

(19) 日本国特許庁(JP)

(12) 特許公報(B2)

(11) 特許番号

特許第4657878号
(P4657878)

(45) 発行日 平成23年3月23日(2011.3.23)

(24) 登録日 平成23年1月7日(2011.1.7)

(51) Int.Cl.

F 1

H04L 12/46 (2006.01)
H04L 12/56 (2006.01)H04L 12/46
H04L 12/56Z
Z

請求項の数 12 (全 12 頁)

(21) 出願番号 特願2005-296526 (P2005-296526)
 (22) 出願日 平成17年10月11日 (2005.10.11)
 (65) 公開番号 特開2006-115505 (P2006-115505A)
 (43) 公開日 平成18年4月27日 (2006.4.27)
 審査請求日 平成20年8月1日 (2008.8.1)
 (31) 優先権主張番号 04024017.8
 (32) 優先日 平成16年10月8日 (2004.10.8)
 (33) 優先権主張国 欧州特許庁 (EP)

(73) 特許権者 501263810
 トムソン ライセンシング
 Thomson Licensing
 フランス国, 92130 イッシー レ
 ムーリノー, ル ジヤンヌ ダルク,
 1-5
 1-5, rue Jeanne d' Arc, 92130 ISSY LES
 MOULINEAUX, France
 (74) 代理人 100077481
 弁理士 谷 義一
 (74) 代理人 100088915
 弁理士 阿部 和夫

最終頁に続く

(54) 【発明の名称】ピアグループ間で通信を確立する方法

(57) 【特許請求の範囲】

【請求項 1】

第1のピアグループと第2のピアグループとの間に通信を確立する方法において、前記第2のピアグループのメンバーである第2のピアにおいて第1のピアからのメッセージを受信するステップであって、前記第1のピアは、第1のピアグループのメンバーであるか、または、別個の接続を介して2次ピアと接続可能である1次ピアであって前記第1のピアグループのメンバーである1次ピアと接続可能な前記2次ピアであり、前記メッセージは前記第2のピアグループのメンバーに送信される、受信するステップと、

前記メッセージから、第1のピアのピア識別子と、第1のピアグループのピアグループ識別子と、第2のピアグループにおける第1のピアの一時的なグループメンバーシップのための申し込みと、第1のピアが第2のピアグループから第1のピアグループまでの接続の形成を要求していることの指示と、を検出するステップと、

第1のピアグループに対する接続が第2のピアグループに許可されるかを検出するステップと、

接続が許可される場合、第1のピアに対して第2のピアグループとのメンバーシップを許可するステップ

とを有することを特徴とする方法。

【請求項 2】

1次ピアおよび2次ピアは、同一のハードウェア上で動作するソフトウェアインスタンスであるか、またはスレッドである、請求項1記載の方法。

【請求項 3】

1 次ピアおよび 2 次ピアは、他のピアには既知でない秘密のプロトコルまたは暗号を使用する、請求項 1 または 2 記載の方法。

【請求項 4】

第 1 のピアに前記第 2 のピアグループとのメンバーシップが許可された後、該第 1 のピアは、

データまたはメッセージを送信し、および / または第 2 のピアグループから第 1 のピアグループへサービスを供給するステップ、および / または、

第 1 のピアグループからデータまたはメッセージを受信し、および / またはサービスを要求して、第 2 のピアグループへ供給するステップ

を有する、請求項 1 から 3 までのいずれか 1 項記載の方法。

10

【請求項 5】

第 2 のピアグループへ供給されるデータまたはメッセージおよび / またはサービスの要求は、少なくとも、別のピアグループとの接続を保持する第 2 のピアグループ内のすべてのピアに対してブロードキャストされる、請求項 4 記載の方法。

【請求項 6】

第 2 のピアグループ内のデータおよび / またはサービスは、少なくとも 1 つの第 1 のクラスと 1 つの第 2 のクラスとに分類され、

該第 1 のクラスのデータおよび / またはサービスを前記第 1 のピアグループに供給することは許可され、該第 2 のクラスのデータおよび / またはサービスを該第 1 のピアグループに供給することは許可されず、

20

第 1 のピアグループに対する接続が第 2 のピアグループに許可されるかを検出するステップには、第 2 のピアグループのどの特定のデータおよび / またはサービスが該第 1 のクラスに分類されているかまたは該第 2 のクラスに分類されているかを検出するステップが含まれる、請求項 1 から 5 までのいずれか 1 項記載の方法。

