE SYSTEM

Field of the invention

The present invention relates to telecommunications systems, for example to telephone systems as well as to decentralized telecommunications systems operating according to a peer-to-peer principle. Moreover, the invention also relates to methods of operating such telephone systems and telecommunications systems.

Background to the invention

Contemporary telecommunications systems presently deployed, for example "public switched telephony network" (PSTN), mobile telephone and "Voice over Internet protocol" (VoIP), are substantially centralized in nature. They often employ central exchanges linked to users through trunk lines, local metro-rings and similar distribution structures. More recently, software-operated end-user devices have become available for connecting to such contemporary telephone systems, for example desk telephones, mobile telephones and VoIP devices. However, for performing almost any function offered by the telephony service provider, end-user devices are obliged to communicate with a central telephone exchange and/or branch exchange which executes one or more desired functions for them. In most cases, two end-user telephones of such a contemporary telephone system are not able to communicate directly to one another without a central exchange of the system linking the two end-user telephones together. For example, two people using their mobile telephones to converse together is facilitated by their two telephones communicating by radio via one or more mobile base stations, such base station communication being required even when the two people and their associated mobile telephones are in the same building. In another example, two people using "Voice over IP" software to converse together over the public Internet is facilitated by their software applications communicating via a central server, such server being required even though a connection can be established directly between the two people.

The use of centralized telephone systems places considerable demands on central switching exchanges. Such central exchanges are increasingly dependent on wide bandwidth optical connections employing dense wavelength division multiplexing (DWDM) with up to 120 optical channels distributed into wavelength bands of 50 GHz frequency spacing at an optical carrier frequency in the order of 300 THz. Such centralized exchanges are extremely costly and complex items of equipment which are susceptible to occasional malfunction, such malfunction potentially resulting in loss of communication traffic therethrough with potential corresponding compensation payments due to

customers. Moreover, the cost of operating such central exchanges scales proportionally with the number of end users.

The inventors of the present invention have appreciated that such a centralized approach is sub-optimal in many situations and that advantages arise from the deployment of other alternative telephone system architectures.

In order to address issues arising from adoption of such alternative architectures, the inventors have devised the present invention.

Summary of the invention

A first object of the invention is to provide a substantially decentralized telephone network system.

A second object of the invention is to provide such a decentralized telephone system in which subscriber authentication, network access control and accounting are performable in a more robust and reliable manner.

A third object of the invention is to provide a decentralised telephone system operable to reduce concentration of communication traffic therein by transferring responsible for establishing connections to end-users of the system.

According to a first aspect of the present invention, there is provided a peer-to-peer telephone system comprising a plurality of end-users and a communication structure through which one or more end-users are couplable for communication purposes, characterised in that:

(a) the communication structure is substantially de-centralized with regard to communication route switching therein for connecting said one or more end-users;

(b) said one or more end-users are operable to establish their own communication routes through the structure based on verification of one or more authorisation certificates to acquire access to the structure; and

(c) said structure includes administrating means for issuing said one or more certificates to said one or more end-users.

The invention is of advantage in that it is capable of addressing at least one of the aforementioned objects of the invention.

The invention is capable of addressing issues associated with less-centralized architectures, namely issues of control and user-authorisation, for example for billing/invoicing purposes to which the present invention is directed.

Preferably, in the system, the administrating means is operable to administer at least one of end-user sign-up and end-user payment for access to the communication structure.

More preferably, for example to try to circumvent unauthorised free and/or fraudulent use of the system, the administrating means is operable to generate one or more private-public key pairs, the administrating means being operable to maintain said one or more private keys secret and to distribute said one or more corresponding public keys within the system for certificate authentication purposes. Yet more preferably in the system, the administrating means is operable to generate private-public key pairs using a Rivest-Shamir-Adelman (RSA) method.

Preferably, for purposes of enhancing network robustness in the system, the structure includes a peer-to-peer communication network through which the end-users are mutually connectable. More preferably, the peer-to-peer network is implemented as a combination of interfacing nodes and storage nodes, said storage nodes being configured in one or more slots for database access purposes. Beneficially, the structure is implemented by way of a proprietary Global Index peer-to-peer network technology.

Preferably, in the system, the administrating means is arranged to perform one or more of:

(a) providing an end-user accounts database;
(b) providing a synchronizing time reference for the communication structure;
(c) providing globally-configurable settings for the system;
(d) providing peer discovery during bootstrap of the structure;
(e) handling new end-user registration; and
(f) monitoring operation of the structure for controlling desired modes of operation thereof.

