(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5255065号
(P5255065)
(45)発行日　平成25年8月7日(2013.8.7)　(24)登録日　平成25年4月26日(2013.4.26)

(51)Int.Cl.　　F I
H04L 12/46 (2006.01)　　H04L 12/46　A
H04L 9/32 (2006.01)　　H04L 9/00　675B

請求項の数 10　(全 18 頁)

(21)出願番号	特願2010-532680 (P2010-532680)
(86)(22)出願日	平成20年10月8日 (2008.10.8)
(65)公表番号	特表2011-509539 (P2011-509539A)
(43)公表日	平成23年3月24日 (2011.3.24)
(86)国際出願番号	PCT/IB2008/054132
(87)国際公開番号	WO2009/057004
(87)国際公開日	平成21年5月7日 (2009.5.7)
審査請求日	平成23年10月11日 (2011.10.11)
(31)優先権主張番号	60/984,527
(32)優先日	平成19年11月1日 (2007.11.1)
(33)優先権主張国	米国(US)
(31)優先権主張番号	12/036,757
(32)優先日	平成20年2月25日 (2008.2.25)
(33)優先権主張国	米国(US)

(73)特許権者　598036300
テレフオンアクチーボラゲット　エル　エム　エリクソン（パブル）
スウェーデン国　ストックホルム　エス－１６４　８３
(74)代理人　100095957
弁理士　亀谷　美明
(74)代理人　100096389
弁理士　金本　哲男
(74)代理人　100101557
弁理士　萩原　康司
(74)代理人　100128587
弁理士　松本　一騎

最終頁に続く

(54)【発明の名称】プロキシを通じて接続されたホスト間の安全なネイバディスカバリ

(57)【特許請求の範囲】
【請求項１】
プロキシを通じて接続されたホスト間の安全なネイバディスカバリの方法であって、
第１ホストから、前記プロキシにおいて、第２ホストを宛先としたネイバディスカバリ（ＮＤ）メッセージを受信するステップであって、前記ＮＤメッセージは、前記第１ホストのインターネットプロトコル（ＩＰ）アドレスと、前記第１ホストのレイヤ２アドレスと、前記第１ホストのレイヤ２アドレスに少なくとも部分的に基づく前記第１ホストの第１署名とを含むステップと、
前記プロキシにおいて、前記ＮＤメッセージを、
前記ＮＤメッセージから前記第１ホストのレイヤ２アドレスを追加メッセージフィールドへコピーし、
前記第１ホストのレイヤ２アドレスを前記プロキシのレイヤ２アドレスで上書きし、
前記プロキシのレイヤ２アドレスに少なくとも部分的に基づく前記プロキシの第２署名を挿入すること
によって、修正するステップと、
修正した前記ＮＤメッセージを前記第２ホストへ送信するステップと
を含む方法。
【請求項２】
前記第２ホストにおいて、修正した前記ＮＤメッセージを受信するステップと、
前記プロキシの公開鍵をトラストアンカから取得するステップと、

前記第２ホストにおいて、前記プロキシの前記公開鍵を用いて、前記第２署名を検証するステップと、
前記第２ホストにおいて、前記プロキシのレイヤ２アドレスを、前記第１ホストのＩＰアドレスと関連させて記憶するステップと
をさらに含む、請求項１に記載の方法。
【請求項３】
前記プロキシにおいて、前記第２ホストから、前記第１ホストのＩＰアドレスと、前記プロキシのレイヤ２アドレスとを含むデータパケット受信するステップ
をさらに含む、請求項２に記載の方法。
【請求項４】
前記第２ホストにおいて、修正された前記ＮＤメッセージを受信するステップと、
前記第２ホストにおいて、前記第２署名を検証するステップと、
前記第２ホストにおいて、前記プロキシのレイヤ２アドレスを前記第１ホストのレイヤ２アドレスで上書きすることによって、前記ＮＤメッセージを再構成するステップと、
前記第１ホストの前記第１署名を検証するステップと、
前記第２ホストにおいて、前記プロキシのレイヤ２アドレスを、前記第１ホストのＩＰアドレスと関連させて記憶するステップと
さらに含む、請求項１に記載の方法。
【請求項５】
前記プロキシの前記第２署名は、前記第１ホストのＩＰアドレスと、前記第２ホストのＩＰアドレスと、前記第１ホストのレイヤ２アドレスと、前記第１ホストの前記第１署名とにさらに基づく、請求項１に記載の方法。
【請求項６】
前記プロキシの前記第２署名は、前記ＮＤメッセージの全部の情報フィールドに基づく、請求項５に記載の方法。
【請求項７】
ホストにおいてネイバディスカバリ（ＮＤ）メッセージを安全に受信する方法であって、
前記ホストにおいて、プロキシのレイヤ２アドレスと、ピアホストのレイヤ２アドレスと、前記ピアホストの署名と、前記プロキシの署名とを含む前記ＮＤメッセージを受信するステップと、
前記プロキシの公開鍵を使用して、前記プロキシの署名を検証するステップと、
前記プロキシのレイヤ２アドレスを前記ピアホストのレイヤ２アドレスで置き換えることによって、前記ＮＤメッセージを修正するステップと、
前記ピアホストの公開鍵を使用して、前記ピアホストの署名を検証するステップと、
前記ピアホストと通信するためのレイヤ２アドレスとして、前記プロキシのレイヤ２アドレスを記憶するステップと
前記ホストから、前記ホストの秘密鍵に基づく署名を含むＮＤ応答メッセージを送信するステップと、
を含む方法。
【請求項８】
第１ホストからネイバディスカバリ（ＮＤ）メッセージを受信する第１レイヤ２接続と、
前記第１レイヤ２接続から前記ＮＤメッセージを受信し、
前記第１ホストのレイヤ２アドレスである少なくとも１つの元のアドレスを含む第１フィールドと、前記第１ホストの第１署名を含む第２フィールドとを前記ＮＤメッセージから読み出し、
受信した前記ＮＤメッセージから前記少なくとも１つの元のアドレスを第３フィールドへコピーし、
前記第１フィールドにおいて前記少なくとも１つの元のアドレスのうちの１つをプロキ

