(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5318947号
(P5318947)
(45)発行日　平成25年10月16日(2013.10.16)　(24)登録日　平成25年7月19日(2013.7.19)

(51)Int.Cl.　　F I
H04L 9/32 (2006.01)　　H04L 9/00 675A
G09C 1/00 (2006.01)　　G09C 1/00 640E

請求項の数 56　(全 25 頁)

(21)出願番号　特願2011-514869(P2011-514869)
(86)(22)出願日　平成21年6月19日(2009.6.19)
(65)公表番号　特表2011-525339(P2011-525339A)
(43)公表日　平成23年9月15日(2011.9.15)
(86)国際出願番号　PCT/US2009/048046
(87)国際公開番号　WO2009/155568
(87)国際公開日　平成21年12月23日(2009.12.23)
審査請求日　平成23年2月21日(2011.2.21)
(31)優先権主張番号　61/073,903
(32)優先日　平成20年6月19日(2008.6.19)
(33)優先権主張国　米国(US)
(31)優先権主張番号　12/486,415
(32)優先日　平成21年6月17日(2009.6.17)
(33)優先権主張国　米国(US)

(73)特許権者　595020643
クゥアルコム・インコーポレイテッド
ＱＵＡＬＣＯＭＭ　ＩＮＣＯＲＰＯＲＡＴＥＤ
アメリカ合衆国、カリフォルニア州　９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ　５７７５
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100109830
弁理士　福原　淑弘

最終頁に続く

(54)【発明の名称】ピアトゥピアオーバレイネットワーク内で選択位置攻撃の有効性を低減する方法および装置

(57)【特許請求の範囲】
【請求項１】
ピアトゥピアオーバレイネットワーク内で選択位置攻撃から保護するためにノードを動作させる方法であって、
新しいノード識別子がオーバレイネットワーク内の複数のノードのために生成されるべきであることを判定することと、
選択されたパラメータをハッシュ関数に入力して選択されたノード識別子を生成することと、
選択されたノード識別子の生成前に前記ノードに隣接するノードの第２の組とのリンクを保ちながら、前記選択されたノード識別子の生成の後に前記ノードに隣接するノードの第１の組とリンクを確立することにより、前記選択されたノード識別子に関連付けられたピアトゥピアオーバレイネットワーク内の位置を採用することと、前記ノードの第１の組は、前記ノードの第２の組とは異なり、
を備える方法。
【請求項２】
前記選択されたパラメータを備えるデータベースを保持することをさらに備える、請求項１に記載の方法。
【請求項３】
少なくとも１つのソルト値を受信することと、
前記選択されたパラメータの部分として少なくとも１つのソルト値を前記ハッシュ関数

に入力して前記選択されたノード識別子を生成することと
をさらに備える、請求項１に記載の方法。
【請求項４】
前記判定することが、時間標識に基づいて前記新しいノード識別子が生成されるべきであることを判定することを備える、請求項１に記載の方法。
【請求項５】
前記選択されたパラメータが、時間標識、電子メールアドレス、ＩＰアドレス、現在のノード識別子、およびソルト値のうちの少なくとも１つを備える、請求項１に記載の方法。
【請求項６】
ピアトゥピアオーバレイネットワーク内で選択位置攻撃から保護するために動作可能なノードであって、
オーバレイネットワーク内の複数のノードのために新しいノード識別子が生成されるべきであることを判定するための手段と、
選択されたパラメータをハッシュ関数に入力して選択されたノード識別子を生成するための手段と、
選択されたノード識別子の生成前に前記ノードに隣接するノードの第２の組とのリンクを保ちながら、前記選択されたノード識別子の生成の後に前記ノードに隣接するノードの第１の組とリンクを確立することにより、前記選択されたノード識別子に関連付けられたピアトゥピアオーバレイネットワーク内の位置を採用するための手段と、前記ノードの第１の組は、前記ノードの第２の組とは異なり、
を備えるノード。
【請求項７】
前記選択されたパラメータを備えるデータベースを保持するための手段をさらに備える、請求項６に記載のノード。
【請求項８】
少なくとも１つのソルト値を受信するための手段と、
前記選択されたパラメータの部分として前記少なくとも１つのソルト値をハッシュ関数に入力して前記選択されたノード識別子を生成するための手段と
をさらに備える、請求項６に記載のノード。
【請求項９】
前記判定するための手段が、時間標識に基づいて前記新しいノード識別子が生成されるべきであることを判定するための手段を備える、請求項６に記載のノード。
【請求項１０】
前記選択されたパラメータが、時間標識、電子メールアドレス、ＩＰアドレス、現在のノード識別子、およびソルト値のうちの少なくとも１つを備える、請求項６に記載のノード。
【請求項１１】
ピアトゥピアオーバレイネットワーク内で選択位置攻撃から保護するために動作可能なノードであって、
前記オーバレイネットワーク内の複数のノードのために新しいノード識別子が生成されるべきであることを判定するように構成されたタイミングモジュールと、
選択されたパラメータをハッシュ関数に入力して選択されたノード識別子を生成し、選択されたノード識別子の生成前に前記ノードに隣接するノードの第２の組とのリンクを保ちながら、前記選択されたノード識別子の生成の後に前記ノードに隣接するノードの第１の組とリンクを確立することにより、その選択されたノード識別子に関連付けられたピアトゥピアオーバレイネットワーク内の位置を採用するように構成され、前記ノードの第１の組は、前記ノードの第２の組とは異なる、プロセッサモジュールと
を備えるノード。
【請求項１２】

前記選択されたパラメータを備えるデータベースを保持するように構成されたメモリをさらに備える、請求項１１に記載のノード。

【請求項１３】

少なくとも１つのソルト値を受信することと、

前記選択されたパラメータの部分として少なくとも１つのソルト値をハッシュ関数に入力して前記選択されたノード識別子を生成することと

を行うように前記プロセッサモジュールがさらに構成された、請求項１１に記載のノード。

【請求項１４】

前記タイミングモジュールが時間標識に基づいて新しいノード識別子が生成されるべきであることを判定するように構成された、請求項１１に記載のノード。

【請求項１５】

前記選択されたパラメータが、時間標識、電子メールアドレス、ＩＰアドレス、現在のノード識別子、およびソルト値のうちの少なくとも１つを備える、請求項１１に記載のノード。

【請求項１６】

ピアトゥピアオーバレイネットワーク内で選択位置攻撃から保護するために動作可能なコンピュータプログラムを有するコンピュータ可読媒体であって、

前記コンピュータプログラムは、

オーバレイネットワーク内の複数のノードのために新しいノード識別子が生成されるべきであることを判定することと、

選択されたパラメータをハッシュ関数に入力して選択されたノード識別子を生成することと、

選択されたノード識別子の生成前に前記ノードに隣接するノードの第２の組とのリンクを保ちながら、前記選択されたノード識別子の生成の後に前記ノードに隣接するノードの第１の組とリンクを確立することにより、前記選択されたノード識別子に関連付けられたピアトゥピアオーバレイネットワーク内の位置を採用することとのために動作可能なコードを含み、前記ノードの第１の組は、前記ノードの第２の組とは異なる、コンピュータプログラム可読媒体。

【請求項１７】

前記コードがさらに前記選択されたパラメータを備えるデータベースを保持するように構成された、請求項１６に記載のコンピュータ可読媒体。

【請求項１８】

少なくとも１つのソルト値を受信することと、

前記選択されたパラメータの部分として前記少なくとも１つのソルト値をハッシュ関数に入力して前記選択されたノード識別子を生成することと

を行うように前記コードがさらに構成された、請求項１６に記載のコンピュータ可読媒体。

【請求項１９】

前記コードがさらに時間標識に基づいて前記新しいノード識別子が生成されるべきであることを判定するように構成された、請求項１６に記載のコンピュータ可読媒体。

【請求項２０】

前記選択されたパラメータが、時間標識、電子メールアドレス、ＩＰアドレス、現在のノード識別子、およびソルト値のうちの少なくとも１つを備える、請求項１６に記載のコンピュータ可読媒体。