【請求項 7】

前記第 2 のピアグループのどの特定のデータおよび / またはサービスが該第 1 のクラスに分類されているかまたは該第 2 のクラスに分類されているかを検出するステップには、インターネットベースのサーバによって供給された中央のリストをチェックするステップまたはローカルのリストをチェックするステップが含まれている、請求項 6 記載の方法。

30

【請求項 8】

前記第 2 のピアグループのどの特定のデータおよび / またはサービスが該第 1 のクラスに分類されているかまたは該第 2 のクラスに分類されているかを検出するステップには、第 2 のピアグループが第 1 のピアグループに確認のためにコンタクトするステップが含まれている、請求項 6 記載の方法。

【請求項 9】

第 1 のピアに対して第 2 のピアグループとのメンバーシップを許可する接続を、所定の時間後または所定のイベントに応じて終了する、請求項 1 から 8 までのいずれか 1 項記載の方法。

【請求項 10】

40

第 2 のピアグループから第 1 のピアグループへ送信されるデータまたはメッセージがマークリングされ、

第 1 のピアグループのピアは前記マークリングを検出し、前記マークリングの検出に応じて、該データまたはメッセージのコピーまたは更なる分配を拒否する、請求項 1 から 9 までのいずれか 1 項記載の方法。

【請求項 11】

第 1 のピアは、1 次ピアに関連する 2 次ピアであり、
ピアおよびピアグループは個別の識別子を有し、

2 次ピアの識別子は第 1 のピアグループのピアグループ識別子と同じである、請求項 1 記載の方法。

50

【請求項 12】

第 1 のピアグループと第 2 のピアグループとの間で通信を確立するための装置において、

第 2 のピアグループのメンバーである第 2 のピアにおいて第 1 のピアからメッセージを受信するための手段であって、前記第 1 のピアは、第 1 のピアグループのメンバーであるか、または、別個の接続を介して 2 次ピアと接続可能である 1 次ピアであって前記第 1 のピアグループのメンバーである 1 次ピアと接続可能な前記 2 次ピアであり、前記メッセージは前記第 2 のピアグループのメンバーに送信される、手段と、

該メッセージから、第 1 のピアのピア識別子と、第 1 のピアグループのピアグループ識別子と、第 2 のピアグループにおける第 1 のピアの一時的なグループメンバーシップのためのアプリケーションと、第 1 のピアが第 2 のピアグループから第 1 のピアグループまでの接続の形成を要求していることの指示と、を検出するための手段と、

第 1 のピアグループに対する接続が第 2 のピアグループに許可されているかを検出するための手段と、

接続が許可されていることが検出された場合、第 1 のピアに対して第 2 のピアグループとのメンバーシップを許可するための手段とが設けられていることを特徴とする装置。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、異なるピアグループ間で通信を確立する方法に関する。

20

【背景技術】

【0002】

現在のピアツーピア (P2P) システムは、所有権が主張されている同様のソフトウェアおよびプロトコルを実行してピアのメッセージ通信および共働を行うために明確に定義されている。これらの適用例に、Kazaa または EDonkey がある。ピアが通常のコンピュータと異なる点は、サーバ クライアント構造である。ここでは、ピアはサーバを必要としない。

【0003】

WO 02/057917 に、JXTA の名称で知られている P2P ネットワーク計算プラットフォームが開示されている。これは、ピアツーピア計算用の全般的なフレームワークであり、同様のフレームワークを使用して異なるアプリケーションを指定するためのものである。たとえば、1 つのピアグループがファイル共有グループであるのに対し、別のピアグループでは IP 経由音声サービスが提供される。JXTA ではピアメンバーシッププロトコルが使用され、これによってピアをメンバーシップに割り当て、完全なグループ広告と一緒にメンバーシップクレデンシャル (信任状) を受け取る。ピア間のメッセージには 1 つまたは複数のクレデンシャルが含まれてあり、これは受信者に対して送信者を識別するために使用される。ピアは個別の識別子を有しており、この識別子はたとえば UUID とされる。クレデンシャルは、たとえばピア等の個人に限定されたデジタル文書であり、別の個人に提示される場合には、認証プロセスで確認される。P2P プラットフォーム構成要素を具現化するプロセスはインスタンシエーションと称され、この具現化は構成要素の実体と称される。