Preferably, in the system, a plurality of end-users are operable to mutually exchange their authorisation certificates prior to commencing communication therebetween where at least one of said certificates is identified to be authentic.

Preferably, for example to assist adoption of the system in practice, the structure is arranged to support end-user free-trial use of the system, such free-trial use being subject to administration from the administrating means by repeated issuing of authorisations.

Preferably, the administrating means is operable to invoice one or more end-users on a flat-fee rate substantially irrespective of use of the system exercised by said one or more end-users.

Preferably, in order to promote usage of the system in existing deployed equipment, the system is arranged to be configurable to operate concurrently with POTS and/or PSTN. Abbreviations POTS and PSTN correspond to "Plain Old Telephone System" and "Public Switch Telephone Network" respectively.

Preferably, the administrating means is implemented by way of one or more central computer servers. Such an implementation is especially beneficial when the system is configured in conjunction with the public Internet. Alternatively, the administrating means is otherwise susceptible to being implemented in a substantially de-centralized manner.

Preferably, the administrating means is operable to apply an heuristics fraud detection analysis of end-user registration and system usage data for detecting fraudulent access to the system by end-users.

According to a second aspect of the present invention, there is provided a method of operating a peer-to-peer telephone system comprising a plurality of end-users and a communication structure through which one or more end-users are couplable for communication purposes, characterised in that the method includes steps of:

(a) arranging for the communication structure to be substantially de-centralized with regard to communication route switching therein for connecting said one or more end-users;

(b) arranging for said one or more end-users to be operable to establish their own communication routes through the structure based on verification of one or more authorisation certificates to acquire access to the structure; and

(c) arranging for said structure to include administrating means for issuing said one or more certificates to said one or more end-users.

The method is of advantage in that its application to the system is capable of addressing at least one of the objects of the invention.

Preferably, in the method, the administrating means is operable to administer at least one of end-user sign-up and end-user payment for access to the communication structure.

Preferably, in the method, the administrating means is operable to generate one or more private-public key pairs, the administrating means being operable to maintain said one or more private keys secret and to distribute said one or more corresponding public keys within the system for certificate authentication purposes.

Preferably, in the method, the administrating means is operable to generate private-public key pairs using a Rivest-Shamir-Adelman (RSA) method. However, other approaches to private-public key generation are also susceptible to being used in the method.

Preferably, in the method, the structure includes a peer-to-peer communication network through which the end-users are mutually connectable. More preferably, the peer-to-peer network is implemented as a combination of interfacing nodes and storage nodes, said storage nodes being configured in one or more slots for database access purposes.

Preferably, in the method, the administrating means is arranged to perform one or more of:

(a) providing an end-user accounts database;
(b) providing a synchronizing time reference for the communication structure;
(c) providing globally-configurable settings for the system;
(d) providing peer discovery during bootstrap of the structure;
(e) handling new end-user registration; and
(f) monitoring operation of the structure for controlling desired modes of operation thereof.

Preferably, in the method, a plurality of end-users are operable to mutually exchange their authorisation certificates prior to commencing communication therebetween where at least one of said certificates is identified to be authentic.

Preferably, to encourage adoption of the system, the method is implemented such that the structure is arranged to support end-user free-trial use of the system, such free-trial use being subject to administration from the administrating means by repeated issuing of authorisations.

Preferably, in the method, the administrating means is operable to invoice one or more end-users on a flat-fee rate substantially irrespective of use of the system exercised by said one or more end-users.

Preferably, in order to encourage use of the system where existing telephone infrastructure exists, the method is implemented such that the system is arranged to be configurable to operate concurrently with POTS and/or PSTN. Abbreviations POTS and PSTN correspond to "Plain Old Telephone System" and "Public Switched Telephone Network" respectively.

Preferably, in the method, the administrating means is implemented by way of one or more central computer servers.

Preferably, in order to avoid fraudulent use of the system when implementing the method, the administrating means is operable to apply an heuristics fraud detection analysis of end-user registration and system usage data for detecting fraudulent access to the system by end-users.

According to a third aspect of the present invention, there is provided software operable to implement at least part of the telephone system according to the first aspect of the invention.