【請求項２１】

ピアトゥピアオーバレイネットワーク内で選択位置攻撃から保護するためにノードによって使用可能な方法であって、

選択されたノードに関連付けられた新しいノード識別子を受信することと、

前記選択されたノードに関連付けられた選択されたパラメータをハッシュ関数に入力し

て対応するノード識別子を生成することと、前記対応するノード識別子は、選択されたノード識別子の生成前に前記ノードに隣接するノードの第２の組とのリンクを保ちながら、前記選択されたノード識別子の生成の後に前記ノードに隣接するノードの第１の組とリンクを確立することにより、ピアトゥピアオーバレイネットワーク内の位置を採用するために使用され、前記ノードの第１の組は、前記ノードの第２の組とは異なり、
前記新しいノード識別子を前記対応するノード識別子と比較することと、
前記新しいノード識別子が前記対応するノード識別子と一致しない場合に、その選択されたノードが潜在的攻撃者であると判定することと
を備える方法。
【請求項２２】
前記選択されたパラメータを備えるデータベースを保持することをさらに備える、請求項２１に記載の方法。
【請求項２３】
前記選択されたパラメータが、すべてその選択されたノードに関連付けられている、時間標識、電子メールアドレス、ＩＰアドレス、ノード識別子、およびソルト値のうちの少なくとも１つを備える、請求項２１に記載の方法。
【請求項２４】
前記新しいノード識別子が対応するノード識別子と一致しない場合にオーバレイネットワークからその選択されたノードを除外することをさらに備える、請求項２１に記載の方法。
【請求項２５】
ピアトゥピアオーバレイネットワーク内で選択位置攻撃から保護するように構成されたノードであって、
選択されたノードに関連付けられた新しいノード識別子を受信するための手段と、
前記選択されたノードに関連付けられた選択されたパラメータをハッシュ関数に入力して対応するノード識別子を生成するための手段と、前記対応するノード識別子は、選択されたノード識別子の生成前に前記ノードに隣接するノードの第２の組とのリンクを保ちながら、前記選択されたノード識別子の生成の後に前記ノードに隣接するノードの第１の組とリンクを確立することにより、ピアトゥピアオーバレイネットワーク内の位置を採用するために使用され、前記ノードの第１の組は、前記ノードの第２の組とは異なり、
前記新しいノード識別子を前記対応するノード識別子と比較するための手段と、
前記新しいノード識別子が前記対応するノード識別子と一致しない場合にその選択されたノードが潜在的攻撃者であると判定するための手段と
を備えるノード。
【請求項２６】
前記選択されたパラメータを備えるデータベースを保持するための手段をさらに備える、請求項２５に記載のノード。
【請求項２７】
前記選択されたパラメータが、すべてその選択されたノードに関連付けられている、時間標識、電子メールアドレス、ＩＰアドレス、ノード識別子、およびソルト値のうちの少なくとも１つを備える、請求項２５に記載のノード。
【請求項２８】
前記新しいノード識別子が前記対応するノード識別子と一致しない場合にその選択されたノードをオーバレイネットワークから除外するための手段をさらに備える、請求項２５に記載のノード。
【請求項２９】
ピアトゥピアオーバレイネットワーク内で選択位置攻撃から保護するために動作可能なノードであって、
選択されたノードに関連付けられた新しいノード識別子を受信するように構成されたトランシーバと、

前記選択されたノードに関連付けられた選択されたパラメータをハッシュ関数に入力して対応するノード識別子を生成すること、前記対応するノード識別子は、選択されたノード識別子の生成前に前記ノードに隣接するノードの第２の組とのリンクを保ちながら、前記選択されたノード識別子の生成の後に前記ノードに隣接するノードの第１の組とリンクを確立することにより、ピアトゥピアオーバレイネットワーク内の位置を採用するために使用され、前記ノードの第１の組は、前記ノードの第２の組とは異なり、

前記新しいノード識別子を前記対応するノード識別子と比較すること、および

前記新しいノード識別子が前記対応するノード識別子と一致しない場合にその選択されたノードが潜在的攻撃者であると判定すること

を行うように構成されたプロセッサと

を備えるノード。

【請求項３０】

前記プロセッサがさらに前記選択されたパラメータを備えるデータベースを保持するように構成された、請求項２９に記載のノード。

【請求項３１】

前記選択されたパラメータが、すべてその選択されたノードに関連付けられている、時間標識、電子メールアドレス、ＩＰアドレス、ノード識別子、およびソルト値のうちの少なくとも１つを備える、請求項２９に記載のノード。

【請求項３２】

前記プロセッサがさらに、前記新しいノード識別子が前記対応するノード識別子と一致しない場合にその選択されたノードをオーバレイネットワークから除外するように構成された、請求項２９に記載のノード。

【請求項３３】

ピアトゥピアオーバレイネットワーク内で選択位置攻撃から保護するように構成されたコンピュータプログラムを有するコンピュータ可読媒体であって、

前記コンピュータプログラムは、

選択されたノードに関連付けられた新しいノード識別子を受信し、

前記選択されたノードに関連付けられた選択されたパラメータをハッシュ関数に入力して対応するノード識別子を生成することと、前記対応するノード識別子は、選択されたノード識別子の生成前に前記ノードに隣接するノードの第２の組とのリンクを保ちながら、前記選択されたノード識別子の生成の後に前記ノードに隣接するノードの第１の組とリンクを確立することにより、ピアトゥピアオーバレイネットワーク内の位置を採用するために使用され、前記ノードの第１の組は、前記ノードの第２の組とは異なり、

前記新しいノード識別子を前記対応するノード識別子と比較し、

前記新しいノード識別子が前記対応するノード識別子と一致しない場合にその選択されたノードが潜在的攻撃者であると判定することと

のために実行可能なコードを備える、コンピュータ可読媒体。

【請求項３４】

前記コードが前記選択されたパラメータを備えるデータベースを保持するようにさらに構成された、請求項３３に記載のコンピュータ可読媒体。

【請求項３５】

前記選択されたパラメータが、すべて前記選択されたノードに関連付けられている、時間標識、電子メールアドレス、ＩＰアドレス、ノード識別子、およびソルト値のうちの少なくとも１つを備える、請求項３３に記載のコンピュータ可読媒体。

【請求項３６】

前記コードがさらに、前記新しいノード識別子が前記対応するノード識別子と一致しない場合にその選択されたノードをオーバレイネットワークから除外するように構成された、請求項３３に記載のコンピュータ可読媒体。

【請求項３７】

ピアトゥピアオーバレイネットワーク内で選択位置攻撃から保護するためにノードを動

作させる方法であって、
それぞれ、１つまたは複数のノードに関連付けられた１つまたは複数のノード識別子の更新を開始する責任を検出することと、
前記１つまたは複数のノード識別子を生成するために前記１つまたは複数のノードによって使用されることができるパラメータを生成することと、
ピアトゥピアオーバレイネットワーク上でパラメータを伝送することと、前記パラメータは、選択されたノード識別子を生成するために使用され、前記選択されたノード識別子は、前記選択されたノード識別子の生成前に前記ノードに隣接するノードの第２の組とのリンクを保ちながら、前記選択されたノード識別子の生成の後に前記ノードに隣接するノードの第１の組とリンクを確立することにより、ピアトゥピアオーバレイネットワーク内の位置を採用するために使用され、前記ノードの第１の組は、前記ノードの第２の組とは異なる、
を備える方法。
【請求項３８】
前記パラメータが更新時間およびソルト値のうちの少なくとも１つを備える、請求項３７に記載の方法。
【請求項３９】
前記更新時間にノード識別子の更新を実行することをさらに備える、請求項３８に記載の方法。
【請求項４０】
前記検出することが、現在のノード識別子が選択された値と同等であるときに責任を検出することを備える、請求項３７に記載の方法。
【請求項４１】
前記検出することが、現在のノード識別子が他のどのノード識別子よりも選択された値に近いときに責任を検出することを備える、請求項３７に記載の方法。
【請求項４２】
ピアトゥピアオーバレイネットワーク内で選択位置攻撃から保護するように構成されたノードであって、
それぞれ、１つまたは複数のノードに関連付けられた１つまたは複数のノード識別子の更新を開始する責任を検出するための手段と、
前記１つまたは複数のノード識別子を生成するために前記１つまたは複数のノードによって使用されることができるパラメータを生成するための手段と、
ピアトゥピアオーバレイネットワーク上でパラメータを伝送するための手段と、前記パラメータは、選択されたノード識別子を生成するために使用され、前記選択されたノード識別子は、前記選択されたノード識別子の生成前に前記ノードに隣接するノードの第２の組とのリンクを保ちながら、前記選択されたノード識別子の生成の後に前記ノードに隣接するノードの第１の組とリンクを確立することにより、ピアトゥピアオーバレイネットワーク内の位置を採用するために使用され、前記ノードの第１の組は、前記ノードの第２の組とは異なる、
を備えるノード。
【請求項４３】
前記パラメータが更新時間およびソルト値のうちの少なくとも１つを備える、請求項４２に記載のノード。
【請求項４４】
前記更新時間にノード識別子の更新を実行するための手段をさらに備える、請求項４３に記載のノード。
【請求項４５】
前記検出するための手段が、現在のノード識別子が選択された値と同等であるときに責任を検出するための手段を備える、請求項４２に記載のノード。
【請求項４６】

前記検出するための手段が、現在のノード識別子が他のどのノード識別子よりも選択された値に近いときに責任を検出するための手段を備える、請求項４２に記載のノード。
【請求項４７】
ピアトゥピアオーバレイネットワーク内で選択位置攻撃から保護するように構成されたノードであって、
それぞれ、１つまたは複数のノードに関連付けられた１つまたは複数のノード識別子の更新を開始する責任を検出すること、および
前記１つまたは複数のノード識別子を生成するために前記１つまたは複数のノードによって使用されることができるパラメータを生成すること
を行うように構成されたプロセッサと、
ピアトゥピアオーバレイネットワーク上でパラメータを伝送するように構成されたトランシーバと、前記パラメータは、選択されたノード識別子を生成するために使用され、前記選択されたノード識別子は、前記選択されたノード識別子の生成前に前記ノードに隣接するノードの第２の組とのリンクを保ちながら、前記選択されたノード識別子の生成の後に前記ノードに隣接するノードの第１の組とリンクを確立することにより、ピアトゥピアオーバレイネットワーク内の位置を採用するために使用され、前記ノードの第１の組は、前記ノードの第２の組とは異なる、
を備えるノード。
【請求項４８】
前記パラメータが更新時間およびソルト値のうちの少なくとも１つを備える、請求項４７に記載のノード。
【請求項４９】
前記プロセッサがさらに前記更新時間にノード識別子の更新を実行するように構成された、請求項４８に記載のノード。
【請求項５０】
前記プロセッサがさらに、現在のノード識別子が選択された値と同等であるときに責任を検出するように構成された、請求項４７に記載のノード。
【請求項５１】
前記プロセッサがさらに、現在のノード識別子が他のどのノード識別子よりも選択された値に近いときに責任を検出するように構成された、請求項４７に記載のノード。
【請求項５２】
ピアトゥピアオーバレイネットワーク内で選択位置攻撃から保護するように構成されたコンピュータプログラムを有するコンピュータ可読媒体であって、
前記コンピュータプログラムは、
それぞれ、１つまたは複数のノードに関連付けられた１つまたは複数のノード識別子の更新を開始する責任を検出することと、
前記１つまたは複数のノード識別子を生成するために前記１つまたは複数のノードによって使用されることができるパラメータを生成することと、前記パラメータは、選択されたノード識別子を生成するために使用され、前記選択されたノード識別子は、前記選択されたノード識別子の生成前に前記ノードに隣接するノードの第２の組とのリンクを保ちながら、前記選択されたノード識別子の生成の後に前記ノードに隣接するノードの第１の組とリンクを確立することにより、ピアトゥピアオーバレイネットワーク内の位置を採用するために使用され、前記ノードの第１の組は、前記ノードの第２の組とは異なり、
前記ピアトゥピアオーバレイネットワーク上でパラメータを伝送することと
のために実行可能なコードを具備するコンピュータ可読媒体。
【請求項５３】
前記パラメータが更新時間およびソルト値のうちの少なくとも１つを備える、請求項５２に記載のコンピュータ可読媒体。
【請求項５４】
前記コードがさらに前記更新時間にノード識別子の更新を実行するように構成された、