30

【0004】

欧州特許出願 EP 1427141 では、ピアグループのコンセプトを使用してオーナーゾーンコンセプトが具現化される。ここではピアグループは、ユーザの家における装置のホームネットワークである。このコンセプトによって、個別のホームネットワーク間で相互接続および通信を行うことができ、たとえば、相互に信頼するユーザの相互接続および通信を行うことができる。1 つのオーナーゾーンのユーザおよび別のオーナーゾーンのユーザは相互に、特定の信頼のレベルを定義し、オーナーゾーンは相互に「信頼ゾーン」と見なされ、多かれ少なかれコンテンツおよびサービスを自由に共用する。しかし、異なるピアグループ間で接続を形成する方法は詳細には知られておらず、とりわけ、信頼ゾーン間

40

50

で一時的な接続を形成する方法は詳細には知られていない。

【0005】

JXTAの基本的原則の1つに、ピアはメッセージを1つのピアグループ内で交換するが、ピアグループを超えて交換できないことがある。このことは、ピアグループに巨大な数のピアが含まれる可能性のあるインターネットベースのP2Pアプリケーションのための良好な解決手段である。たとえばJXTAは、数十万までのピアに拡大するよう設計されており、複数のピアグループが並行して設けられている。たとえばインターネットに接続されることがあるホームネットワークでは、この周辺環境は非常に不利である。

【特許文献1】WO 02/057917

10

【特許文献2】EP 1427141

【発明の開示】

【発明が解決しようとする課題】

【0006】

本発明の課題は、2つのピアグループ間で、とりわけ相互に「信頼ゾーン」ステータスを有する2つのオーナーゾーン間で通信を確立する方法および装置を提供することである。

【課題を解決するための手段】

【0007】

前記課題を解決する手段は、第1のピアグループのメンバーであるかまたは1次ピアと接続可能な2次ピアである第1のピアによって、第2のピアグループのメンバーへメッセージを送信するステップと、第2のピアグループのメンバーである第2のピアによって該メッセージを受信し、該メッセージから第1のピアのピア識別子と第1のピアグループのピアグループ識別子とを検出し、第1のピアが第2のピアグループにおける一時的なグループメンバーシップを申し込むことと、第1のピアが第2のピアグループから第1のピアグループまでの接続を形成しようとしていることの指示とを検出するステップと、第2のピアグループにおいて第1のピアグループとの接続が許可されているか否かを検出するステップと、このような接続が許可されている場合、第1のピアに対して第2のピアグループとのメンバーシップを許可し、第1のピアが許可された後、データまたはメッセージを送信し、および/または第2のピアグループから第1のピアグループへサービスを供給できるようにするステップとを有し、該1次ピアは、第1のピアグループのメンバーであり、別個の接続を介して該2次ピアに関連付けられていることを特徴とする方法である。

20

【発明を実施するための最良の形態】

【0008】

本発明では、以下のように構成されている。すなわち、第1のピアグループのメンバーであるかまたは第1のピアグループのメンバーである別のピアに対して緊密な関係を有する第1のピアが第2のピアグループにコンタクトして該第2のピアグループ内の一時的なメンバーシップを申し込むように構成されている。この緊密な関係は、たとえば別個の1対1の接続である。後者の場合、2つのピアはたとえば、相互に別個のチャネルを介して通信することができるように共通のハードウェア上の別個のソフトウェア実体とするか、または、他のピアには既知でない特別なプロトコルまたは暗号を使用して対を形成する2つの別個のピアとすることができます。第2のピアグループの制御機能またはサービス機能は、次のことを検出する。すなわち、第1のピアが第2のピアグループ内の一時的なメンバーシップのみを申し込んでいることと、第1のピア自体または第1のピアと緊密な関係を有する別のピアが第1のピアグループのメンバーであることと、ブリッジヘッドまたは代表者として第1のピアグループとの接続を形成するためのものであることを検出する。この情報は、第1のピアが送信する広告メッセージに含まれる。さらに第2のピアグループは、コンタクトが許可されているピアグループのリストを保持し、オプションとして、どの程度のコンタクトが許可されているかも検出する。第2のピアグループは、第1のピアグループがこのリストに含まれているか否かをチェックし、その場合(すなわち、リス

30

40

50

トに含まれている場合)には、第1のピアに対してグループメンバーシップを許可する。このようにして第1のピアは、第2のピアグループから第1のピアグループへデータを送信するか、またはサービスを供給することを許可される。

【0009】

第2のピアグループにあるデータおよびサービスは、分類することができ、どの特定のデータおよびサービスを第1のピアグループへ供給できるかということは、上記のコンタクトの許可されている程度に依存する。第1のピアグループがピアグループのリストに含まれていない場合には、第1のピアを拒否し、および/または第2のピアグループのユーザまたは管理者に、第1のピアグループをリストに付加するか否かを決定することができる。それに相応してピアグループは、コンタクトが許可されていないピアグループが含まれている否定リストを保持することができる。