シのレイヤ２アドレスである前記プロキシのアドレスで上書きし、
前記プロキシの前記アドレスと、前記少なくとも１つの元のアドレスとに基づく前記プロキシの第２署名を挿入すること
によって、前記ＮＤメッセージを修正する処理部と、
修正された前記ＮＤメッセージを第２ホストへ送信する第２レイヤ２接続と
を備えるプロキシ。
【請求項９】
自ホストのレイヤ２アドレス及び秘密鍵と、ピアホストの公開鍵と、プロキシの公開鍵と、前記ピアホストと通信するためのレイヤ２アドレスとを記憶する記憶部と、
前記プロキシのレイヤ２アドレスと、前記ピアホストのレイヤ２アドレスと、前記ピアホストの署名と、前記プロキシの署名とを含むネイバディスカバリ（ＮＤ）メッセージをリンクで受信するレイヤ２接続と、
前記プロキシの公開鍵を使用して前記プロキシの署名を検証し、
前記プロキシのレイヤ２アドレスを前記ピアホストのレイヤ２アドレスで置き換えることによって前記ＮＤメッセージを修正し、
前記ピアホストの公開鍵を使用して前記ピアホストの署名を検証し、
前記ピアホストと通信するためのレイヤ２アドレスとして、前記プロキシのレイヤ２アドレスを前記記憶部内に記憶する処理部と
を備えるホスト。
【請求項１０】
前記処理部は、さらに、前記ホストの秘密鍵とレイヤ２アドレスとを前記記憶部から読み出し、前記秘密鍵を使用して、前記ホストのレイヤ２アドレスに基づく前記ホストの署名を作成し、前記ホストのレイヤ２アドレスと署名とを含むＮＤ応答を作成し、前記ＮＤ応答を送信するよう前記レイヤ２接続に要求する、
請求項９に記載のホスト。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ディスカバリメッセージについて安全にプロキシを行う方法、プロキシ、およびホストに関する。
【背景技術】
【０００２】
パケット交換コンピュータネットワークにおいて、ホストやルータなどのノードは、ネイバディスカバリ（ＮＤ：neighbor discovery）信号送信を使用して、付されたリンクに存在することがわかっているネイバのリンクレイヤアドレスを決定する。単一のリンクを越えてネットワークを存在させるには、ブリッジを使用して、共通リンクを共有しないサブネットワークを接続するのが一般的である。ＮＤプロキシが、複数のリンクを単一のネットワークにブリッジする方法を提供する。ＮＤプロキシを通過するＮＤ信号送信を修正することで、ＮＤプロキシはブリッジを行う。ＩＥＴＦ（Internet Engineering Task Force：インターネットエンジニアリングタスクフォース）は、「Neighbor Discovery Proxies (ND Proxy)（ネイバディスカバリプロキシ（ＮＤプロキシ））」という題名のＲＦＣ４３８９というＲＦＣ（Request For Comments：リクエストフォーコメンツ）を公開しており、ここには、複数のリンクレイヤセグメントがプロキシを通じて単一のセグメントにブリッジされる方法が記載されている。ＲＦＣ４３８９はＩＣＭＰ（Internet Control Message Protocol：インターネット制御メッセージプロトコル）を規定している。ＩＣＭＰを使用すると、ブリッジの片側のホストが、アドレシング情報を交換して、ＩＰ（Internet Protocol：インターネットプロトコル）アドレスとＭＡＣ（Media Access Control：媒体アクセス制御）アドレスとの間のブリッジングを作成することができる。ＭＡＣアドレスは、リンクレイヤアドレスやレイヤ２アドレスとしても知られている。図１（先行技術）は、ＮＤプロキシ１８０として動作するブリッジを通じて接続

された２つのサブネットワーク１１０および１５０を含んだ単純なネットワーク１００を示している。サブネットワーク１１０は第１リンクレイヤ接続１３０を備えており、第１ホスト１２０などの複数のホストが第１リンクレイヤ接続１３０に接続されている。同様に、サブネットワーク１５０は第２リンクレイヤ接続１７０を備えており、第２ホスト１６０などの複数のホスト第２リンクレイヤ説即１７０に接続されている。ＮＤプロキシ１８０は、第１リンクレイヤ１３０と第２リンクレイヤ１７０とにそれぞれ接続されたポートを備えている。リンクレイヤの１つに対する各接続はＭＡＣアドレスを備えている。ゆえに、第１ホスト１２０は、第１リンクレイヤにＭＡＣアドレスを有しており、第２ホスト１６０は第２リンクレイヤ１７０にＭＡＣアドレスを有しており、ＮＤプロキシ１８０は、各リンクレイヤにそれぞれ１つずつ、２つのＭＡＣアドレスを有している。第１ホスト１２０が最初は第２ホスト１６０のＭＡＣアドレスを知らずに、第２ホスト１６０に接続するためには、第１ホスト１２０は、第１ホスト１２０のＩＰアドレスおよびＭＡＣアドレスと第２ホスト１６０のＩＰアドレスとを含んだネイバソリシテーションメッセージをブロードキャストする。ＮＤプロキシ１８０はこのネイバソリシテーションメッセージを受信し、内部キャッシュに第１ホスト１２０のＭＡＣアドレスを記憶することもできる。ＮＤプロキシ１８０は、メッセージ内の第１ホスト１２０のＭＡＣアドレスを第２リンクレイヤ１７０のＮＤプロキシ１８０のＭＡＣアドレスで置き換えた後、ネイバソリシテーションメッセージを第２リンクレイヤ１７０に転送する。第２ホスト１６０は、第１ホスト１２０のＩＰアドレスを、第２リンクレイヤ１７０のＮＤプロキシ１８０のＭＡＣアドレスと関連させてネイバキャッシュに記憶する。そして、第２ホスト１６０は、第２リンクレイヤ１７０におけるネイバアドバタイズメントメッセージで応答する。ネイバアドバタイズメントメッセージは、第２ホスト１６０のＩＰアドレスおよびＭＡＣアドレスと、任意で第１ホスト１２０のＩＰアドレスおよび第２リンクレイヤ１７０のＮＤプロキシ１８０のＭＡＣアドレスとを含む。ＮＤプロキシ１８０は、第２のホスト１６０のネイバアドバタイズメントメッセージを検出し、第２ホスト１６０のＭＡＣアドレスを、第１リンクレイヤ１３０のＮＤプロキシ１８０自体のＭＡＣアドレスで置き換え、含まれている場合は第２リンクレイヤ１７０のＮＤプロキシ１８０自体のＭＡＣアドレスを第１ホスト１２０のＭＡＣアドレスで置き換え、第１リンクレイヤ１３０のネイバアドバタイズメントメッセージを転送する。第１ホスト１２０は、第２ホスト１６０のＩＰアドレスを、第１リンクレイヤ１１０のＮＤプロキシ１８０のＭＡＣアドレスと関連させてネイバキャッシュに記憶する。後に第１ホスト１２０が第２ホスト１６０のＩＰアドレスを使用して第２ホスト１６０との通信を行う必要があれば、そのネイバキャッシュが、第１リンクレイヤ１３０のＮＤプロキシ１８０のＭＡＣアドレスへメッセージまたはパケットを送信する必要があると示すことになる。同様に、第２ホスト１６０が第１ホスト１２０のＩＰアドレスを使用して第１ホスト１２０との通信を行う必要があれば、第２ホスト１６０のネイバキャッシュが、第２リンクレイヤ１７０のＮＤプロキシ１８０のＭＡＣアドレスへメッセージまたはパケットを送信する必要があると示すことになる。