According to a fourth aspect of the invention, there is provided software operable to execute at least part of the method according to the second aspect of the invention.

It will be appreciated that features of the invention are susceptible to being combined in any combination without departing from the scope of the invention.

Diagrams of embodiments of the invention

Embodiments of the invention will now be described, by way of example only, with reference to the following diagrams wherein:

Figure 1 is a schematic diagram of a telephone system according to the present invention; and

Figure 2 is a schematic representation of a per-to-peer structure of the system of Figure 1.

Description of embodiments of the invention

A telephone system according to the present invention is substantially a decentralised structure comprising a spatially distributed array of end-users connected by way of a peer-to-peer communication network. The structure is substantially devoid of any form of centralized exchange except for one or more administration nodes for performing some specific network administration functions such as subscriber sign-up and payment for communication network usage. In the decentralised structure, most routine functions, for example placing a telephone call, are handled entirely by end-user devices operable to communicate substantially directly to each other or via some form of local exchange such as an optical metro ring or distributed relay nodes on the public Internet.

In a system according to the present invention, the system indicated generally by 10 in Figure 1, a first end-user (FEU) 20 of the system 10 desiring to send a message to a second end-user (SEU) 30 thereof adopts a method of communication as follows:

(a) the first end-user 20 locates the second end-user 30; such location is executed by way of peer-to-peer technologies, for example using a "Global Index" (GI) proprietary peer-to-peer technology which will be described later and/or contemporary "Distributed Hash Table" technology, arranged to provide node look-up functionality;

(b) the first end-user 20 receives information regarding the address of the second end-user 30 and also details of one or more communication path-ways 50, 60 which may be used for making a connection from the first end-user 20 to the second end-user 30; and

(c) the first end-user 10 then follows a protocol to establish the one or more communication pathways 50, 60 to the second end-user 30.

In the GI peer-to-peer technology, there is provided a network of participating nodes interlinked through a distributed communication network. The participating nodes are allocated to be either interfacing nodes or storage nodes. Preferably, the number of storage nodes is arranged to be considerably less than the number of interfacing nodes, for example 100 times more interfacing nodes than storage nodes. Moreover, the storage nodes are responsible for storing data records whereas the interfacing nodes are responsible for processing queries and sending requests to the storage nodes for sending data records therefrom in response to the queries. Moreover, the interfacing nodes are also responsible for receiving data records to be stored and determining one or more appropriate groups of storage nodes to receive the data records for storage therein. The storage nodes are arranged in groups known as slots wherein association of a given storage node with a particular slot is dependent upon address data held in each of the storage nodes. The GI technology is described in a patent application approximately contemporary with the present patent application, the contents of the GI technology patent application herewith being incorporated by reference for purposes of describing the telephone system of the present invention.

In the system 10, there is a considerable requirement for subscriber authentication, access control and accounting. Using major system functions of the system 10 is only possible if one or more end-users thereof have paid or otherwise have authorized access to such functions. In a contemporary conventional telephone system, end-user access to one or more major system functions is checked by a central office thereof in a manner of centralised control. In contradistinction, in the system 10, access is checked by end-user devices using public-key cryptography. In such cryptography, each end-user, also referred to as subscriber, has associated therewith a cryptography key pair which is created by the end-user's device. Upon subscriber sign-up or payment, a central office of

the system 10 issues to the subscriber a digital certificate, such certificate also being referred to as a User Identity Certificate (UIC), whereby the central office certifies that the owner of this key pair is an authorised subscriber.

In step (c) of the aforementioned method, when the first end-user 20 communicates with other subscriber devices, namely the second end-user 30, the first end-user 20 provides the certificate, namely the aforementioned UIC, as a proof of subscription. In the system 10, end-user devices are arranged to refuse to mutually communicate where there exists an absence of such proof of subscription. Moreover, using public-key cryptography, end-user devices of the system 10 are arranged to be operable to verify each other's certificates (UIC's) without needing to communicate with the aforesaid central office of the system 10 responsible for issuing certificates (UIC's). The system 10 thus functions in a de-centralized manner on account of the end-users 20, 30 not needing to communicate with the central office of the system 10 when establishing a communication route between the end-users 20, 30.