10

【0010】

本発明では、信頼ゾーン通信を実施するために2つの異なる実施形態が提案される。
1つはJXTA対JXTAブリッジを使用する信頼ゾーン通信である。
もう1つは代表ノードを使用する信頼ゾーン通信である。

【0011】

本発明の有利な実施形態は、従属請求項、以下の説明および図面に開示されている。

【実施例】

【0012】

本発明の実施例を、添付図面と関連して説明する。

20

【0013】

ここでは、信頼ゾーン通信を行うための本発明の2つの主要な実施形態が開示されている。それは、ブリッジング構想および代表者構想である。

【0014】

<1. JXTA対JXTAブリッジを使用する信頼ゾーン通信>

設定することができるブリッジングサービスには、2つの異なる種類がある。第1の種類は、2つのオーナゾーン間の1対1の接続である。これによってたとえば、ある人が友人のホームネットワークに接続してその友人とコンテンツを交換することができる。第2の種類は、オーナゾーン用のコラボレーション(協働)プラットフォームとして機能するピアグループとの接続である。この解決手段では、「信頼ゾーン」通信のためだけに特化された専用のピアグループを使用する。

30

【0015】

図1には、1対1のブリッジ構成の一例が示されている。ブリッジングピアB Rが所属のオーナゾーンO Z 1に参加するために、1次アドレスGを使用する。すなわち、ブリッジングピアは第1のオーナゾーンに所属する。オーナゾーンO Z 1のメンバーとして、このピアはブリッジングサービスを該オーナゾーン内の他のピアに対して公開する。したがって、該オーナゾーン内のピアのうちどれでも、信頼ゾーン接続を要求することができる。さらにこのような信頼ゾーン接続は、アプリケーションによって事前構築することもできる。ブリッジングピアが信頼ゾーン接続を実行するように命令されると、2次ピアエンティティが「エクスポート」される。すなわち、「ネットピアグループ」においてインスタンス化される。この「ネットピアグループ」は、アプリケーションのデフォルトのベースピアグループである。2次ピアは、ネットピアグループおよび存在する他のピアグループに関する必要なピアグループ情報を取得し、ターゲットの信頼ゾーンにコンタクトする。第1のピアエンティティGおよび2次ピアエンティティHは、任意のプロトコルを使用する別個の1対1の接続によって接続される。

40

【0016】

本発明のこの実施形態による装置では、異なる(論理)アドレスすなわちU U I Dを有し1対1接続によって相互に接続された2つのピアエンティティをインスタンス化することによるブリッジングサービスを提供する。1次アドレスを使用して、ピアはピアグループに参加し、該ピアグループ内部でブリッジングサービスを公開する。このピアグループ

50

はオーナゾーンとすることができる。図1では、2つのオーナゾーンOZ1, OZ2がブリッジング装置BRによって接続されており、このブリッジング装置BRには、相互接続INによって接続された2つのピアエンティティG, Hが含まれている。第1のオーナゾーンOZ1はピアA, B, C, Gを有しており、第2のオーナゾーンOZ2は初期では、ピアD, E, Fを有している。ブリッジング装置BRのピアエンティティのうち1つは第1のアドレスを有する1次ピアエンティティGであり、他は第2のアドレスを有する2次ピアエンティティHである。ブリッジング装置BRが多重スレッドソフトウェアを実行できる場合、シームレスに2つのピアグループ内で、これらの異なるピアエンティティG, Hおよびこれらのピアエンティティの相互接続INを使用して並列的に動作させることができる。それに対して逐一的に、2つのピアエンティティG, Hのうちその都度一方のみをアクティブにして、該ピアエンティティG, H間で交換すべきデータをたとえば、ブリッジング装置BR内の専用の共用メモリに一時記憶することができる。

【0017】

本発明によれば、2次ピアエンティティHが他のオーナゾーンOZ2をインスタンス化し、ブリッジピアとしてメンバーシップを要求する。すなわち第2のオーナゾーンOZ2は、2次ピアエンティティHがブリッジング装置の2次ピアエンティティであることを検出することができる。ピアエンティティHは自身に固有のピアクレデンシャルをオーナゾーンOZ1のクレデンシャルとともに供給し、ピアエンティティHは「ホーム」ピアグループと見なされるか、または、リンクを確立しようとする対象であるピアグループと見なされることができる。この時点で、他方のオーナゾーンOZ2のメンバーシップサービスにより、入ろうとしているピアエンティティHが信頼ゾーンから来ているか否かがチェックされる。そうである場合、メンバーシップサービスは要求を受け入れ、2次ピアHに対してメンバーシップを許可する。この2次ピアHは、たとえばある種の「ゲスト」ステータスを得る。