【０００３】

「SEcure Neighbor Discovery (SEND)（安全なネイバディスカバリ（ＳＥＮＤ））」という題名のＲＦＣ３９７１は、ネイバソリシテーションメッセージやネイバアドバタイズメントメッセージにおけるアドレスに対する悪意のある修正（なりすまし）などの特定の脅威に対してネイバディスカバリ信号送信の安全を確保する方法を規定する。ＳＥＮＤプロトコルは、ＮＤパケットが改ざんされていた場合に受信ノードが検出可能な、ＮＤ信号送信の安全確保法を提供する。デジタル署名を使用して、ネイバディスカバリに関するメッセージを保護する。署名はメッセージの完全性を保護し、メッセージ送信簿との完全性を証明する証明を使用して、その送信元の完全性を認証する。実際、各メッセージは、送信元の秘密鍵と送信元のアドレスとに基づく署名を含んでいる。受信側で、送信元の秘密鍵を使用して、署名を検証することができる。送信元の秘密鍵は、受信側も送信元も認知および信頼しているトラストアンカに対するクエリを使用して、受信側に証明を与える。署名の検証は、送信元のアドレスを確認する。

【０００４】
図２（先行技術）は、ＲＳＡ署名のフォーマットを示している。ＲＳＡ署名２００は、周知のＲＳＡ（Rivest-Shamir-Adleman：リベスト‐シャミール‐エイドルマン）アルゴリズムに基づいており、ＳＥＮＤにおいて規定されている。ＲＳＡ署名２００は、ＮＤ信号送信メッセージに追加される。ビットマーカ２７０が、ＲＳＡ署名２００のフォーマットに関する情報を提供する。ＲＳＡ署名２００に含まれるフィールドは、以下のものを含んでいる。
・タイプ２１０：ＩＥＴＦによって割り当てられ、１２に等しく設定された値
・長さ２２０：８オクテットのユニットにおけるＲＳＡ署名２００の長さ（図２の全パラメータを含む）
・予約２３０：将来使用するために予約されている１６ビットフィールド
・キーハッシュ２４０：ＲＳＡ署名２００の構成に使用する公開鍵のＳＨＡ－１（Secure Hash Standard-1：安全ハッシュ規格－１）ハッシュの最重要（一番左）１２８ビットを含む１２８ビットフィールド
・デジタル署名２５０：送信元の公開鍵を以下のオクテットシーケンスに使用して構成される、ＰＫＣＳ（Public Key Cryptography Standards：公開鍵暗号規格）を含む長さ可変のフィールド
１．ＳＥＮＤプロトコル専用に定まれる１２８ビットＣＧＡメッセージタイプタグ値
２．ＳＥＮＤプロトコルによって保護されているＮＤ信号送信メッセージのＩＰヘッダの１２８ビットソースアドレスフィールド
３．ＩＰヘッダの１２８ビット宛先アドレスフィールド
４．保護されたメッセージのＩＣＭＰ（インターネット制御メッセージプロトコル）ヘッダの８ビットタイプ、８ビットコード、１６ビットチェックサムフィールド
５．ＩＣＭＰチェックサムフィールド後の第１オクテットから始まり、ＮＤプロキシ特定パラメータまで続くがＮＤプロキシ特定パラメータは含まないＮＤプロキシメッセージヘッダ
６．ＲＳＡ署名２００に先行する全ＮＤプロキシ特定パラメータ。具体的には、これらのパラメータはＮＤメッセージを送信するノードのリンクレイヤアドレスを含んでおり、ＮＤメッセージが別のＮＤメッセージに対する応答である場合には、これらのパラメータは、メッセージの宛先であるノードのリンクレイヤアドレスも含んでいる。
・パディング２６０：パディングを含む長さ可変のフィールド

【０００５】
ＲＳＡ署名２００に先行する全メッセージパラメータは、デジタル署名２５０の計算に含まれている。結果として、これらのメッセージパラメータのいくつかを変更しようとする「man in the middle（間にいるもの）」の攻撃は、受信ノードが署名を検証すれば、すぐに検出されるであろう。

【０００６】
ＳＥＮＤおよびＮＤプロキシは、相反する要求に基づいているため、基本的には互換性がない。一方で、今日規定されるように、ＳＥＮＤについては、ＩＰアドレスのアドバタイズメントを行うノードがＩＰアドレスの所有者であり、アドバタイズメントが行われたＩＰアドレスに基づいてデジタル署名を生成するのに使用する秘密鍵を所有していると想定する。他方で、ＮＤプロキシでは、最初にそのＩＰアドレスのアドバタイズメントを行い、そのＩＰアドレスとＭＡＣアドレスに基づいてデジタル署名を作成したノードのＭＡＣアドレスは、ＮＤメッセージ内で、プロキシのＭＡＣアドレスで置き換えられる。アドバタイズメントを行う元のノードのデジタル署名は、ＭＡＣアドレスが上書きされているため、そのＭＡＣアドレスに対して受信側では検証することができない。ＮＤプロキシがあれば、実際には元のＮＤ署名を修正したのは真正プロキシであるのに、悪意のあるノードが元のＮＤ信号送信を改ざんしたかもしれないと、受信側のＳＥＮＤプロトコルが推察するであろう。ＲＦＣ４３８９は、「ＮＤプロキシ」を規定するもので、ＳＥＮＤ ＲＦＣ３９７１の後、２００６年４月に公開されたものであるが、プロキシネイバディスカバ