請求項５３に記載のコンピュータ可読媒体。
【請求項５５】
前記コードがさらに、現在のノード識別子が選択された値と同等であるときに責任を検出するように構成された、請求項５２に記載のコンピュータ可読媒体。
【請求項５６】
前記コードがさらに、現在のノード識別子が他のどのノード識別子よりも選択された値に近いときに責任を検出するように構成された、請求項５２に記載のコンピュータ可読媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
合衆国法典第３５編第１１９条に基づく優先権の主張
本特許出願は、本願の譲受人に譲渡され、参照により本明細書に明示的に組み込まれる、２００８年6月１９日に出願された米国仮特許出願第６１／０７３９０３号、表題「Ｍｅｔｈｏｄｓ ａｎｄ Ａｐｐａｒａｔｕｓ ｆｏｒ ｒｅｄｕｃｉｎｇ ｔｈｅ Ｅｆｆｅｃｔ ｏｆ Ｃｈｏｓｅｎ Ｌｏｃａｔｉｏｎ Ａｔｔａｃｋｓ ｉｎ ａｎ Ｏｖｅｒｌａｙ Ｎｅｔｗｏｒｋ」の優先権を主張する。
【０００２】
本特許出願は、概してオーバレイネットワークの動作に関し、特に、ピアトゥピアオーバレイネットワーク内で選択位置攻撃の有効性を低減する方法および装置に関する。
【背景技術】
【０００３】
サーバベースの基盤がないときにメンバノードがその中でサービスを取得するネットワークを、本明細書では、「ピアトゥピア」オーバレイネットワークと称する。ピアトゥピアオーバレイでは、ピアノードは、サービスを提供するためとネットワークを維持するためとの両方で互いに協力する。ピアトゥピアオーバレイネットワークは、インターネットプロトコル（ＩＰ）を使用するネットワークなどの、基礎ネットワークの上に構築されることができる。
【０００４】
分散ハッシュ表（ＤＨＴ）ベースのピアトゥピアオーバレイネットワークは、情報を識別するハッシュに基づく識別子を使用する。一般に、同一のハッシュベースの機構が、ノード識別子とリソース識別子との両方の作成のために使用される。無許可の実体が特定のノード識別子を選択することができる場合、それらは特定のノードにルーティングされたクエリ内でクリティカルなプレーヤになるかまたは特定のリソースを制御することができる。かかる活動は、一般に、選択位置攻撃と称される。
【０００５】
ＤＨＴベースのネットワークにおける選択位置攻撃を解決するための従来の手法は、ノードの集中化された登録である。ノードを許可する責任を負う集中登録サーバは、ノード識別子の提供が真にランダムであることを保証することができる。選択位置攻撃を組み込むために、攻撃者は結合するための多数の試み、攻撃ベクトルを提供しない割り当てられた識別子を捨てること、を行わなければならない。登録サーバが識別の証明を求める場合、攻撃を組み込むのに十分な数の結合の試みを行うことは不可能になり得る。しかし、中央登録サーバを使用することはいくつかの問題を与える。たとえば、登録サーバが大きな責任を負い、したがって、可用性を確保するために連続した電源をもつ必要があることがある。加えて、登録サーバは、バックアップおよび特別なネットワークサーバを必要とすることがある。さらに、登録サーバが適切に動作しているとしても、それ自体が危険にさらされ、それによって、オーバレイネットワーク全体の動作を危険にさらすことがある。
【０００６】
したがって、ピアトゥピアオーバレイネットワークで選択位置攻撃の有効性を低減するために動作するシンプルな費用効率の高い機構をもつことが望ましい。

【発明の概要】
【０００７】
１つまたは複数の態様では、ピアトゥピアオーバレイネットワーク内で選択位置攻撃から保護するために動作する方法および装置を備える、ピアトゥピアオーバレイネットワーク保護システムが提供される。
【０００８】
一態様では、ピアトゥピアオーバレイネットワーク内で選択位置攻撃から保護するためにノードを動作させるための方法が提供される。この方法は、オーバレイネットワーク内の複数のノードのために新しいノード識別子が生成されるべきであると判定すること、選択されたパラメータをハッシュ関数に入力して選択されたノード識別子を生成すること、および、その選択されたノード識別子に関連付けられたピアトゥピアオーバレイネットワーク内の位置を採用することを備える。
【０００９】
一態様では、ピアトゥピアオーバレイネットワーク内で選択位置攻撃から保護するために動作することができるノードが提供される。このノードは、オーバレイネットワーク内の複数のノードに新しいノード識別子が生成されるべきであると判定するように構成されたタイミングモジュール、および、選択されたパラメータをハッシュ関数に入力して選択されたノード識別子を生成し、その選択されたノード識別子に関連付けられたピアトゥピアオーバレイネットワーク内の位置を採用するように構成されたプロセッサモジュールを備える。
【００１０】
一態様では、ピアトゥピアオーバレイネットワーク内で選択位置攻撃から保護するためにノードによって使用可能な方法が提供される。この方法は、選択されたノードに関連付けられた新しいノード識別子を受信すること、その選択されたノードに関連付けられた選択されたパラメータをハッシュ関数に入力して対応するノード識別子を生成すること、新しいノード識別子を対応するノード識別子と比較すること、および、その新しいノード識別子が対応するノード識別子と一致しない場合にその選択されたノードが潜在的攻撃者であると判定することを備える。
【００１１】
一態様では、ピアトゥピアオーバレイネットワーク内で選択位置攻撃から保護するために動作することができるノードが提供される。このノードは、選択されたノードに関連付けられた新しいノード識別子を受信するように構成されたトランシーバと、その選択されたノードに関連付けられた選択されたパラメータをハッシュ関数に入力して対応するノード識別子を生成し、その新しいノード識別子をその対応するノード識別子と比較し、その新しいノード識別子がその対応するノード識別子と一致しない場合にその選択されたノードが潜在的攻撃者であると判定するように構成されたプロセッサとを備える。
【００１２】
一態様では、ピアトゥピアオーバレイネットワーク内で選択位置攻撃から保護するためにノードを動作させる方法が提供される。その方法は、それぞれ、１つまたは複数のノードに関連付けられた１つまたは複数のノード識別子の更新を開始する責任を検出すること、その１つまたは複数のノード識別子を生成するためにその１つまたは複数のノードによって使用されることができるパラメータを生成すること、および、ピアトゥピアオーバレイネットワーク上でそのパラメータを伝送することを備える。
【００１３】
一態様では、ピアトゥピアオーバレイネットワーク内で選択位置攻撃から保護するように構成されたノードが提供される。そのノードは、それぞれ、１つまたは複数のノードに関連付けられた１つまたは複数のノード識別子の更新を開始する責任を検出し、その１つまたは複数のノード識別子を生成するためにその１つまたは複数のノードによって使用されることができるパラメータを生成するように構成されたプロセッサを備える。そのノードはさらに、ピアトゥピアオーバレイネットワーク上でそのパラメータを伝送するように