When a subscribing device of the system, for example the first end-user 20, has located a recipient, for example the second end-user 30, they will subsequent need to mutually communicate. Such communication is preferably by a direct route, for example along the path-way 60 illustrated in Figure 1. However, for example for reasons of spatial separation and/or terrain, such a direct route is not always technically feasible; for example, if communication is desired from the first end-user 20 to the second end-user 30 via the public Internet, such communication is not feasible when the second end-user 30 has a private address that is not accessible from outside a local network of the system 10. In a situation where direct communication is not feasible, the system 10 is operable to route communication via one or more peer nodes in its peer-to-peer structure 80 to assist the first and second end-users 20, 30 to mutually communicate. These one or more peer nodes are preferably implemented by subscriber devices that need not necessarily belong to the first and second end-users 20, 30 involved in making a telephone call therebetween. Thus, for example, in such a scenario where direct connection is not feasible, a subscriber communicates to another device that is directly accessible, and this other device communicates directly with the final recipient.

Architectural aspects of the system 10 will now be described in further detail. The peer-to-peer structure 80 is subdivided into two sections as illustrated in Figure 2, namely central servers (CS) 100 on the one hand and a peer-to-peer network (P2PN) 110 on the other hand.

The central servers 100 are preferably operated by the proprietor of the structure 80. These servers 100 are arranged to execute one or more of the following tasks:

(i) providing an end-user accounts database for recording end-users' accounting details;

(ii) providing a synchronizing time reference for the structure 80;

(iii) providing globally-configurable settings for the system 10;

(iv) providing peer discovery during bootstrap of the structure 80 and handling new end-user registration;

(v) electronically signing critical information pertinent to the system 10, for example signing end-user identities as described in the foregoing, for example the aforementioned User Identity Certificates (UIC's), using digital signatures using secret cryptographic keys known only to the proprietor of the system 10;

(vi) providing add-on services from one or more of the proprietor's infrastructure, rented infrastructure and outsourced infrastructure; and

(vii) monitoring operation of the central servers 100 and the network 110 for ensuring desired modes of operation thereof.

The add-on services referred in (vi) above relate to one or more of:

(1) "Public Switched Telephone Network" (PSTN) and/or "plain old telephone system" (POTS) connectivity, to "Voice over Internet Protocol " (VoIP) traffic termination and reverse thereof, for example from POTS to the proprietor's system 10;

(2) handling "Instant Message" (IM) to "Short Message Service" (SMS) connectivity; and

(3) handling end-user conferencing, voicemail and similar activities couplable to back-end servers included within the central servers 100.

The peer-to-peer network 110 preferably comprises end-user computing devices arranged to execute thereon software provided by the proprietor of the system 10. The network 110 is also preferably based on a version of the aforementioned GI protocol customized by the proprietor of the system 10. The network 110 is operable to perform functions preferably including one or more of:

(a) administering end-user buddy lists;

(b) handling end-user preferences, for example buddy online/offline notification;

(c) providing end-user identification by way of one or more of the following: node identification (ID), username, end-user profile data;

(d) maintaining basic statistics, for example a number of end-users currently actively communicating within the system 10; and

(e) maintaining firewall and/or "Network Address Translation" (NAT) traversal via random peer nodes within the network 110 functioning as ad hoc proxies supporting communication therethrough.

In (c) above pertaining to the peer-to-peer network 110, the username is effectively useable as a "telephone number" within the system 10. Moreover, the end-user profile data relates to data records if provided by the end-users, such records including one or more of: real name (e.g. Roger Smith, Annie Hansen), spatial location (e.g. Washington USA; Copenhagen, Denmark), date of birth and e-mail address.

The inventors have appreciated that operation of the system 10 is dependent on security provided by, for example, the use of public key encryption therein. In devising the system 10, the inventors have further anticipated that a peer-to-peer IM/VoIP system is inherently less secure than POTS or any comparable telephone system reliant on one or more central servers; as in the foregoing, abbreviations IM, VoIP and POTS refer to "Instant Messaging", "Voice over Internet Protocol" and "Plain Old Telephone System" respectively. In the system 10, the inventors have arranged for the use of contemporary Rivest-Shamir-Adelman (RSA) public key encryption and associated digital signatures to cater for most basic security requirements within the system 10. However, it will be appreciated that other types of public-private key encryption are susceptible to being employed in the system 10.

Upon an end-user, for example one of the end-users 20, 30, seeking registration at the central servers 100, the end-user proceeds to generate a RSA encryption key pair, namely complementary private and public keys wherein said private key is not derivable from said public key and vice versa. The end-user's public key appears in the User Identity Certificate (UIC) provided to the end-user, whereas the private key is stored locally at the end-users premises.