リ処理の保護に使用可能な機構はないと明確に記述している。プロキシオペレーションはＲＳＡ署名を無効にするものであり、ＮＤメッセージを受信するＳＥＮＤ可能ノードに、そのＮＤメッセージを破棄させたり、あるいはそのＮＤメッセージを安全ではないものとして処理させたりしてしまう。

【発明の概要】

【発明が解決しようとする課題】

【０００７】

方法、プロキシ、ホストを有することで、ブリッジ、プロキシ、またはルータを通じて、ネイバディスカバリメッセージのプロキシを安全に行うことが可能になるという明らかな効果があろう。

【０００８】

したがって、本発明の広い目的は、ホストがプロキシを通じて接続されている場合に、ホスト間のネイバディスカバリ（ＮＤ）信号送信の安全を確保する方法、プロキシ、ホストを提供することである。本発明は、ＮＤプロキシがＮＤメッセージにおけるリンクレイヤアドレスをＮＤプロキシ自体のもので置き換えることができる方法を提供する。このように修正されたアドバタイズメントを受信するノードは、ＮＤプロキシが変更を行うことを許可されているかどうか検証する。この検証について、ノードは、ＮＤプロキシに発行された証明に依存して、このような変更を許可する。ＮＤプロキシングは、プロキシを通過するＮＤメッセージの元のコンテンツを修正し、それによって送信元ホスト署名を壊し、本発明のプロキシは、元のコンテンツを、修正前にそれらを新たなメッセージフィールドに移すことで保存する。プロキシは、プロキシを通過するＮＤメッセージにプロキシ署名を追加する。それにより、修正したＮＤメッセージの正当性を受信ホストが検証することができる。受信ホストは、新たなメッセージフィールドを使用して、ＮＤメッセージの元のコンテンツを再構成し、それによって送信元ホスト署名を修復することができる。

【課題を解決するための手段】

【０００９】

本発明の第１の観点は、プロキシを通じて接続されたホスト間のネイバディスカバリの安全を確保する方法に対するものである。当該方法は、プロキシが、第２ホストを宛先としたネイバディスカバリ（ＮＤ）メッセージを第１ホストから受信すると開始する。ＮＤメッセージは、第１ホストのインターネットプロトコル（ＩＰ）アドレスおよびレイヤ２アドレスと、第１ホストのレイヤ２アドレスに少なくとも部分的に基づいて第１ホストによって構成された第１署名とを含む。プロキシは、まずは第１ホストのレイヤ２アドレスをプロキシのレイヤ２アドレスで上書きして、ＮＤメッセージを修正する。プロキシは、さらに、プロキシの第２署名を挿入することによってＮＤメッセージを修正する。プロキシ署名は、プロキシのレイヤ２アドレスに少なくとも部分的に基づく。そして、プロキシは、修正したＮＤメッセージを第２ホストへ送信する。

【００１０】

本発明の第２の観点は、プロキシを通じて接続されたホスト間のネイバディスカバリの安全を確保する方法の変更例に対するものである。当該方法はいくつかの追加ステップを含む。プロキシは、修正したＮＤメッセージの追加フィールドに第１ホストのレイヤ２アドレスをコピーし、その追加フィールドを使用して、プロキシの第２署名を計算する。第２ホストは、修正したＮＤメッセージを受信すると、プロキシの第２署名を検証する。第２ホストは、さらに、プロキシのレイヤ２アドレスを第１ホストのレイヤ２アドレスで上書きすることによって、ＮＤメッセージをその元の形態に戻す。ゆえに、第２ホストは、第１ホストの第１署名を検証することができる。第２ホストは、第１ホストのＩＰアドレスを、プロキシのレイヤ２アドレスと関連させて記憶する。

【００１１】

本発明の第３の観点は、ホストにおいてネイバディスカバリ（ＮＤ）メッセージを安全に受信する方法に対するものである。当該方法は、プロキシのレイヤ２アドレスと、ピアホストのレイヤ２アドレスと、ピアホストの署名と、プロキシの署名とを含むＮＤメッセ

ージをホストが受信すると開始する。ホストはプロキシの公開鍵を使用して、プロキシの署名を検証する。そしてホストは、プロキシのレイヤ２アドレスをピアホストのレイヤ２アドレスで置き換えることによって、ＮＤメッセージを修正する。これにより、ホストは、ピアホストの公開鍵を使用して、ピアホストの署名を検証することが可能となる。２つの署名の検証に続いて、ホストは、ピアホストと通信するためのレイヤ２アドレスとしてプロキシのレイヤ２アドレスを記憶する。

【００１２】

本発明の第４の観点は、プロキシに対するものである。当該プロキシは、第１ホストからネイバディスカバリ（ＮＤ）メッセージを受信するのに使用する第１レイヤ２接続を有する。また、当該プロキシは処理部も有する。処理部は、第１レイヤ２接続からＮＤメッセージを受信し、少なくとも１つの元のアドレスを含む第１フィールドと、第１ホストの第１署名を含む第２フィールドとをＮＤメッセージから読み出す。そして、処理部は、受信したＮＤメッセージから少なくとも１つの元のアドレスを第３フィールドへコピーすることで、ＮＤメッセージを修正する。次に処理部は、第１フィールドにおいて少なくとも１つの元のアドレスのうちの１つをプロキシのアドレスで上書きする。処理部は、プロキシのアドレスと、少なくとも１つの元のアドレスとに基づくプロキシの第２署名を挿入する。そして処理部は、第２レイヤ２接続に命令し、修正したＮＤメッセージを第２ホストへ送信させる。