構成されたトランシーバを備える。

【００１４】

以下に記載される図面の簡単な説明、発明を実施するための形態、および特許請求の範囲を検討した後に他の態様も明らかとなろう。

【００１５】

本明細書で説明される前述の態様は、添付の図面とともに以下の説明を参照することによってより容易に明らかとなろう。

【図面の簡単な説明】

【００１６】

【図１】ピアトゥピアオーバレイ保護システムの態様を説明するネットワークを示す図。

【図２】ピアトゥピアオーバレイ保護システムの態様による、ノード識別子の更新が生じた後の図１のネットワークを示す図。

【図３】ピアトゥピアオーバレイ保護システムの態様による、ノード識別子の更新が生じた後の、ノードが互いとの通信を確立した、図２のネットワークを示す図。

【図４】ピアトゥピアオーバレイ保護システムの態様による、ノード識別子の更新が生じた後の、選択されたｆｉｎｇｅｒをノードが保持する、図３のネットワークを示す図。

【図５】ピアトゥピアオーバレイ保護システムの態様で使用される保護モジュールを示す図。

【図６】ピアトゥピアオーバレイネットワーク保護システムの態様を提供するようにノードを動作させる例示的な方法を示す図。

【図７】ピアトゥピアオーバレイネットワーク保護システムの態様で使用されるノード識別子の更新を開始するようにノードを動作させるための例示的な方法を示す図。

【図８】ピアトゥピアオーバレイネットワーク保護システムの態様で使用されるノード識別子を検証するためにノードを動作させるための例示的な方法を示す図。

【図９】ピアトゥピアオーバレイネットワーク保護システムの態様で使用される例示的な保護モジュールを示す図。

【図１０】ピアトゥピアオーバレイネットワーク保護システムの態様で使用される例示的な保護モジュールを示す図。

【図１１】ピアトゥピアオーバレイネットワーク保護システムの態様で使用される例示的な保護モジュールを示す図。

【発明を実施するための形態】

【００１７】

以下の記述は、ピアトゥピアオーバレイネットワーク内で選択位置攻撃から保護するために動作するピアトゥピアオーバレイネットワーク保護システムの態様を説明する。一態様では、分散ハッシュ表（ｄｉｓｔｒｉｂｕｔｅｄ　ｈａｓｈ　ｔａｂｌｅ、ＤＨＴ）ベースのピアトゥピアオーバレイネットワークが、オーバレイ内のすべてのノードが時間同期された協調時間サービス（cooperative time service）を維持する。たとえば、一態様では、ネットワーク時間プロトコル（ＮＴＰ）と類似した機構が、協調時間サービスを提供するために使用されることができる。ノードがピアトゥピアオーバレイネットワークに結合するとき、それはピアトゥピアオーバレイネットワークによって選択される１セットの入力を使用してハッシュ関数によって生成されるそれ自体のノード識別子をアサートする。一実装形態では、新たに結合するノードの特権は、ノード識別子の遷移のいくつか（即ち、１つまたは２つ）をノードが完了するより前の期間中に限られる。しかし、アサートされるノード識別子は、永続的ではなく、ピアトゥピアオーバレイネットワークは、各ノードが、その現在のノード識別子、現在の時刻、ソルト値、または他の情報などの情報をハッシュ関数への入力として使用して、定期的にそのノード識別子を更新することを必要とすることになる。一態様では、ノードがそれぞれの識別子を更新する時刻は、最後の変更または更新時にランダムに識別されたノードによって有限期間内にランダムに設定される。

【００１８】

企てられる選択位置攻撃は、ピアトゥピアオーバレイネットワーク上の特定の位置へのアクセスを攻撃者に与える特定のノード識別子を攻撃者がアサートするときに生じ得る。システムは、ピアトゥピアオーバレイネットワーク内のノードにノード識別子を定期的に、または選択された時間／事象の発生時に変更させることによって、このタイプの選択位置攻撃を軽減するように動作する。ノード識別子の変更は、ピアトゥピアオーバレイネットワーク上の知られている位置を攻撃者が確保するのを妨げる。たとえば、選択されたノード位置は、最長で更新と更新の間の一時間間隔、持続するので、攻撃の影響は大幅に低減される。ピアトゥピアオーバレイネットワークに結合する新しいノードの動作を、それが少なくとも１回のノード識別子の更新を経るまで、制限することによって、それはさらに低減される。ルーティングピアはノードがその識別子を正しく更新したことを確認することができるので、システムは、非常に簡単な、定量化可能な形態の評価を提供する。

【００１９】

図１は、ピアトゥピアオーバレイネットワーク保護システムの態様を説明するネットワーク１００を示す。ネットワーク１００は、インターネットプロトコルネットワークなどの任意のタイプのネットワークを備える基礎ネットワーク１０２を備える。基礎ネットワーク１０２は単一の実体として示されているが、基礎ネットワークは、ＷＡＮ、ＬＡＮ、無線ネットワーク、もしくは他のタイプのネットワークなどの任意のタイプまたは数のネットワークを備えることができる。

【００２０】

ピアトゥピアオーバレイネットワーク１０４は、基礎ネットワーク１０２の１サブセットのノードを備え、基礎ネットワーク１０２のサービスを使用してそれらのノードが通信することができるようにするために動作する。たとえば、ノード１（１０６で示す）は、ピアトゥピアオーバレイネットワーク１０４の部分であるノードを表す。ピアトゥピアオーバレイネットワーク１０４において、ノードは、通信リンク１０８によって接続されて円形ルーティング経路を形成する。通信リンク１０８は、基礎ネットワーク１０２によって提供される安全なトンネルでもよい。ピアトゥピアオーバレイネットワーク１０４は、基礎ネットワーク１０２とは異なる１セットの許可および対話で動作する。ピアトゥピアオーバレイネットワーク１０４は、任意のルーティングパターンを可能にするために任意のトポロジまたはアーキテクチャをもつことができ、それは図１に示すルーティングに限定されないことにも留意されたい。

【００２１】

ピアトゥピアオーバレイネットワーク１０４内の各ノードは、ノード識別子を設定する。説明を簡潔および簡単にするために、ピアトゥピアオーバレイネットワーク１０４の８つのノードのノード識別子は（１、４、７、１０、１３、１６、１９、および２２）である。実際には、オーバレイネットワークは、非常に多数のノードを備えることができ、より大きなノード識別子を使用することができることに留意されたい。動作中、トラフィックはピアトゥピアオーバレイネットワーク１０４の周りをどちらの方向にも流れる。したがって、ノード１は、経路１１０に沿ってトラフィックを伝送することによってノード１０と通信することができる。同様に、ノード１は、経路１１２に沿ってトラフィックを伝送することによってノード１９と通信することができる。

【００２２】

選択位置攻撃の場合には、無許可の実体が、ピアトゥピアオーバレイネットワーク１０４上の特定の位置でそれ自体をアサートしようと試みることがある。たとえば、無許可の実体１１４は、ピアトゥピアオーバレイネットワーク上のノード２１としてそれ自体をアサートすると仮定されることになる。その際、ノード２１は、ノード１９と２２の間のトラフィックを監視、中断、または、そうでない場合は備えることができる。

【００２３】

ノード２１によって提示される選択位置攻撃から保護するために、ピアトゥピアオーバレイネットワーク１０４の各ノードは、保護システムの部分として動作して定期的にまたは選択された時点にノード識別子の更新および検証を実行する保護モジュール（ＰＭ）１

１６を備える。ノード識別子を更新することによって、ノード２１で図示されるような選択位置攻撃の有効性は低減されることができる。ＰＭ１１６についてさらに詳しい説明が、それらがどのようにして選択位置攻撃からピアトゥピアオーバレイネットワーク１０４を保護するために動作するかを含めて、以下に与えられる。

【００２４】

オーバレイネットワークに結合する

図１を再び参照すると、実体１１４が、ノード識別子２１をアサートすることによってピアトゥピアオーバレイネットワーク１０４に結合し、それによって、オーバレイネットワーク上のその位置を判定する。保護システムは集中登録サーバを使用しないので、実体１１４は疑われず、ノード識別子２１を使用してオーバレイに結合することを許可される。しかし、ノード２１はピアトゥピアオーバレイネットワーク１０４にとって新しいので、保護システムはオーバレイネットワーク上のノード２１の動作を制限するように動作する。たとえば、一態様では、ノード２１は、トラフィックがピアトゥピアオーバレイネットワーク１０４上のノード間で経路指定されることができるようにするためにルーティングノードとして動作することを制限される。しかし、この制限は、下述のように、ノード識別子の少なくとも１回の更新の後まで、ノード２１がサービスにアクセスするまたはそれを提供することを、或いは、リソースまたは他のネットワーク機能に関する責任を負うことを妨げる。

【００２５】

ノード識別子の更新

図２は、ピアトゥピアオーバレイ保護システムの態様に従ってノード識別子の更新が生じた後のネットワーク１００を示す。一態様では、各ノードのＰＭ１１６は、選択された時点でまたは選択された時間間隔でノード識別子の更新を実行するように動作する。ノード識別子の更新を容易にするために、各ノードのＰＭ１１６は、同期化されたタイミングを維持する。ノード識別子の更新中、ＰＭ１１６は、それらがハッシュ関数への入力として保持する様々なタイプの情報を使用して更新ノード識別子を判定する。以下は、ハッシュ関数への選択可能な入力になり得る各ＰＭ１１６によって保持される情報の例示的なリストである。

【００２６】

１．現在の時刻
２．ノード電子メールアドレス
３．ノードＩＰアドレス
４．ソルト値
５．現在のノード識別子

図２に示されるように、オーバレイネットワーク１０４の各ノードについて、丸括弧内に示される古いノード識別子に沿って、新しいノード識別子が示されている。この説明では、図２に示す新しいノード識別子は例示的であり、他のノード識別子が生成されることが可能である。たとえば、ノード識別子１を以前にもっていたノードが今は新しいノード識別子７をもつ。ピアトゥピアオーバレイネットワーク１０４内の他のノードもまた、図２に示すように新しいノード識別子をもつ。

【００２７】

ノード識別子２１を以前にアサートした実体１１４に関して、この実体は今はノード識別子９をアサートする。

【００２８】

更新されたノード識別子を確認する

新しいノード識別子が判定された後は、各ノードの各ＰＭはその新しい識別子をその隣接ノードに伝送する。たとえば、各ノードは、ノード識別子の更新の直前に、その隣接ノードへの通信リンクを保持する。その更新の後、ＰＭは、ピアトゥピアオーバレイネットワーク１０４を介した配布のために、隣接ノードに存在する通信リンクを介して新しいノード識別子を伝送する。