【0018】

次のリストには、信頼ゾーンの信頼性チェックを実行する幾つかの手段が挙げられている。

1. インターネットベースのサーバが、オーナゾーン間の関係を文書化した中央の信頼ゾーンリストを作成し、オーナゾーンが信頼ゾーン接続の権限を許可する前にこのリストをチェックする。このようなリストはたとえば、特定のトピックに関するものであり、管理者によってメンテナンスされる。

2. オーナゾーンが固有の信頼ゾーンリストを保持し、独立してオーナゾーンの信頼性をチェックする。このリストも通常は管理者によってメンテナンスされるか、またはユーザによってメンテナンスされる。

3. オーナゾーンが相互にコンタクトし、ゾーンの信頼性をチェックする。

【0019】

メンバーシップが許可されると、2次ブリッジングピアエンティティHはいわゆるブリッジアイデンティティをもってオーナゾーンOZ2に参加し、オーナゾーンOZ2内でそのサービスを公開する。また、2次ピアエンティティHは1次ピアエンティティGに対して、信頼ゾーン接続の確立が完了したことの指示も行う。この時点から、2つのピアエンティティG, Hは相互に通信してメッセージを交換し、2つのオーナゾーンOZ1, OZ2間でブリッジングサービスを介してデータを交換することができるようになる。完全な端末対端末のアドレス指定および認証を行うのに必要な標準的なJXTAメッセージへの拡張が可能である。送信側ピアを識別するための送信者情報は、送信側オーナゾーンの信頼性によって補足されなければならず、受信側ピアを識別するための受信者情報は、信頼ゾーンアドレスによって補足される必要がある。信頼ゾーンアドレスは、受信者が所属するオーナゾーンを識別するのに必要とされる。クレデンシャルによって送信側オーナゾーンが識別される。というのも、送信側ピアは受信者オーナゾーン内では未知である場合があり、メッセージを転送するブリッジピアHのみが受信者オーナゾーンOZ2で既知だからである。

10

20

30

40

50

【0020】

ブリッジングサービスの第2の種類は、上記で挙げたように、コラボレーションプラットフォームである。図2には、複数のオーナーゾーンOZ_A, ..., OZ_Dが示されている。これらは、コラボレーションピアグループCPGに対して信頼ゾーンとして定義されているので、該コラボレーションピアグループと通信することができる。異なるオーナーゾーンのブリッジピアが、コミュニティメッセージを交換するために設けられたコラボレーションピアグループCPGに参加することができる。このコミュニティメッセージはたとえば、信頼ゾーン情報、電子プログラムガイド(EPG)、またはソフトウェア更新等のコミュニティニュース等である。上記のメカニズムを受けて、複数のブリッジピアはそれら自身の2次ピアエンティティを使用し、このような専用のピアグループにある別のブリッジピアと共に働く。コラボレーションピアグループの構成は大抵、ブロードキャスト形式のメッセージのために設計される。とりわけ、コラボレーションピアグループCPGはランデブーピアを含む。ランデブーピアという用語は、別のピア、ピアグループ、サービスおよびパイプに関する情報を見つけるための待ち合わせ場所として機能するピアを指す。ランデブーピアは、別のピアに対して有用な情報をキャッシュする。たとえば、接続されたオーナーゾーンが独立してアドレス指定可能である場合、最も有利なのはコラボレーショングループのランデブーピアが、ブリッジピアとオーナーゾーンとの間の関連を示すマッピングテーブルを構成することである。

【0021】

上記の方法の変形形態では、ブリッジングピアはオーナーゾーンの汎用固有識別子(UUID)を2次ピアアドレスとして使用する。このようにすると、マッピングテーブルは必要なくなる。2次ピアアドレスはオーナーアドレスと同一とすることができる。というのも、JXTA等のシステムでは2次ピアアドレスとオーナーアドレスが混同する可能性がないからである。このようなシステムでは、異なる広告メッセージ形式を使用することにより、ピア情報とピアグループ情報を区別する。たとえば図1では、ブリッジング装置BRの2次ピアHは、その1次ピアGのホームオーナーゾーンの識別子UUID_Nと同一であるピア識別子を有する。ピアグループ識別子UUID_Nは、2次ピアHのピア識別子の中に明示的または暗示的に含まれ、第2のオーナーゾーンがこの2次ピア識別子を使用して、1次ピアGが所属するピアグループIDを決定することもできる。