【００１３】

本発明の第５の観点は、ホストに対するものである。当該ホストは、ピアホストの公開鍵と、プロキシの公開鍵と、ピアホストと通信するためのレイヤ２アドレスとを記憶する記憶部を備える。当該ホストは、プロキシからネイバディスカバリ（ＮＤ）メッセージをリンクで受信するレイヤ２接続を有する。ＮＤメッセージは、プロキシのレイヤ２アドレスと、ピアホストのレイヤ２アドレスと、ピアホストの署名と、プロキシの署名とを含む。当該ホストにおいて、処理部が、プロキシの公開鍵を使用してプロキシ署名を検証する。そして処理部は、プロキシのレイヤ２アドレスをピアホストのレイヤ２アドレスで置き換えることによってＮＤメッセージを修正する。処理部は、さらに、ピアホストの公開鍵を使用してピアホストの署名を検証する。それらの検証に続いて、処理部は、ピアホストと通信するためのレイヤ２アドレスとして、プロキシのレイヤ２アドレスを記憶する。

【図面の簡単な説明】

【００１４】

本発明、その目的および効果についてより詳細に理解するために、添付図面と併せて、以下の説明を参照可能である。

【図１】図１は、ネイバディスカバリプロキシとして動作するネイバディスカバリプロキシを通じて接続された２つのサブネットワークを含んだ単純なネットワークの先行技術を表す。

【図２】図２は、リベスト‐シャミール‐エイドルマン署名のフォーマットの先行技術を表す。

【図３】図３は、安全ネイバディスカバリプロキシを通じて接続された２つのサブネットワークを含んだネットワーク例を示す。

【図４】図４ａ、４ｂ、４ｃは、本発明の方法のステップ例を表したシーケンス図を示す。

【図５】図５は、本発明のいくつかの観点によってプロキシ署名を計算する方法例を示す。

【図６】図６は、本発明のいくつかの観点によって単純化したネイバディスカバリメッセージコンテンツを示す。

【図７】図７は、本発明の一観点によって構成されたプロキシ例を示す。

【図８】図８は、本発明の一観点によって構成されたホスト例を示す。

【発明を実施するための形態】

【００１５】

好ましい実施形態の様々な使用例や観点を特に参照しながら、本発明の革新的開示を記載する。しかしながら、この実施形態は、本発明の革新的開示の多くの効果的用途のうちのいくつかの例だけを提供するものであるということを理解すべきである。一般に、本願明細書における記載は、必ずしも、本発明で請求する様々な観点のうちのいずれかを限定するものではない。また、ある進歩的特徴に適用可能だが、他の特徴には適用不可能である記載もある。図面の記載において、同様の番号は、本発明の同様の構成を表している。

【００１６】

本発明によれば、アドレス所有およびアドレスアドバタイズメントの役割は、明らかに別々のものである。標準ネイバディスカバリ（ＮＤ）プロキシの通常オペレーションは、ＩＥＴＦ（インターネットエンジニアリングタスクフォース）のＲＦＣ（リクエストフォーコメンツ）第４３８９号において定義されている。本発明では、元のＮＤメッセージを修正する許可ＳＥＮＤプロキシと、同じことをする悪意のあるノードとを受信ノードが区別できることを確証する特徴をさらに備えたＳＥＮＤ（安全なネイバディスカバリ）プロキシが提供される。これについては、許可ＳＥＮＤプロキシの鍵で署名してＮＤメッセージを修正することによって達成される。許可ＳＥＮＤプロキシは、署名および修正が行われたＮＤメッセージに、それが置き換えたＮＤメッセージの元のコンテンツも含むことが好ましい。これは、受信ノードがさらなる検証に使用することができる。ＳＥＮＤプロキシの署名は、プロキシ署名情報（ＰＳＩ：proxy signature information）という新たな情報フィールドに含めるものとすることができる。署名は、元のＮＤメッセージのＲＳＡ（リバスト‐シャミール‐エイドルマン）署名フィールドを含んだ、メッセージに存在するＮＤプロキシ情報フィールドに行われる。ＰＳＩは、好ましくは最後の情報フィールドとして、メッセージに追加される。プロキシ署名は、以下の点を除いて、図２に示したＲＳＡ署名と同様のフォーマットを有する。第１に、プロキシ署名は、図２のタイプ２１０の値とは異なる別個のタイプ値を有する。第２に、デジタル署名はＰＳＩに先行する全ＮＤプロキシ特定パラメータに基づくのが好ましいため、ＰＳＩ内のデジタル署名は、ＲＳＡ署名自体の一部に基づくのが好ましい。

【００１７】

また、Ｄプロキシを使用して、安全にＮＤメッセージのプロキシを行うことを可能にする方法と、ＰＳＩ可能なホストとが提供される。

【００１８】

本発明において、ＮＤプロキシは、ブリッジと、ルータと、スイッチと、その他いかなるパケット転送装置を含むものとしてもよい。ＳＥＮＤプロキシは、同様の物理および／またはリンクレイヤプロパティを有するサブネットワークに接続しても、同様ではない物理および／またはリンクレイヤプロパティを有するサブネットワークに接続してもよい。ある例では、ＳＥＮＤプロキシは、２つの別個のイーサネット（登録商標）サブネットワークを接続するものとすることができる。別の例では、ＳＥＮＤプロキシはＷＬＡＮ（wireless location area network：無線ロケーションエリアネットワーク）とセルラ無線ネットワークとの間をブリッジするものとすることができる。ホストは、いかなる端末、エンドユーザ装置、ルータ、アプリケーションサーバなどを含むものとしてもよい。ホストは、１または２以上の物理接続と、関連リンクレイヤアドレスおよびリンクレイヤプロパティとを含んだものとすることができる。例えば、パーソナルコンピュータを、イーサネット（登録商標）接続とＷＬＡＮ接続とを備えたものとして、そのどちらかを本発明に関して使用するものとすることが可能である。また、ホストは、Ｂｌｕｅｔｏｏｔｈ™もセルラ接続も使用する移動端末を含んだものとしてもよい。