During a call set-up from the first end-user 20 to the second end-user 30, similarly during an Instant Message (IM) sending, prior to commencing communication, both end-users 20, 30 present their User Identity Certificate (UIC), or Temporary Identification Number (TIN) where the system 10 is set up to accept these, as appropriate to the other; if they have a user name, they present their UIC. If a UIC is presented from a primary one of the end-users 20, 30 to a secondary one thereof, the secondary end-user verifies the signature provided by the primary end-user, such verification not requiring any contact with the central servers 100. Moreover, the secondary end-user verifies that the primary end-user has the corresponding secret key by issuing a challenge data packet for the primary end-user's public key and checks that the primary end-user is capable of decrypting it. After completion of such activities, the primary end-user is in a position to safely believe that the primary end-user legitimately has the username it claims to hold.

When calls are made within the system 10, additional checking is required because calls require payment unless permission for a limited trial period has been granted. In the system 10, it is difficult to monitor in a secure manner duration of calls or number of calls

made; in this respect, the inventors have appreciated that it is advantageous to employ a time-based subscription as a basis of billing/invoicing within the system 10. Thus, in order to implement such time-based subscription, User Identity Certificate (UIC) privileges are checked and non-trial calls are not communicated through the peer-to-peer network 110 if neither of the end-users 20, 30 in the above example has a User Identity Certificate (UIC) with non-expired subscription privileges. In other words, a call will propagate through the peer-to-peer network 110 if one or more of the end-users 20, 30 has a valid subscription or trial.

To keep their subscriptions from expiring, end-users of the system 10 are obliged to renew their User Identity Certificate (UIC) periodically for instance by paying a fee for a coming month/year; it will be appreciated that other payment periods are possible or that UICs may be extended based on other criteria than payment. Upon receipt of renewal payments, the central servers 100 are operable to issue new UIC's in response in the earlier end-users' names, the new UIC's having associated new subscription privilege expiry details. When credit/debit card billing/invoicing has been authorised by one or more of the end-users of the system 10, billing/invoicing is susceptible to being performed automatically by the central servers 100 without the need for associated end-user intervention.

Thus, in the system 10, a preferred method of payment for calls made is by flat-fee monthly or yearly subscription entitling the user to an unlimited number of calls in the system 10. Such a billing/invoicing arrangement is acceptable in the system 10 from a business perspective because calls made do not incur operating expenses to the proprietor of the system 10 as central exchange resources are substantially not utilized when making such calls. In contradistinction, calls to or from POTS/PSTN incur real per-minute operating costs and are therefore appropriately charged separately and distinctly from calls made according to the invention in the system 10.

When the peer-to-peer structure 80 is implemented in the manner of the aforementioned GI protocol, the end-users 20, 30 in Figure 1 together with other end-users not shown, the central servers 100 and the peer-to-peer network 110 are effectively participating nodes. In such a configuration, each end-user advertises its presence to GI storage nodes by periodically sending thereto its information about its identity or Temporary Identification Number (TIN) when the system 10 is configured to accept such TIN's. When one or more end-users make GI queries, for example akin to telephone directory enquiries, the storage nodes are responsive to send such stored User Identity Certificates (UIC) or Temporary Identification Numbers (TIN) as data packets in response to such queries.

In the case of UIC's, corresponding data packets despatched by the GI storage nodes are received at end-users which sign off the data packets with their end-user private keys;

one or more querying end-users are thereby capable of verifying authenticity of the data packets received thereat, for example in response to making an enquiry, using a corresponding public key. Such an arrangement is advantageous because it is substantially capable of guaranteeing that no-one is able to fake User Identity Certificate (UIC) end-user directory entries. The rationale of such an approach is that a participating node who owns a User Identity Certificate (UIC) is operable, for example when advertising its presence, to send its private-key-signed data packets corresponding to its UIC to one or more storage nodes and another participating node if required. The signed UIC received from one or more of the storage nodes and stored therein for subsequent release is verifiable at an enquiring participating node by using a corresponding public key. Such an arrangement is capable of circumventing tampering with UIC and even faked UIC's.