【0022】

<2. 代表ノードを使用して行われる信頼ゾーン通信>

信頼ゾーン通信を実施するための本発明の第2の実施形態は、上記で挙げたように、代表ノードである。これは或るピアが、信頼ゾーン通信を許可する代表者サービスを提供することを意味する。上記のブリッジサービスと異なり、必要なのは、1つのピアエンティティと1つのアドレスだけである。これは、該ピアが特定の時点でただ1つのピアグループのアクティブなメンバーであり、異なるピアグループ間をジャンプできることを意味する。

【0023】

図3~5には、2つのピアグループOZ1, OZ2間の代表形式の通信の手法が示されている。これらのピアグループはこの例では、ネットピアグループと称されるデフォルトの親ピアグループNPGを有する。すなわち、ピアグループOZ1, OZ2のすべてのピアNode_ID1, ..., Node_ID5がデフォルトによって共通の親ピアグループNPGと他のピアグループとの相違点は、ピアは、デフォルトピアグループの内部では自由に通信することができず、それぞれ定義されたホームピアグループOZ1, OZ2の内部でのみ自由に通信できることである。デフォルトピアグループの内部であり、かつ、ホームピアグループ外部での通信およびデータ交換は、いくつかのベーシック形式のメッセージに制限されている。しかし本発明のこの実施形態では、代表ノードをこの目的で使用することができる。代表ノードはたとえば、ユーザまたは管理者によって指名されるか、または該代表ノードの特徴、たとえば特別なハードウェア接続またはハードウェアインターフェー

10

20

30

40

50

スにしたがって自動的に決定される。

【0024】

この実施例では、第1のオーナーゾーンOZ1が第2のオーナーゾーンOZ2に接続しようとしている。したがって、第1のオーナーゾーンOZ1の代表ピアNode_ID3が所属のホームピアグループの接続サービスからタスクを得て、該ピアグループOZ2との信頼ゾーン接続を確立する。この接続サービスは、他のピアグループOZ2のグループ識別子および/または該他のグループの代表ピアNode_ID2のノード識別子を提供する。次に、代表ピアNode_ID3は図3に示されているようにそのホームピアグループOZ1を出発し、該代表ピアNode_ID3がすでに有している他のピアグループOZ2に関する情報に依存して他のグループの代表ピアNode_ID2を親ピアグループNPGに直接コントタクトさせるか、または切り替える。通常は、他のピアグループOZ2からの広告を見つける試行が行われる。

【0025】

代表ピアNode_ID3は別のピアグループOZ2を、たとえば広告メッセージの受信によって見つけた場合、ピアグループOZ2をインスタンス化して、代表ピアNode_ID3のホームピアグループOZ1の代表ノードとしてのメンバーシップを要求する。この時点で、新たなピアグループOZ1のメンバーシップサービスはクレデンシャルチェックを実行し、たとえば、代表ピアNode_ID3が信頼ゾーンから来ているか否かをチェックする。すなわち、信頼ゾーンが該オーナーゾーンに入ろうとしているか否かをチェックする。

【0026】

以下のリストに、信頼ゾーンの信頼性チェックを実行する3つの手段が挙げられている。

1. インターネット内のサーバは、中央の信頼ゾーンリストを作成し、ピアグループはこのリストをチェックしてから、信頼ゾーン接続を許可する。このようなリストは、たとえば固有のトピックに関連するもの、たとえば特定のサッカー用語等であり、管理者によってメンテナンスされる。

【0027】

2. 各ピアグループが、固有の信頼ゾーンリストを保持する。

【0028】

3. 代表者を受け入れる前に、ピアグループは相互にコントタクトし、接続要求を確認する。

【0029】

ピアグループのクレデンシャルはこの場合、信頼ゾーンチェックにおいてピアのクレデンシャルよりも重要である。第2のピアグループOZ2のメンバーシップサービスが代表ピアNode_ID3をメンバーとして受け入れる前に、ピアのクレデンシャルだけでなく、第1のピアグループOZ1のクレデンシャルも確認する必要がある。この第1のピアグループOZ1のクレデンシャルは、該代表ピアが付随して持っているものか、または要求に応じて第1のピアグループOZ1から直接受信されたものである。両方のクレデンシャルが、たとえば上記の信頼性チェックのうち1つにしたがって確認されると、メンバーシップサービスは自身のグループに対する代表ノードのアクセス権を許可する。次に、代表ピアNode_ID3は、代表者ステータスおよび代表者のアイデンティティをもってグループに参加する。しかしピアグループは、このゾーン内部での代表ピアの権利を自由に制限することができる。たとえば、代表ピアは定義されたコンテンツにのみアクセスすることを許可される。信頼ゾーンが異なると、定義されるコンテンツも異なることがある。