【００１９】

本発明の記載において、「レイヤ２（layer 2）」、「リンクレイヤ」、「ＭＡＣ（媒体アクセス制御）」という用語を使用した場合、互いに置き換えることができる。

【００２０】

ここで図面を参照する。図３は、ＳＥＮＤプロキシ３８０を通じて接続された２つのサブネットワーク３１０および３５０を含んだネットワーク例３００を示している。ネット

ワーク３００は、本発明のある開示として構成されたノードを備える。２つのネットワーク３１０および３５０の各々はホストをサポートするものであり、第１ホスト３２０、第２ホスト３６０をそれぞれサポートする。いうまでもなく、サブネットワーク３１０および３５０はもっと多くのホストをサポートすることも可能であり、ＳＥＮＤプロキシ３８０は複数のサブネットに相互接続を提供することも可能である。図３は、本発明の説明を簡単にするために単純化してある。第１ホスト３２０は、ＭＡＣ（媒体アクセス制御）アドレスＭＡＣ＿Ｈ１を有するポートを介して、サブネットワーク３１０に接続されている。同様に、第２ホスト３２０は、ＭＡＣアドレスＭＡＣ＿Ｈ２を介して、サブネットワーク３５０に接続されている。ＳＥＮＤプロキシ３８０は、両サブネットワークに対する接続を有するため、サブネットワーク３１０および３５０にそれぞれ接続する２つのＭＡＣアドレスＭＡＣ＿Ｐ１およびＭＡＣ＿Ｐ２を有している。第１ホスト３１０、第２ホスト３６０、ＳＥＮＤプロキシ３８０の間のやり取りは、以下の図に関連して説明する。

【００２１】

図４ａ、４ｂ、４ｃは、本発明の方法のステップ例を表したシーケンス図を示している。図３に関連して導入した第１ホスト３２０と、第２ホスト３６０と、ＳＥＮＤプロキシ３８０と、トラストアンカ４００とが図４ａ、４ｂ、４ｃのシーケンスに関与する。トラストアンカ４００を図３のネットワークに追加することにより、信頼のあるインフラストラクチャの中にホスト３２０および３６０とＳＥＮＤプロキシとを含めることができる。

【００２２】

この方法はステップ４０３から任意に開始するものとすることが可能であり、ここで、第１ホスト３２０は、ＳＥＮＤプロキシ３８０を通じて他のホストと通信する必要があることを知っており、トラストアンカ４００から、ＳＥＮＤプロキシ３８０のセキュリティ証明を要求することができる。そうした場合には、トラストアンカ４００は、ステップ４０６において、ＳＥＮＤプロキシ３８０の公開鍵を含んだＳＥＮＤプロキシ３８０の証明で応答する。同様に、第２ホスト３６０も、ステップ４０９において、トラストアンカ４００からＳＥＮＤプロキシ３８０の証明を任意で要求することができる。そうした場合、ステップ４１２においてトラストアンカはＳＥＮＤプロキシ３８０のセキュリティ証明で応答する。言うまでもなく、第１ホストおよび第２ホストは、時間を延長して、トラストアンカ４００のセキュリティ証明のそれぞれの写しを記憶しておくことが可能である。したがって、ステップ４０３～４１２については、図４ａ、４ｂ、４ｃのシーケンスを実行する度に繰り返す必要はない。

【００２３】

ステップ４１５において、第１ホスト３２０は、第２ホスト３６０との通信を始めることを所望する。第１ホストと第２ホストとが以前に通信していた場合であっても、例えば第２ホスト３６０がそのレイヤ２接続を修正していることもあるため、以下で説明するＮＤ手続を再度行うのが好ましいという状況もあろう。第２ホスト３６０がそのレイヤ２接続を修正する例の１つとしては、イーサネット（登録商標）接続が使用されておらず、ＷＬＡＮ接続が第２ホスト３６０のトラフィックを支配しているという場合があろう。第１ホストおよび第２ホストが別個のサブネットワークに位置しているため、単純なＮＤ手続が使用不可能で、２つのサブネットワークを接続するブリッジをディスカバリ信号送信が通過する必要があり、ＳＥＮＤプロキシ３８０がブリッジ機能を提供する。ステップ４１８において、第１ホスト３２０はＲＳＡ署名を構成する。ＲＳＡ署名は従来のものとして、例えば図２のＲＳＡ署名フォーマット２００にしたがって構成することができる。ＲＳＡ署名は、少なくとも第１ホスト３２０のＭＡＣアドレスＭＡＣ＿Ｈ１であるＳＬＬＡ（source link layer address：ソースリンクレイヤアドレス）を含む様々なパラメータにしたがって構成することができる。ステップ４２１において、第１ホスト３２０が、アドレスＭＡＣ＿Ｈ１を有するポートを使用して、サブネットワーク３１０のリンクのネイバソリシテーションメッセージを送信する。サブネットワーク３１０の同一リンクに接続されたＳＥＮＤプロキシ３８０が、ＳＥＮＤプロキシ３８０自体のＭＡＣアドレスＭＡＣ＿Ｐ１を介してネイバソリシテーションメッセージを検出する。ステップ４２４において

、ＳＥＮＤプロキシ３８０は、修正したネイバソリシテーションを第２ホスト３６０へ転送するのに使用するプロキシ署名を構成する。プロキシ署名は、上述のＰＳＩフォーマットにしたがって、修正したネイバソリシテーションに追加される。