The system 10 is further provided with a free-trial facility, such a facility being of commercial advantage for purposes of attracting new end-users to the system 10. Preferably, such a free-trial facility pertains to X_1 free days or, alternatively or additionally, X_2 free calls. For such free-trial days or calls, the central servers 100 are required to provide explicit permission for each free call made. Preferably, all permissions given or requested are recorded in a database of the system 10, for example for heuristic fraud detection purposes as described later. If the end-user has already used up free days and/or free calls allocated thereto, permission is not granted from the central servers 100 and the end-user is subsequently requested to pay if it still desires to make calls within the system 10.

The system 10 is capable of being operated concurrently within, or in combination with, a conventional telephone system, for example a conventional telephone system capable of implementing the Internet.

The aforementioned free-trial permission scheme is intended by the inventors only to pertain to the system 10. For conventional paid subscription calls undertaken in connection with the system 10, a normal conventional subscription regime applies and per-call permissions are neither requested nor recorded. For PSTN calls, a free-trial scheme does not pertain although it is potentially capable of being provided in connection with the system 10.

For each free-call permission request received in the system 10, the central servers 100 are operable to record at least one of the following parameters with regard to a call:

(a) calling end-user's identity in the form of a username or Temporary Identification Number (TIN);

(b) calling end-user's computer identification (ID);

(c) calling end-user's Internet Protocol (IP) address;

(d) called end-user's identity in the form of a username or TIN;
(e) called end-user's computer ID;
(f) called end-user's IP address;
(g) time and date of the call;
(h) whether or not permission was granted for the call.

Thus, in the system 10, a "trial user" explicit status is not accommodated; preferably, there is merely a need for an end-user to make some free calls from a defined starting date D. Any end-user is entitled to make free calls if its first free calls were less than X_1 days ago (or the end-user has not yet exercised a free-call option within the system 10). Alternatively, the system 10 may be set up in such a way as to allow a free-trial period to consist of X number of free calls as opposed to X days.

Hacked version of system 10 software enables fraudulent end-users to omit free-trial permission asking and permission checking provisions employed within the system 10. However, on account of the system 10 implementing both calling end-user and called end-user permission checking, such hacking only enables fraudulent end-users to call other fraudulent end-users free of charge; in other words, pirated fraudulent end-user software is only capable of providing very limited benefit when employed on the system 10. In many cases, such limited fraudulent use of the system 10 can be accommodated without significant financial loss to the proprietor of the system 10.

The inventors have appreciated that a major opportunity of fraud exists in the system 10 when a hacker attempts to fake a username or computer ID and repetitively starts new free trials. Such a major opportunity of fraud requires the hacker to omit from system 10 compatible software all local shareware-type checks. In order to counteract such fraud, the central servers 100 are programmed to perform heuristic fraud detection to identify repetitive fraud patterns. For example, the central servers 100 are operable to detect a fraudulent end-user seeking free-call provisions Z times and then subsequently seeking with the same IP address and new computer ID for new free-call permission to call the same people. Since explicit permission for free calls in the system 10 is required from the central servers 100, there is considerable information available within the system 10 for input to such heuristics fraud detection software executing within the system 10. However, the inventors are aware that such heuristics fraud detection is unlikely to detect all cases of hacking occurring within the system 10.

It will be appreciated that embodiments of the invention described above are susceptible to being modified without departing from the scope of the invention.

In the foregoing, the system 10 is described as being able to support the use of Temporary Identification Numbers (TINs). However, the system 10 is capable of being

modified so that TINs are not utilized therein, such that user names and associated User Identity Certificates (UIC's) with associated time-limited substantially cost-free privileges are employed for free-trial purposes. If required, the system 10 is even susceptible to being configured so that free-trial usage as described earlier is not provided to end-users; alternatively, other arrangements for free trials can be utilized, for example reimbursement of initial paid subscription fee.

The system 10 is preferably implemented, at least in part, using software executable on computing hardware. Such software can be distributed to users via a communication network such as the Internet and/or via the software stored on a suitable data carrier such as a CD ROM supplied to users.

In the foregoing description of embodiments of the invention relating to the telephone system 10, it will be appreciated that the invention is relevant to telecommunications systems in general and the term "telephone" should therefore be construed accordingly. Specifically, other forms of communication susceptible to being performed with the system include video calls, conference calls and text messaging.

In the foregoing, terms such as "contain", "include", comprise", "have", "has", "is", "are", "incorporate" and "encompass" are intended to be construed as being non-exclusive, namely other items not disclosed are also potentially present.