【００２９】
保護システムの一態様では、ノードの新しい識別子はピアトゥピアオーバレイネットワーク１０４内の他のノードによって検証されることができる。たとえば、特定のノードのＰＭがハッシュ関数への入力として使用する情報は、ピアトゥピアオーバレイネットワーク１０４内の他のノードに知られている。たとえば、各ノードで保持される前述の情報は、ピアトゥピアオーバレイネットワーク１０４上のすべてのノードに入手可能である。したがって、ピアトゥピアオーバレイネットワーク１０４上の他のノードが、その特定のノードに関連する情報を使用してハッシュ関数を実行することによって特定のノードによってアサートされる更新されたノード識別子を検証することができる。ノードの識別子が検証されることができない場合、そのノードはそのピアトゥピアオーバレイネットワークから排除されることができる、または何らかの他のアクションが取られることができる。
【００３０】
図２を再び参照すると、実体１１４は、その新しいノード識別子９をその以前の隣接ノード（即ち、新しいノード識別子１６および４）にアサートすることができる。ノード１６および４のＰＭは、ノード識別子９を再生成しようとして実体１１４によって使用された入力のハッシュ値を再計算することによってノード識別子９が正しいことを確認するために動作する。新しいノード識別子９がどの隣接ノードによっても検証されることができない場合、実体１１４はそのピアトゥピアオーバレイネットワークから排除されることができる、または何らかの他のアクションが取られることができる。
【００３１】
図３は、ノード識別子の更新が生じた後のネットワーク１００を示し、ここでノードは、ピアトゥピアオーバレイ保護システムの態様に従って所望のルーティングパターンを取得するために互いとの通信を確立している。たとえば、ノード識別子の更新が生じた後、各ノードは、新しい近隣への新しい通信リンクが確立され、それによってオーバレイネットワークの周りの特定のルーティング経路が再確立されることができるようにするために、その新しい近隣が誰かを判定する。
【００３２】
実体１１４に関連付けられたノード識別子９がオーバレイネットワーク内の他のノードによって検証されることができないと仮定すると、実体１１４はそのオーバレイから排除される。たとえば、実体１１４はノード識別子９をもつノードがあるであろう位置に示されるが、実体１１４はそのオーバレイから除外されたものとして示され、それはピアトゥピアオーバレイネットワーク内の他のノードへの通信リンクをもたない。
【００３３】
オーバレイネットワークのｆｉｎｇｅｒを更新する
図４は、ノードがピアトゥピアオーバレイ保護システムの態様に従って所望のルーティングパターンを取得するために互いとの通信を確立している、ノード識別子の更新が生じた後のネットワーク１００を示す。新しい通信リンクが確立された後、ノードは、ピアトゥピアオーバレイネットワークを横切る直接経路を形成するコード（またはｆｉｎｇｅｒ）を形成するその元の通信リンクをまだもつことができる。たとえば、ノード７は、３０２で示されるノード１６とのおよび３０４で示されるノード１９とのその通信リンクを保持する。
【００３４】
一態様では、「古い」ｆｉｎｇｅｒを保持することは、ランダムのそして新しいノード識別子から判定された隣接のみを使用して存在するであろうものよりもより深いノード間の相互接続セットを提供するための機構である。そのようなものとして、システムは、特定のノードへのアクセスをうまく妨害する選択位置攻撃の能力に対する二次的な保護を提供する。たとえば、成功する攻撃はノードの現在のおよび以前のノード識別子位置を同時に攻撃しなければならないことになろうが、これはそのノードの以前の隣接ノードの現在のノード識別子の知識を暗示する。したがって、一態様では、深い相互接続のセットがそれ自体有益であり、システムは、全体的な接続性の目標を達成するために、保持する以前

の隣接の数を調整するように動作することができる。

【００３５】

一態様では、通信ｆｉｎｇｅｒは、新しい通信リンクが確立された後に、維持されるまたは取り除かれることができる。たとえば、一態様では、ｆｉｎｇｅｒは、たとえば次のノード識別子更新が実行された後など、時間が経つと省かれる。

【００３６】

したがって、ピアトゥピアオーバレイネットワーク保護システムは、新しいノード識別子が生成されることができるようにしそれによって選択位置攻撃の有効性を最小化するように動作する保護モジュールを備える。さらに、特定のノードに関連付けられた任意の新しい識別子が、ピアトゥピアオーバレイネットワーク上の他のノードによって検証されることができる。これは、選択位置攻撃を企てるいずれかの実体の動作がノード識別子の更新間の時間間隔に制限されることになるので、この実体の動作の有効性をさらに低減する。加えて、オーバレイに結合する新しいノードの動作がさらに制限されて、任意の攻撃者の影響をさらに軽減する。

【００３７】

図５は、ピアトゥピアオーバレイ保護システムの態様で使用される保護モジュール５００を示す。たとえば、保護モジュール５００は、図１に示す保護モジュール１１６としての使用に適する。保護モジュール５００は、プロセッサモジュール５０２、ソルトモジュール５０４、メモリ５０６、タイミングモジュール５０８、およびトランシーバモジュール５１０を備え、それらはすべてデータバス５１２に結合されている。保護モジュール５００は単に一実装形態であり、態様の範囲内で他の実装形態が可能であることに留意されたい。

【００３８】

トランシーバモジュール５１０は、保護モジュール５００がピアトゥピアオーバレイネットワーク上の複数のノードとデータもしくは他の情報を通信することを可能にするように動作するハードウェアおよび／またはハードウェア実行ソフトウェアを備える。一態様では、トランシーバモジュール５１０は、ピアトゥピアオーバレイネットワークのノードと１つまたは複数の通信リンク５１４を確立するように動作することができる。たとえば、通信リンク５１４は、基礎ＩＰネットワークのサービスを使用して形成される安全なトンネルでもよい。

【００３９】

メモリモジュール５０６は、ピアトゥピアオーバレイネットワークの１つまたは複数のノードに関連する情報を備えるデータベースを格納するように動作することができる任意の適切なストレージデバイスを備える。たとえば、その情報は、電子メールアドレス、ＩＰアドレス、ノード識別子、ソルト値または任意の他のタイプの情報を含むがこれらに限定されない。たとえば、そのデータベースは、いつ新しいノード識別子が生成されるべきかを指示する時間値もまた含むことができる。

【００４０】

タイミングモジュール５０８は、保護モジュール５００に同期化されたタイミングを提供するために動作するハードウェアおよび／またはハードウェア実行ソフトウェアを備える。一態様では、タイミングモジュール５０８は、ピアトゥピアオーバレイネットワークの他のノードと同期化される。それによって、タイミングモジュールは、保護モジュール５００がピアトゥピアオーバレイネットワークの他のノードと同期化された機能を実行することを可能にする。かかる機能は、新しいノード識別子の生成を含む。

【００４１】

ソルトモジュール５０４は、新しいノード識別子を生成するために使用されることができるソルト値を生成するために動作するハードウェアおよび／またはハードウェア実行ソフトウェアを備える。一態様では、ソルトモジュール５０４によって生成されるソルト値は、ピアトゥピアオーバレイネットワーク上の他のノードに伝送される。ソルト値は、新しいノード識別子を生成するために、ハッシュ関数への入力として使用される。一態様で

は、ソルトモジュール５０４は、ソルト値を生成するために、任意の適切な関数またはアルゴリズムを使用する。

【００４２】

１つまたは複数の態様で、プロセッサモジュール５０２は、ＣＰＵ、プロセッサ、ゲートアレイ、ハードウェア論理、記憶素子、および／またはハードウェア実行ソフトウェアのうちの少なくとも１つを備える。一態様では、プロセッサモジュール５０２は、保護モジュールを制御して以下の機能を実行するために動作することができる。

【００４３】

ノード識別子の生成

一態様では、プロセッサモジュール５０２は、新しいノード識別子を生成するために、ハッシュ関数を実行する。たとえば、プロセッサモジュール５０２は、ハッシュ関数への選択可能な入力になり得るメモリ５０６に格納されたデータベース内の情報を保持する。データベースに格納された情報はまた、新しいノード識別子が生成されるべき時間を識別する。プロセッサモジュールは、タイミングモジュール５０８を使用して新しいノード識別子を生成する時間がいつ生じたかを検出し、それに応答して、データベースからの選択された情報をハッシュ関数への入力として使用して新しいノード識別子を生成する。プロセッサモジュール５０２は、トランシーバモジュール５１０を制御することによってピアトゥピアオーバレイネットワーク上の他のノードにその新しいノード識別子を伝送して通信リンク５１４上でその情報を伝送するために動作する。

【００４４】

ノード識別子を検証する

もう１つの態様では、プロセッサモジュール５０２は、１つまたは複数のノードに関連付けられたノード識別子を検証するように構成される。ノード識別子の更新が生じた後、ピアトゥピアオーバレイネットワークのノードは、ピアトゥピアオーバレイネットワーク上でそれらの新しいノード識別子を伝送する。プロセッサモジュール５０２は、特定のノードに関連付けられた新しいノード識別子が正しいかどうかを検証するために動作する。たとえば、プロセッサモジュール５０２は、メモリ５０６に格納されたデータベースから特定のノードに関連付けられた情報を取得する。一態様では、ノードが新しいノード識別子を生成するために使用する情報は、ピアトゥピアオーバレイネットワーク上のすべてのノードに知られている。選択された情報を取得した後、プロセッサモジュール５０２は、特定のノードのためにノード識別子を生成するために、適切な情報を入力として使用してハッシュ関数を実行する。この生成されたノード識別子は、その特定のノードから受信される新しいノード識別子と一致しなければならない。生成されたノード識別子が受信された識別子と一致しない場合、そのときそのノードは可能性のある攻撃者であり、ピアトゥピアオーバレイネットワークからさらに制限されることができると見なされる。