【００２４】

図４ａのステップ４２４におけるプロキシ署名の構成法の詳細を図５に示す。図５は、本発明のいくつかの観点によってプロキシ署名を計算する方法例を示している。図５の方法は、さらに図６に関連して説明する。図６は、本発明のいくつかの観点による単純化したネイバディスカバリメッセージコンテンツを示す。図６を参照すると、ＮＤメッセージ６００が、元のアドレスフィールド６１０と、ＮＤメッセージを発したホスト（ソースホスト）のＲＳＡ署名６２０を含んでいる。元のアドレスフィールド６１０は、ソースホストのＭＡＣアドレス６１２と、ソースＩＰ６１４ともいうソースホストのＩＰアドレスと、宛先ＩＰ６１６ともいうＮＤメッセージの宛先であるホストの宛先アドレスとをさらに含む。図６に示す他のフィールドは、以下で参照する補足アドレスフィールド６３０とプロキシ署名６４０とを含む。図５の方法はステップ５００から開始し、例えば図４ａのステップ４２１のネイバソリシテーションメッセージなどのＮＤメッセージをＳＥＮＤプロキシ３８０が受信する。ステップ５１０において、ＳＥＮＤプロキシ３８０はＮＤメッセージからソースＭＡＣアドレス６１２を読み出す。ソースＭＡＣアドレス６１２は、補足アドレスフィールド６３０に任意でコピーされ、ステップ５２０においてＮＤメッセージ６００が修正される。するとステップ５３０において、ＳＥＮＤプロキシ３８０が、ＳＥＮＤプロキシ３８０自体のＭＡＣアドレスを元のアドレスフィールド６１０に書き込むことで、ＮＤメッセージをさらに修正し、ソースＭＡＣ６１２を上書きする。ＳＥＮＤプロキシ３８０自体のＭＡＣアドレスは、例えば、図３に示すように、第２ホスト３６０と同一のサブネットワークのＳＥＮＤプロキシ３８０のレイヤ２アドレスであるＭＡＣ＿Ｐ２とすることが可能である。ステップ５４０において、ＳＥＮＤプロキシ３８０はプロキシ署名６４０を計算し、修正したＮＤメッセージに追加する。この署名は、ＳＥＮＤプロキシ３８０のＲＳＡ署名であることが好ましく、ＰＳＩフォーマットにしたがって構成されたものであることが好ましい。プロキシ署名６４０は、ステップ５３０で修正された元のアドレスフィールド６１０を含んだＮＤメッセージの全部の情報フィールドと、ソースホストのＲＳＡ署名６２０とに基づいていることが好ましい。署名は、補足アドレスフィールド６３０にも基づいていることが好ましい。言うまでもなく、プロキシ署名６４０は、他のパラメータにも基づいたものとすることも可能である。

【００２５】

図４ａ、４ｂ、４ｃのシーケンスに戻ると、ステップ４２４においてＳＥＮＤプロキシ３８０がプロキシ署名６４０を構成した後、ＳＥＮＤプロキシ３８０は、ステップ４２７において、第２サブネットワーク３５０のリンクレイヤに、アドレスＭＡＣ＿Ｐ２を有するそのポートを使用してメッセージを置くことによって、修正したネイバソリシテーションメッセージを第２ホスト３６０へ転送する。サブネットワーク３５０の同一リンクに接続された第２ホストは、ＭＡＣアドレスＭＡＣ＿Ｈ２を有する第２ホスト自体のポートを介して、修正したネイバソリシテーションメッセージを受信する。この時点で、第２ホスト３６０は、任意のステップ４０９および４１２において、ＳＥＮＤプロキシ３８０の証明を事前に取得しておくことも可能である。修正したネイバソリシテーションの受信に従事する第２ホスト３６０に証明が存在していない場合、第２ホスト３６０は、ステップ４３０および４３３において証明を取得する。そしてステップ４３６において、第２ホスト３６０は、ＳＥＮＤプロキシ３８０の証明に含まれたＳＥＮＤプロキシ３８０の公開鍵を使用して、ＳＥＮＤプロキシ３８０のＲＳＡ署名を検証する。この検証により、修正したネイバソリシテーションが真正ノードによって送信されたものであると、第２ホスト３６０が確かめることができる。ＳＥＮＤプロキシ３８０が、第２ホスト３６０が認知する信頼のあるインフラストラクチャの一部である場合、ステップ４３６のＳＥＮＤプロキシＲＳＡ署名の検証は、修正したネイバソリシテーションのコンテンツ全体が有効であると第２ホスト３６０が考慮するのに十分である。そして処理は直接ステップ４４５へ続くもの

とすることができる。しかしながら、第２ホスト３６０が全体的にＳＥＮＤプロキシ３８０を信頼しない場合は、ネイバソリシテーションはまた真正ノードによってもともと開始されたと検証することができる。このため、第２ホスト３６０がステップ４３９および４４２を実行することができる。ステップ４３９において、第２ホスト３６０は、今は元のアドレスフィールド６１０に存在するＳＥＮＤプロキシ３８０のＭＡＣアドレスを、補足アドレスフィールド６３０にある値で上書きすることによって、元のネイバソリシテーションメッセージを再構成する。例えば、値ＭＡＣ＿Ｈ１を補足フィールド６３０から読み出し、元のアドレスフィールドへソースＭＡＣ６１２として戻すことができる。ステップ４４２において、第１ホスト３２０のＲＳＡ署名６２０が検証される。ネイバソリシテーションの元のソースＭＡＣアドレス６１２がメッセージにおけるその元の場所に戻されているため、この検証が可能となる。

【００２６】

ステップ４４５において、ＳＥＮＤプロキシＲＳＡ署名によって、または第１ホスト３２０のＲＳＡ署名を検証することによって、修正したネイバソリシテーションで第２ホスト３６０が満足すると想定すると、第２ホスト３６０は、例えばＭＡＣ＿Ｐ２などのプロキシのＭＡＣアドレスを、第１ホスト３２０のＩＰアドレスと関連させてネイバキャッシュに記憶する。第２ホスト３６０は、後にこのアドレスペアを使用して、第１ホスト３２０と通信するであろう。第２ホスト３６０が以前に第１ホスト３２０のキャッシュエントリを有している場合は、ステップ４４５が、キャッシュエントリに対する更新からなる。そして第２ホスト３６０はステップ４４８においてＲＳＡ署名を構成する。ステップ４１８の場合のように、このＲＳＡ署名は従来のものとし、図２のＲＳＡ署名フォーマット２００にしたがって構成されるものとすることができる。ＲＳＡ署名は、第２ホスト３６０のＭＡＣアドレスＭＡＣ＿Ｈ２である第２ホスト３６０のＴＬＬＡ（target link layer address：ターゲットリンクレイヤアドレス）に少なくとも部分的に基づいて構成されるものとすることができる。ステップ４５１において、第２ホスト３６０は、アドレスＭＡＣ＿Ｈ２を有するポートを使用して、サブネットワーク３２０のリンクのネイバアドバタイズメントメッセージ送信を行う。サブネットワーク３２０の同一リンクに接続されたＳＥＮＤプロキシ３８０は、ＳＥＮＤプロキシ３８０自体のＭＡＣアドレスＭＡＣ＿Ｐ２を介して、ネイバアドバタイズメントメッセージを検出する。ステップ４５４において、ＳＥＮＤプロキシ３８０は、修正したネイバアドバタイズメントを第１ホスト３２０を転送するのに使用する別のプロキシ署名６４０を構成する。図５に記載の方法を再度使用して、プロキシ署名６４０を構成する。ステップ４５４から、例えばＴＬＬＡ　ＭＡＣ＿Ｈ２など、ソースＭＡＣ６１２として元のネイバアドバタイズメントに含まれた第２ホスト３６０の元のＭＡＣアドレスは、修正したネイバアドバタイズメントにおける補足フィールド６３０へ移動され、ＳＥＮＤプロキシ３８０自体のＭＡＣアドレスがネイバアドバタイズメントのソースＭＡＣ６１２を上書きする。ＳＥＮＤプロキシ３８０自体のＭＡＣアドレスは、例えば、図３に示すように、第１ホスト３２０と同一のサブネットワークのＳＥＮＤプロキシ３８０のレイヤ２アドレスであるＭＡＣ＿Ｐ１とすることができる。また、プロキシ署名６４０も、２つのアドレスフィールド６１０および６３０の現在のコンテンツに基づいて追加される。修正したネイバソリシテーションの場合のように、修正したネイバアドバタイズメントは、好ましくはＰＳＩフォーマットにしたがったプロキシ署名６４０を含む。