CLAIMS

1. A peer-to-peer telephone system (10) comprising a plurality of end-users (20, 30) and a communication structure (80) through which one or more end-users (20, 30) are couplable for communication purposes, characterised in that:

(a) the communication structure (80) is substantially de-centralized with regard to communication route switching therein for connecting said one or more end-users (20, 30);

(b) said one or more end-users (20, 30) are operable to establish their own communication routes through the structure (80) based on verification of one or more authorisation certificates to acquire access to the structure (80); and

(c) said structure (80) includes administrating means (100) for issuing said one or more certificates to said one or more end-users (20, 30).

2. A system (10) according to Claim 1, wherein the administrating means (100) is operable to administer at least one of end-user sign-up and end-user payment for access to the communication structure (80).

3. A system (10) according to Claim 1 or 2, wherein the administrating means (100) is operable to generate one or more private-public key pairs, the administrating means (100) being operable to maintain said one or more private keys secret and to distribute said one or more corresponding public keys within the system (10) for certificate authentication purposes.

4. A system (10) according to Claim 3, wherein the administrating means (100) is operable to generate private-public key pairs using a Rivest-Shamir-Adelman (RSA) method.

5. A system (10) according to Claim 1, 2, 3 or 4, wherein the structure (80) includes a peer-to-peer communication network (110) through which the end-users (20, 30) are mutually connectable.

6. A system (10) according to Claim 5, wherein the peer-to-peer network (110) is implemented as a combination of interfacing nodes and storage nodes, said storage nodes being configured in one or more slots for database access purposes.

7. A system (10) according to any one of the previous claims, wherein the administrating means (100) is arranged to perform one or more of:

(a) providing an end-user (20, 30) accounts database;

(b) providing a synchronizing time reference for the communication structure (80);
(c) providing globally-configurable settings for the system (10);
(d) providing peer discovery during bootstrap of the structure (80);
(e) handling new end-user (20, 30) registration; and
(f) monitoring operation of the structure (80) for controlling desired modes of operation thereof.

8. A system (10) according to any one of the preceding claims, wherein a plurality of end-users are operable to mutually exchange their authorisation certificates prior to commencing communication therebetween where at least one of said certificates is identified to be authentic.

9. A system (10) according to any one of the preceding claims, wherein the structure (80) is arranged to support end-user free-trial use of the system (10), such free-trial use being subject to administration from the administrating means (10) by repeated issuing of authorisations.

10. A system (10) according to any one of the preceding claims, wherein the administrating means (100) is operable to invoice one or more end-users (20, 30) on a flat-fee rate substantially irrespective of use of the system (10) exercised by said one or more end-users (20, 30).

11. A system (10) according to any one of the preceding claims arranged to be configurable to operate concurrently with POTS and/or PSTN.

12. A system (10) according to any one of the preceding claims, wherein the administrating means (100) is implemented by way of one or more central computer servers.

13. A system (10) according to any one of the preceding claims, wherein the administrating means (100) is operable to apply an heuristics fraud detection analysis of end-user registration and system (10) usage data for detecting fraudulent access to the system (10) by end-users (20, 30).

14. A method of operating a telephone system (10) comprising a plurality of end-users (20, 30) and a communication structure (80) through which one or more end-users (20, 30) are couplable for communication purposes, characterised in that the method includes steps of:
(a) arranging for the communication structure (80) to be substantially de-centralized with regard to communication route switching therein for connecting said one or more end-users (20, 30);

(b) arranging for said one or more end-users (20, 30) to be operable to establish their own communication routes through the structure (80) based on exchange of one or more authorisation certificates to acquire access to the structure (80); and

(c) arranging for said structure (80) to include administrating means (100) for issuing said one or more certificates to said one or more end-users (20, 30).

15. A method according to Claim 1, wherein the administrating means (100) is operable to administer at least one of end-user sign-up and end-user payment for access to the communication structure (80).

16. A method according to Claim 14 or 15, wherein the administrating means (100) is operable to generate one or more private-public key pairs, the administrating means (100) being operable to maintain said one or more private keys secret and to distribute said one or more corresponding public keys within the system (10) for certificate authentication purposes.

17. A method according to Claim 16, wherein the administrating means (100) is operable to generate private-public key pairs using a Rivest-Shamir-Adelman (RSA) method.