【００４５】

ノード識別子の生成を開始する

もう１つの態様では、プロセッサモジュール５０２は、ピアトゥピアオーバレイネットワーク上のすべてのノードのための新しいノード識別子の生成を開始するように構成される。一態様では、プロセッサモジュール５０２は、現在のノード識別子が事前選択された値と等しいかどうか、または現在の識別子がピアトゥピアオーバレイネットワーク上の他のノードよりも選択された値に近いかどうかを判定する。現在の値が最も近い場合、そのときプロセッサモジュール５０２はそれが次のノード識別子更新を開始する責任を負うと判定する。

【００４６】

次のノード識別子更新を開始するために、プロセッサモジュール５０２は、更新の時刻およびソルト値を判定する。ソルト値は、ソルトモジュール５０５から取得される。更新の時刻およびソルト値は、ピアトゥピアオーバレイネットワーク上の他のノードに伝送される。判定された時刻に、ピアトゥピアオーバレイネットワーク上のすべてのノードが、ソルト値、および場合によっては他の情報、をハッシュ関数に入力することによって、新

しいノード識別子を算定する。新しいノード識別子が生成された後、ノードはこれらの識別子をピアトゥピアオーバレイネットワーク上の他のノードに伝送する。

【００４７】

もう１つの態様では、新しいノード識別子を生成する時刻はピアトゥピアオーバレイネットワーク上のすべてのノードに知られていると見なされる。この場合、プロセッサモジュール５０２は、ソルトモジュール５０５からソルト値を取得し、このソルト値をピアトゥピアオーバレイネットワーク上の他のノードに伝送する。したがって、他のノードに配布される情報の量は低減される。

【００４８】

一態様では、ピアトゥピアオーバレイネットワーク保護システムは、機械可読媒体に格納されたまたは実施された１つまたは複数のプログラム命令（「命令」）または「コード」のセットをもつコンピュータプログラム製品を備える。そのコードが少なくとも１つのプロセッサ、たとえばプロセッサモジュール５０２のプロセッサ、によって実行されるとき、それらの実行は保護モジュール５００に本明細書に記載されたピアトゥピアオーバレイネットワーク保護システムの機能を提供させる。たとえば、その機械可読媒体は、フロッピ（登録商標）ーディスク、ＣＤ－ＲＯＭ、メモリカード、フラッシュメモリデバイス、ＲＡＭ、ＲＯＭ、または任意の他のタイプのメモリデバイス、或いは、保護モジュール５００にインタフェースする機械可読媒体を備える。もう１つの態様では、コードのセットは、外部デバイスまたは通信ネットワークリソースから保護モジュール５００にダウンロードされることができる。コードのセットは、実行されるとき、本明細書に記載のピアトゥピアオーバレイネットワーク保護システムの態様を提供するために動作する。

【００４９】

図６は、ピアトゥピアオーバレイネットワーク保護システムの態様を提供するようにノードを動作させるための例示的な方法６００を示す。明確にするために、方法６００は、図５に示す保護モジュール５００を参照して以下に説明される。一態様では、プロセッサモジュール５０２は、保護モジュール５００を制御して下記の機能を実行するために、１つまたは複数のセットのコードを実行する。

【００５０】

ブロック６０２で、ハッシュ関数への入力になることができるパラメータのデータベースが保持される。一態様では、プロセッサモジュール５０２は、メモリ５０６内のデータベースを保持する。たとえば、そのデータベースは、現在の時刻、電子メールアドレス、ＩＰアドレス、現在のノード識別子、ソルト値、または、ピアトゥピアオーバレイネットワーク上で動作する１つまたは複数のノードに関連する他の任意のパラメータを備えるが、これらに限定されない。

【００５１】

ブロック６０４では、任意選択のステップで、少なくとも１つのソルト値がピアトゥピアオーバレイネットワークから受信される。一態様では、トランシーバモジュール５１０が、オーバレイネットワーク内の１つまたは複数の他のノードから少なくとも１つのソルト値を受信し、メモリ５０６内に位置するパラメータのデータベース内にその少なくとも１つのソルト値を格納する。たとえば、その１つまたは複数のソルト値は、その１つまたは複数のソルト値を生成し、オーバレイネットワーク上の他のノードに配布するために指定されたピアトゥピアオーバレイネットワーク内の特定の１つのノードまたは複数のノードから受信されることができる。

【００５２】

ブロック６０６で、ノード識別子の更新が必要かどうかに関する判定が行われる。一態様では、ノード識別子の更新は、現在の時刻および／または選択された事象に基づいて判定される。たとえば、プロセッサモジュール５０２は、現在の時刻および／または事象に基づいて、ノード識別子の更新が必要かどうかを判定する。新しいノード識別子が必要である場合、本方法はブロック６０８に進む。新しいノード識別子更新が必要でない場合、本方法はブロック６０２に進む。

【００５３】
ブロック６０８で、ハッシュ関数への入力になるパラメータが選択される。一態様では、プロセッサモジュール５０２が、メモリ５０６に格納されたデータベースからパラメータを判定する。たとえば、ハッシュ関数への入力になるパラメータは、現在の時刻、電子メールアドレス、ＩＰアドレス、現在のノード識別子、ソルト値、またはデータベースに格納された他の任意のパラメータを備えるが、これらに限定されない。任意のノードにあるパラメータがピアトゥピアオーバレイネットワーク上のすべてのノードに知られていることに留意されたい。したがって、任意の特定のノードに関連付けられたパラメータは、そのノードのノード識別子を検証するために使用されることができる。
【００５４】
ブロック６１０で、新しいノード識別子を生成するために、ハッシュ関数が実行される。一態様では、プロセッサモジュール５０２が、メモリ５０６から適切なパラメータを検索し、そのパラメータを所定のハッシュ関数に入力することによってハッシュ関数を実行して新しいノード識別子を生成するように動作する。
【００５５】
ブロック６１２で、ピアトゥピアオーバレイネットワーク上の新しい位置が、新しいノード識別子に基づいて採用される。一態様では、トランシーバモジュール５１０が、その新しいノード識別子に基づいて現在のノードに現在隣接しているノードとリンクを確立するために動作する。
【００５６】
したがって、本方法６００は、ピアトゥピアオーバレイネットワーク保護システムの態様を提供するために、ノードで使用可能である。本方法６００は単に一実装形態であり、本方法６００の動作は様々な態様の範囲内で再構成または他の方法で修正され得ることに留意されたい。したがって、他の実装形態が本明細書に記載の様々な態様の範囲内で可能である。
【００５７】
図７は、ピアトゥピアオーバレイ保護システムの態様で使用されるノード識別子の更新を開始するようにノードを動作させるための例示的な方法７００を示す。たとえば、本方法７００は、ピアトゥピアオーバレイネットワーク内のすべてのノードについてノード識別子の更新を開始するために指定されたピアトゥピアオーバレイネットワーク内のノードで動作する保護モジュールに適する。明確にするために、本方法７００は、図５に示す保護モジュール５００を参照して以下に説明される。一態様では、プロセッサモジュール５０２が、下記の機能を実行するために、コードの１つまたは複数のセットを実行して保護モジュール５００を制御する。
【００５８】
ブロック７０２で、ノードがピアトゥピアオーバレイネットワーク内でノード識別子の更新を開始する責任を負うという判定が行われる。一態様では、プロセッサモジュール５０２が、現在のノード識別子が事前選択された値に最も近いと判定する。たとえば、事前選択された値に最も近いノード識別子をもつノードが、次のノード識別子の更新を開始する責任を負う。保護モジュール５００は、事前選択された値に最も近いノード識別子をもつノードに含まれると見なされることになる。
【００５９】
ブロック７０４で、ノード識別子の更新がいつ生じるべきかを指示する更新時間が生成される。一態様では、プロセッサモジュール５０２が、更新時間を生成する。
【００６０】
ブロック７０６では、任意選択動作で、ソルト値が生成される。一態様では、ソルトモジュール５０４がソルト値を生成する。一態様では、ソルト値は、ハッシュ関数への入力として使用されるパラメータである。
【００６１】
ブロック７０８で、更新時間および任意選択のソルト値が、ピアトゥピアオーバレイネ

ットワーク上のノードに伝送される。たとえば、トランシーバモジュール５１０が、必要に応じて更新時間およびソルト値を伝送するために動作する。

【００６２】

ブロック７１０で、ノード識別子の更新が指定された更新時間に実行される。一態様では、ピアトゥピアオーバレイネットワーク内のノードが、図６に示す方法６００に従ってノード識別子の更新を実行する。

【００６３】

したがって、方法７００は、ピアトゥピアオーバレイ保護システムの態様で使用されるためのノード識別子の更新を開始するためにノードで使用可能である。方法７００は単に一実装形態であり、方法７００の動作は様々な態様の範囲内で再構成されるまたは他の方法で修正されることができることに留意されたい。

【００６４】

図８は、ピアトゥピアオーバレイネットワーク保護システムの態様で使用されるノード識別子を検証するためにノードを動作させるための例示的な方法８００を示す。明確にするために、本方法８００は、図５に示す保護モジュール５００を参照して以下に説明される。一態様では、プロセッサモジュール５０２が、下記の機能を実行するために、１つまたは複数のセットのコードを実行して保護モジュール５００を制御する。

【００６５】

ブロック８０２で、１つまたは複数の新しいノード識別子が、ピアトゥピアオーバレイネットワーク上の１つまたは複数のノードから受信される。一態様では、トランシーバモジュール５１０が、通信リンク５１４を使用して新しいノード識別子を受信するために動作する。