【0030】

代表者Node_ID3はたとえば、図4に示されるように、他のグループの代表者Node_ID2のみとの通信に制限される。他のグループの代表者Node_ID2は自身の所属するピアグループOZ2内部でアクセス権を制限されている場合がある。これは

ピアグループのユーザが、どのデータに対して、たとえばどのマルチメディアコンテンツに対して他のピアがアクセスできるようにするかフィルタリングする安全な手段である。

【0031】

ノード識別子およびグループ識別子は、いかなる時にもピアグループ内でチェックできる。というのも、ピアが送信するすべてのメッセージにはクレデンシャルが添付されているからである。クレデンシャルは少なくとも、ピアの識別子およびピアグループの識別子を有する。これによって、送信者、該送信者の役割および該ピアグループにおける権利を識別できる。

【0032】

代表者Node_ID3が、第2の代表者Node_ID2のピア識別子も含む第2のピアグループOZ2の広告メッセージを見つけると、代表者Node_ID3は、これら2つの代表者間に信頼ゾーン接続すなわちパイプ接続を要求する。発見された代表者Node_ID2はこのパイプに接続して、他の代表者Node_ID3に対して受入を指示し、この他の代表者Node_ID3は接続が確立されたことを認識する。接続プロセスの次のステップでは、図5に示されたように、代表者Node_ID3は自身のホームピアグループOZ1に戻るが、他の代表者Node_ID2とのパイプ接続を維持している。自身のホームピアグループOZ1に戻った代表者Node_ID3が、信頼ゾーン接続パイプが確立されたことを公表し、この時点からピアグループOZ1, OZ2間で、代表者サービスを介してメッセージを交換できる。メッセージは、代表者サービスで具現化される特別なインターフェースを使用して別のピアグループへ送信されることができる。ここで、受信側のピアグループの識別子およびメッセージが代表ピアによって処理され、パイプにしたがって送信される。すなわち代表者が、各パイプが2つのピアのみの間の接続部となっている複数のパイプに接続することができる。しかしデータの安全性のために、メッセージを送信側ピアのピアグループのクレデンシャルおよび受信側のピアグループのアドレスによって補足することが必要である。

【0033】

本発明の1つの実施形態ではピアグループ間で、JXTAでは「セキュアパイプ」とも称される安全な接続が使用される。

【0034】

1つの実施形態では、信頼ゾーンによるパイプ接続を確立する代わりに、代表者Node_ID3がメッセージを信頼ゾーンOZ2に直接投函する。代表者Node_ID3は応答メッセージを一種の「ポストマン」として回収し、ホームピアグループOZ1に戻る。

【0035】

本発明の1つの実施形態では、確立されたパイプ接続は所定の期間の間アクティブ状態に維持され、または特定のイベントが発生するまで、たとえば単一または固有のファイルまたはメッセージが転送されるまで、アクティブ状態に維持される。その後、自動的に終了される。後に別のデータ転送が必要になった場合には、再作動する必要がある。このようにして、ピアグループ間のネットワークおよび関係の簡潔な構造が維持される。

【0036】

有利には本発明では、たとえばデータ交換またはメッセージ交換を行うために、非常に制限されたアクセスのみを提供するピアグループ間で接続を具現化するための安全な手段が提供される。さらに、ユーザまたは管理者は、自身のピアグループに対して、どのピアグループと共働させるべきかを簡単に定義することができ、また特定の共働レベルまたは機密レベルを定義して、たとえばどのデータを特定のピアグループがアクセスできるかを簡単に定義することができる。代表ピアはこれらのデータをエクスポートする前に、これらのデータに対して「借用されるもの」または「インポートされるもの」とマーキングすることができる。これによって、他のピアグループによるコピーまたは更なる分配が防止できる。この目的のために、たとえばメタデータ、デジタル署名またはデータの電子的透かしが使用される。メタデータを使用してデータの拡大を制御する手段は、たとえば欧州

10

20

30

40

50

特許出願EP1369804に開示されている。受信側ピアグループのピアはこのマーキングを検出し、該マーキングの検出に応じて、たとえばメッセージ等であるデータのコピーまたは更なる分配を拒否する。