18. A method according to Claim 14, 15, 16 or 17, wherein the structure (80) includes a peer-to-peer communication network (110) through which the end-users (20, 30) are mutually connectable.

19. A method according to Claim 18, wherein the peer-to-peer network (110) is implemented as a combination of interfacing nodes and storage nodes, said storage nodes being configured in one or more slots for database access purposes.

20. A method according to any one of Claims 14 to 19, wherein the administrating means (100) is arranged to perform one or more of:

(a) providing an end-user (20, 30) accounts database;

(b) providing a synchronizing time reference for the communication structure (80);

(c) providing globally-configurable settings for the system (10);

(d) providing peer discovery during bootstrap of the structure (80);

(e) handling new end-user (20, 30) registration; and

(f) monitoring operation of the structure (80) for controlling desired modes of operation thereof.

21. A method according to any one of Claims 14 to 20, wherein a plurality of end-users are operable to mutually exchange their authorisation certificates prior to

commencing communication therebetween where at least one of said certificates is identified to be authentic.

22. A method according to any one of Claims 14 to 21, wherein the structure (80) is arranged to support end-user free-trial use of the system (10), such free-trial use being subject to administration from the administrating means (10) by repeated issuing of authorisations.

23. A method according to any one of the Claims 14 to 22, wherein the administrating means (100) is operable to invoice one or more end-users (20, 30) on a flat-fee rate substantially irrespective of use of the system (10) exercised by said one or more end-users (20, 30).

24. A method according to any one of Claims 14 to 23 wherein the system (10) is arranged to be configurable to operate concurrently with POTS and/or PSTN.

25. A method according to any one of the preceding Claims 14 to 24, wherein the administrating means (100) is implemented by way of one or more central computer servers.

26. A method according to any one of Claims 14 to 25, wherein the administrating means (100) is operable to apply an heuristics fraud detection analysis of end-user registration and system (10) usage data for detecting fraudulent access to the system (10) by end-users (20, 30).

27. Software for implementing at least a part of the system (10) according to Claim 1.

28. Software executable on computing hardware for implementing one or more steps of the method according to Claim 14.

29. Software according to Claim 27 or 28 communicable to end-users (20, 30) via a communication network and/or stored on a data carrier.

1 Abstract

There is provided a peer-to-peer telephone system (10) comprising a plurality of end-users (20, 30) and a communication structure (80) through which one or more end-users (20, 30) are couplable for communication purposes. The system (10) is distinguished in that: (a) the communication structure (80) is substantially de-centralized with regard to communication route switching therein for connecting said one or more end-users (20, 30); (b) said one or more end-users (20, 30) are operable to establish their own communication routes through the structure (80) based on exchange of one or more authorisation certificates, namely User Identity Certificates (UIC), to acquire access to the structure (80); and (c) said structure (80) includes an administration arrangement (100) for issuing said one or more certificates to said one or more end-users (20, 30).

2 Representative Drawing

Fig. 1

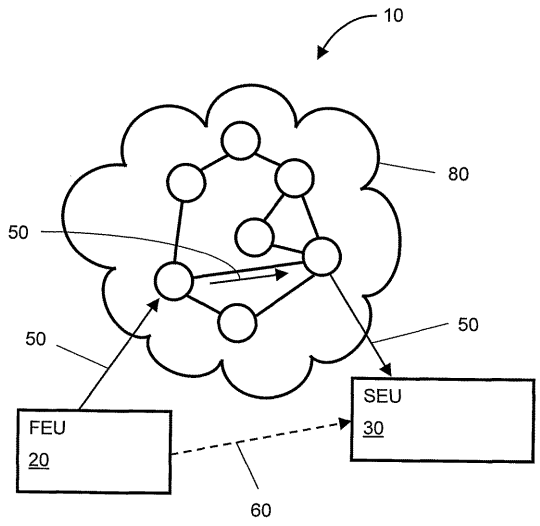


Fig. 1

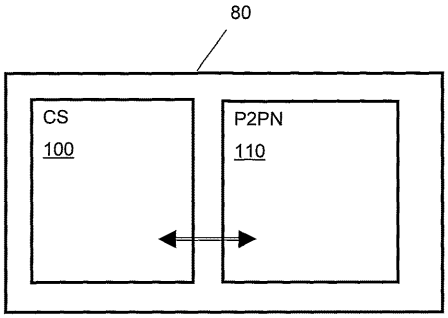


Fig. 2