【００６６】

ブロック８０４では、ブロック８０２で新しいノード識別子を提供したノードのノード識別子を生成するために、ハッシング関数が実行される。一態様では、プロセッサモジュール４０２が動作してメモリ５０６内のデータベースから１つまたは複数のノードのそれぞれに関連付けられたパラメータセットを取得する。各パラメータセットは、対応するノード識別子を生成するためにプロセッサモジュール５０２によって実行されるハッシュ関数への入力である。

【００６７】

ブロック８０６では、ブロック８０２で受信された新しいノード識別子のいずれかがブロック８０４で生成されたそれらの対応する識別子と一致しないかどうかに関する判定が行われる。一態様では、プロセッサモジュール５０２は、新しいノード識別子を対応するノード識別子と比較するために動作する。ノード識別子のうちのいずれかが一致しない場合、本方法はブロック８０８に進む。すべてのノード識別子が一致する場合、本方法はブロック８１０に進む。

【００６８】

ブロック８０８で、一致しなかったノード識別子に関連付けられたノードが可能性のある位置攻撃者であるとしてフラグを立てられる。一態様では、プロセッサモジュール５０２がこの機能を実行する。たとえば、プロセッサモジュール５０２は、オーバレイネットワーク内の他のノードと通信して特定のノード識別子の検証失敗を信号で伝える。

【００６９】

ブロック８１０で、通信リンクが検証されたノード識別子をもつノードと確立される。一態様では、プロセッサモジュール５０２が、所望のピアトゥピアオーバレイネットワークルーティングパターンが確立されることができるように、トランシーバモジュール５１０を制御して検証されたノード識別子をもつノードとの通信リンクを確立するために動作する。

【００７０】

ブロック８１２で、前のノード識別子構成から存在し得る通信ｆｉｎｇｅｒが取り除かれることができる。一態様では、各ノードは、全体的な接続性目標を達成するために、相

互接続セットを保持する。したがって、プロセッサモジュール５０２は、いくつの、および、どの通信ｆｉｎｇｅｒが全体的な接続性目標を達成するために保持されるべきかを判定するために動作する。一態様では、トランシーバモジュール５１０は、全体的な接続性目標が達成されることができるように、プロセッサモジュール５０２による終了のために識別された任意の通信ｆｉｎｇｅｒを終了されるように動作する。

【００７１】

したがって、方法８００は、ピアトゥピアオーバレイネットワーク保護システムの態様で使用されるためのノード識別子を検証するためにノードで作動する。本方法８００は単なる一実装形態であり、本方法８００の動作は様々な態様の範囲内で再構成されるまたは他の方法で修正されることができることに留意されたい。

【００７２】

図９は、オーバレイネットワーク保護システムの態様で使用される例示的な保護モジュール９００を示す。たとえば、保護モジュール９００は、図５に示す保護モジュール５００としての使用に適する。一態様では、保護モジュール９００は、本明細書に記載のオーバレイネットワーク保護システムの態様を提供するように構成された１つまたは複数のモジュールを備える少なくとも１つの集積回路によって実装される。たとえば、一態様では、各モジュールは、ハードウェアおよび／またはハードウェア実行ソフトウェアを備える。

【００７３】

保護モジュール９００は、一態様ではタイミングモジュール５０８を備える、オーバレイネットワーク内の複数のノードのために新しいノード識別子が生成されるべきであることを判定するための手段（９０２）を備える第１のモジュールを備える。保護モジュール９００はまた、一態様ではプロセッサモジュール５０２を備える、選択されたノード識別子を生成するためにハッシュ関数に選択されたパラメータを入力するための手段（９０４）を備える第２のモジュールも備える。保護モジュール９００はまた、一態様ではプロセッサモジュール５０２を備える、選択されたノード識別子に関連付けられたピアトゥピアオーバレイネットワーク内の位置を採用するための手段（９０６）を備える第３のモジュールも備える。

【００７４】

図１０は、オーバレイネットワーク保護システムの態様で使用されるための例示的な保護モジュール１０００を示す。たとえば、保護モジュール１０００は、図５に示す保護モジュール５００としての使用に適する。一態様では、保護モジュール１０００は、本明細書に記載のオーバレイネットワーク保護システムの態様を提供するように構成された１つまたは複数のモジュールを備える少なくとも１つの集積回路によって実装される。たとえば、一態様では、各モジュールが、ハードウェアおよび／またはハードウェア実行ソフトウェアを備える。

【００７５】

保護モジュール１０００は、一態様ではトランシーバモジュール５１０を備える、選択されたノードに関連付けられた新しいノード識別子を受信するための手段（１００２）を備える第１のモジュールを備える。保護モジュール１０００はまた、一態様ではプロセッサモジュール５０２を備える、対応するノード識別子を生成するためにハッシュ関数に選択されたノードに関連付けられた選択されたパラメータを入力するための手段（１００４）を備える第２のモジュールも備える。保護モジュール１０００はまた、一態様ではプロセッサモジュール５０２を備える、新しいノード識別子を対応するノード識別子と比較するための手段（１００６）を備える第３のモジュールも備える。保護モジュール１０００はまた、一態様ではプロセッサモジュール５０２を備える、新しいノード識別子が対応するノード識別子と一致しない場合に選択されたノードが潜在的攻撃者であると判定するための手段（１００８）を備える第４のモジュールも備える。

【００７６】

図１１は、オーバレイネットワーク保護システムの態様で使用されるための例示的な保

護モジュール１１００を示す。たとえば、保護モジュール１１００は、図５に示す保護モジュール５００としての使用に適する。一態様では、保護モジュール１１００は、本明細書に記載のオーバレイネットワーク保護システムの態様を提供するように構成された１つまたは複数のモジュールを備える少なくとも１つの集積回路によって実装される。たとえば、一態様では、各モジュールはハードウェアおよび／またはハードウェア実行ソフトウェアを備える。

【００７７】

保護モジュール１１００は、一態様ではプロセッサモジュール５０２を備える、それぞれ、１つまたは複数のノードに関連付けられた１つまたは複数のノード識別子の更新を開始する責任を検出するための手段（１１０２）を備える第１のモジュールを備える。保護モジュール１１００はまた、一態様ではプロセッサモジュール５０２を備える、１つまたは複数のノード識別子を生成するために１つまたは複数のノードによって使用されることができるパラメータを生成するための手段（１１０４）を備える第２のモジュールも備える。保護モジュール１１００はまた、一態様ではトランシーバモジュール５１０を備える、ピアトゥピアオーバレイネットワーク上でパラメータを伝送するための手段（１１０６）を備える第３のモジュールも備える。

【００７８】

本明細書で開示される態様に関して記載される様々な例示的論理、論理ブロック、モジュールおよび回路は、汎用プロセッサ、ディジタル信号プロセッサ（ＤＳＰ）、特定用途向け集積回路（ＡＳＩＣ）、書替え可能ゲートアレイ（ＦＰＧＡ）、または他のプログラム可能論理デバイス、個別ゲートもしくはトランジスタ論理、個別ハードウェア素子、或いは、本明細書に記載の機能を実行するように設計されたそれらの任意の組合せで実装または実行されることができる。汎用プロセッサはマイクロプロセッサでもよいが、代替では、そのプロセッサは任意の従来のプロセッサ、コントローラ、マイクロコントローラまたは状態機械でもよい。プロセッサはまた、たとえばＤＳＰおよびマイクロプロセッサの組合せ、複数のマイクロプロセッサ、ＤＳＰコアと一緒の１つまたは複数のマイクロプロセッサ、或いは他の任意のかかる構成などのコンピューティングデバイスの組合せとして実装されることもできる。

【００７９】

本明細書で開示される態様に関して記載される方法またはアルゴリズムのステップは、直接ハードウェアに、プロセッサによって実行されるソフトウェアモジュールに、またはその２つの組合せで実施されることができる。ソフトウェアモジュールは、ＲＡＭメモリ、フラッシュメモリ、ＲＯＭメモリ、ＥＰＲＯＭメモリ、ＥＥＰＲＯＭメモリ、レジスタ、ハードディスク、取外し可能ディスク、ＣＤ－ＲＯＭ、または、当技術分野で知られている他の任意の形態の記憶媒体内に存在し得る。例示的な記憶媒体はプロセッサに結合され、そのプロセッサはその記憶媒体から情報を読むまたはそこに情報を書き込むことができる。代替では、記憶媒体はプロセッサに不可欠になり得る。プロセッサおよび記憶媒体はＡＳＩＣ内に存在し得る。ＡＳＩＣは無線通信デバイス内に存在し得る。代替では、プロセッサおよび記憶媒体は、無線通信デバイス内の個別の素子として存在し得る。

【００８０】

開示される態様の説明は、当業者が本発明を作るまたは使用することを可能にするために提供される。これらの態様の様々な修正形態が当業者には容易に明らかになることができ、本明細書に定義される一般的原理は、本発明の趣旨および範囲を逸脱することなく、たとえばインスタントメッセージングサービスまたは任意の一般的な無線データ通信アプリケーションなど、他の態様に適用されることができる。したがって、本発明は、本明細書に示される態様に限定されるものではなく、本明細書で開示される原理および新しい特徴と一致する最も広い範囲を認められるべきものである。用語の「例示的」は、専ら本明細書において使用されて「一例、事例、または実例としての役割を果たす」ことを意味する。「例示的」なものとして本明細書に記載されるいずれの態様も、他の態様よりも好ましいまたは有利なものとして必ずしも解釈されるべきではない。