【0037】

本発明は全般的にピアグループにおいて使用することができ、とりわけ、JXTAプロトコルを使用するピアグループにおいて使用され、さらに特定すると、欧州特許出願EP1427141に開示されたような「オーナーゾーン」形式のピアグループにおいて使用される。

【図面の簡単な説明】

【0038】

10

【図1】2つのオーナーゾーン間のブリッジングを示す図である。

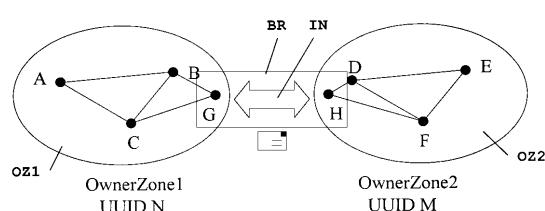
【図2】複数のオーナーゾーン間のブリッジングを示す図である。

【図3】2つのピアグループ間で代表ピアを使用して行われるパイプ通信の生成を示す図である。

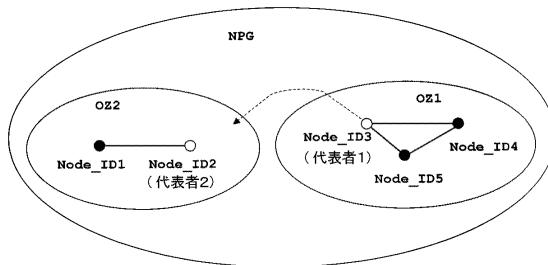
【図4】2つのピアグループ間で代表ピアを使用して行われるパイプ通信の生成を示す図である。

【図5】2つのピアグループ間で代表ピアを使用して行われるパイプ通信の生成を示す図である。

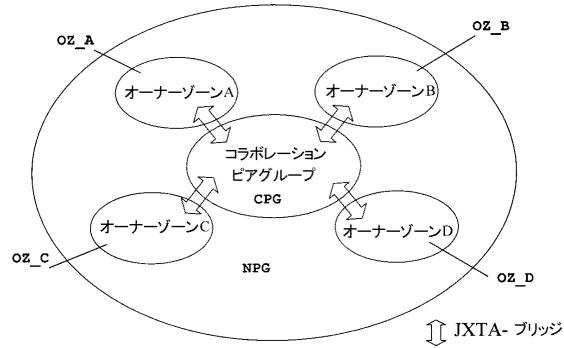
【図1】



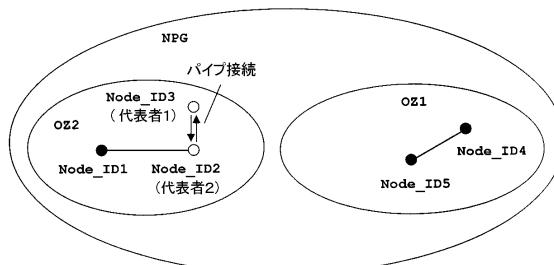
【図3】



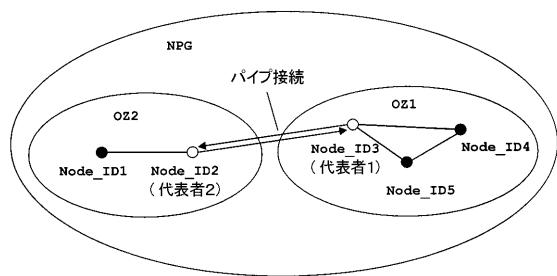
【図2】



【図4】



【図5】



フロントページの続き

(72)発明者 シュテファン クブシュ
　　ドイツ連邦共和国 ホーンホルスト イム オーア 2
(72)発明者 マイノルフ ブラヴァート
　　ドイツ連邦共和国 ハノーファー ズーテルシュトラーセ 54 ツェー
(72)発明者 ヴォルフガング クラウスベルガー
　　ドイツ連邦共和国 ハノーファー アム ウアトウルム 26
(72)発明者 フィ リー
　　ドイツ連邦共和国 ハノーファー ハルテンホフシュトラーセ 221
(72)発明者 ディートマー ヘッパー
　　ドイツ連邦共和国 ハノーファー ヴェルニゲローダー ヴェーク 41

審査官 中木 努

(56)参考文献 欧州特許出願公開第1427140 (EP, A1)

(58)調査した分野(Int.Cl., DB名)

H 04 L 12 / 28 - 46
H 04 L 12 / 56