【００８１】

したがって、ピアトゥピアオーバレイネットワーク保護システムの態様が本明細書において図解され説明されているが、これらの趣旨または本質的特性を逸脱することなくこれらの態様への様々な変更形態が作られ得ることが理解されよう。したがって、本明細書における開示および説明は、例示的なものを意図し、以下の特許請求の範囲に記載の本発明の範囲を制限しない。

【図１】

図 1

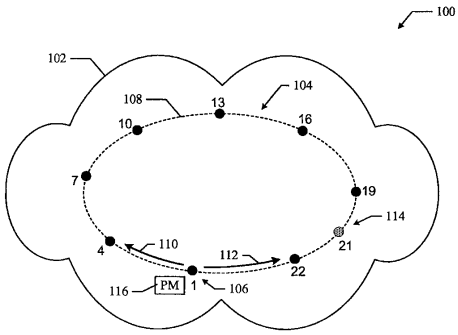

FIG. 1

【図２】

図 2

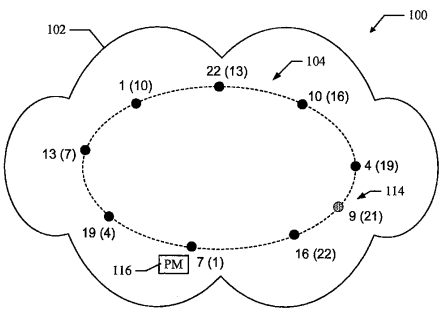

FIG. 2

【図３】

図 3

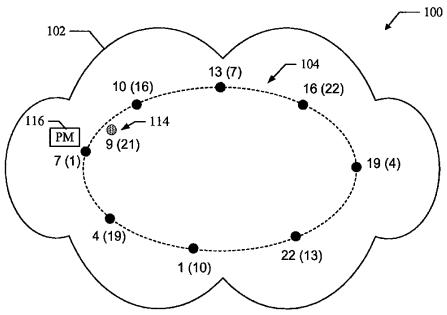

FIG. 3

【図４】

図 4

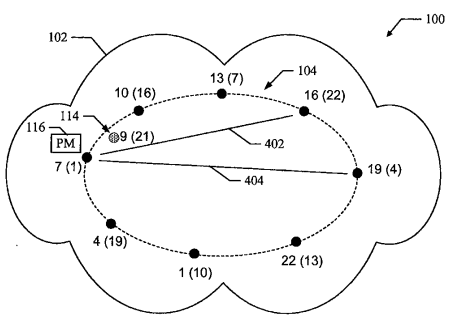

FIG. 4

【図５】

図５

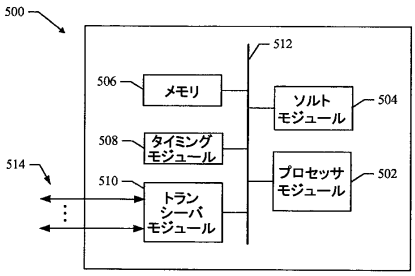

FIG. 5

【図６】

図６

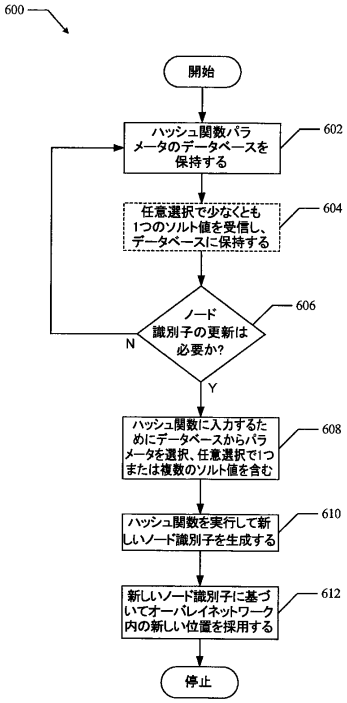

FIG. 6

【図７】

図７

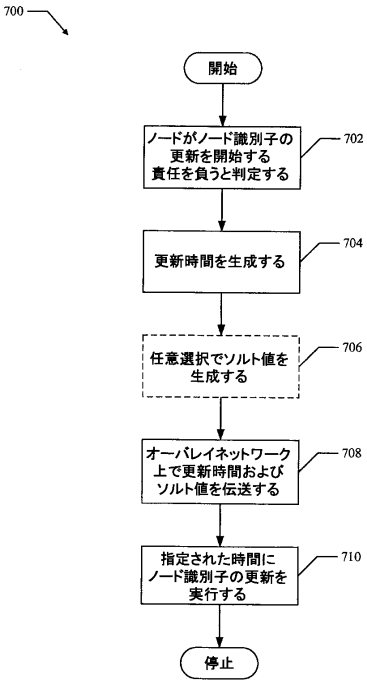

FIG. 7

【図８】

図８

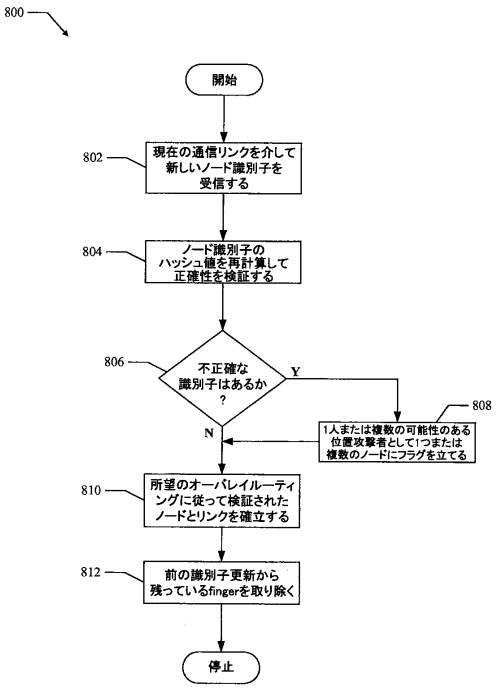

FIG. 8

【図９】

図 9

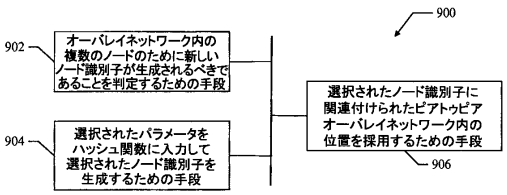

FIG. 9

【図１０】

図 10

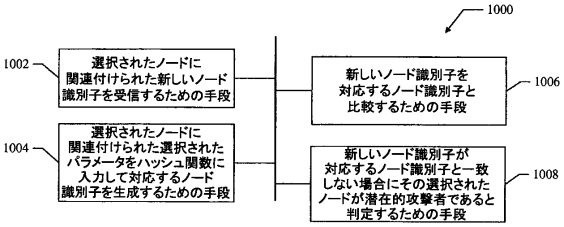

FIG. 10

【図１１】

図 11

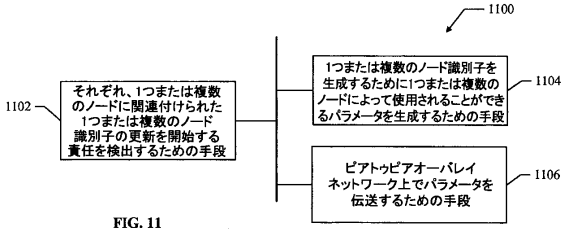

FIG. 11

フロントページの続き

(74)代理人 100075672
弁理士 峰 隆司
(74)代理人 100095441
弁理士 白根 俊郎
(74)代理人 100084618
弁理士 村松 貞男
(74)代理人 100103034
弁理士 野河 信久
(74)代理人 100119976
弁理士 幸長 保次郎
(74)代理人 100153051
弁理士 河野 直樹
(74)代理人 100140176
弁理士 砂川 克
(74)代理人 100101812
弁理士 勝村 紘
(74)代理人 100124394
弁理士 佐藤 立志
(74)代理人 100112807
弁理士 岡田 貴志
(74)代理人 100111073
弁理士 堀内 美保子
(74)代理人 100134290
弁理士 竹内 将訓
(74)代理人 100127144
弁理士 市原 卓三
(74)代理人 100141933
弁理士 山下 元
(72)発明者 ハーディー、エドワード・ティー. ・エル.
アメリカ合衆国、カリフォルニア州 ９２１２１、サン・ディエゴ、モアハウス・ドライブ ５７７５
(72)発明者 ドンデティ、ラクシュミナス・アール.
アメリカ合衆国、カリフォルニア州 ９２１２１、サン・ディエゴ、モアハウス・ドライブ ５７７５
(72)発明者 ジャヤラム、ランジス・エス.
アメリカ合衆国、カリフォルニア州 ９２１２１、サン・ディエゴ、モアハウス・ドライブ ５７７５
(72)発明者 ナラヤナン、ビドヤ
アメリカ合衆国、カリフォルニア州 ９２１２１、サン・ディエゴ、モアハウス・ドライブ ５７７５

審査官 中里 裕正

(56)参考文献 Condie, T. et al., Maelstrom: Churn as Shelter, Technical Report, ２００５年１１月１０日, No. UCB/EECS-2005-11, ＵＲＬ, http://www.eecs.berkeley.edu/Pubs/TechRpts/2005/EECS-2005-11.html
Dinger, J. and Hartenstein, H., Defending the Sybil Attack in P2P Networks:Taxonomy, Challenges, and p Proposal for Self-Registration, Proceedings of the First Internationa

l Conference on Availability Reliability and Security, ２００６年 4月, p.756-763

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ　　９／３２
Ｇ０９Ｃ　　１／００
ＪＳＴＰｌｕｓ／ＪＭＥＤＰｌｕｓ／ＪＳＴ７５８０（ＪＤｒｅａｍＩＩＩ）