【００２７】

ステップ４５４においてＳＥＮＤプロキシ３８０がプロキシ署名６４０を構成した後、ＳＥＮＤプロキシ３８０は、ステップ４５７において、アドレスＭＡＣ＿Ｐ１を有するそのポートを使用して第１サブネットワーク３１０のリンクレイヤにメッセージを置くことによって、修正したネイバアドバタイズメントメッセージを第１ホスト３２０へ転送する。サブネットワーク３１０の同一リンクに接続された第１ホスト３２０は、第１ホスト３２０自体のＭＡＣアドレスＭＡＣ＿Ｈ１を介して、修正したネイバアドバタイズメントメッセージを検出する。この時点で、第１ホスト３２０は、任意のステップ４０３および４

０６において、ＳＥＮＤプロキシ３８０の証明を事前に取得しておくことも可能である。修正したネイバアドバタイズメントの受信に従事する第１ホスト３２０に証明が存在していない場合、第１ホスト３２０は、ステップ４６０および４６３において証明を取得する。そしてステップ４６６において、第１ホスト３２０は、証明に含まれたＳＥＮＤプロキシ３８０の公開鍵を使用して、ＳＥＮＤプロキシ３８０のＲＳＡ署名を検証する。この検証により、修正したネイバソリシテーションが真正ノードによって送信されたものであると、第１ホスト３２０が確かめることができる。任意で、第１ホスト３２０は、ネイバアドバタイズメントもまた真正ノードによってもともと開始されたと検証することができる。このため、第１ホスト３２０がステップ４６９および４７２を実行することができる。ステップ４６９において、第１ホスト３２０は、ソースＭＡＣ６１２を、例えば値ＭＡＣ＿Ｈ２などの補足アドレスフィールド６３０にある値で上書きすることによって、元のネイバアドバタイズメントメッセージを再構成する。ステップ４７２において、第２ホスト３６０のＲＳＡ署名６２０が検証される。ネイバアドバタイズメントの元のソースＭＡＣアドレス６１２がメッセージにおけるその元の場所に戻されているため、この検証が可能となる。ステップ４７５において、第１ホスト３２０は、例えばＭＡＣ＿Ｐ１などのプロキシのＭＡＣアドレスを、第２ホスト３６０のＩＰアドレスに関連させてネイバキャッシュに記憶または更新する。

【００２８】

ここで、本発明の一観点によって構成されたプロキシ例を示した図７を参照しながら、プロキシの構成例を説明する。プロキシ７００は、処理部７１０と、少なくとも２つの接続７２０および７３０とを備える。プロキシ７００は、記憶部（図示せず）を備えたものとしてもよいが、本発明の目的としては、プロキシ７００のオペレーションは記憶部がなくてもよい。本発明のプロキシ７００は、ネットワーキング装置の分野において周知の通常のプロキシ、ブリッジ、スイッチに見られる多くの構成をさらに備えたものとすることも可能である。これらの追加構成は、図示を簡潔なものとするため、ここでは図示していない。

【００２９】

処理部７１０は、例えば、いかなる市販のプログラム可能プロセッサを備えたものとすることも可能である。レイヤ２接続７２０および７３０の各々は、信号、メッセージ、データの受信（入力）および送信（出力）を行う１つの単一装置として実施することもできるし、個別の装置として実施することもできる。プロキシ７００は、複数のホストへ接続される。プロキシ７００をホストへ接続する手段は様々なものがある。例えば、あるホストへの通信を提供するあるレイヤ２接続がイーサネット（登録商標）リンクにあれば、他のリンク２接続の別のホストへの接続はＡＴＭ（asynchronous transfer mode：非同期転送モード）リンクにあるものとすることができる。したがって、プロキシ７００は、様々な種類の複数のリンクを接続する複数の装置を備えたものとすることが可能である。本発明を簡潔に表現するため、２つのレイヤ２接続しか図示していない。

【００３０】

オペレーション中、プロキシ７００は、例えばＭＡＣアドレスＭＡＣ＿Ｐ１のレイヤ２接続７２０などの第１レイヤ２接続において、ＮＤメッセージを第１ホストから受信する。ＮＤメッセージは、ＮＤソリシテーションであることもあれば、ＮＤアドバタイズメントであることもある。レイヤ２接続７２０が処理部７１０に通知する。処理部７１０は、第１ホストの元のＭＡＣアドレスを含んだ第１フィールドと、第１ホストの第１署名を含んだ第２フィールドとをＮＤメッセージからまずは読み出すことによってＮＤメッセージを修正する。処理部７１０は、修正したＮＤメッセージに追加される第３フィールドへ第１ホストのＭＡＣアドレスをコピーする。そして、処理部７１０は、ＭＡＣ＿Ｐ２である他のレイヤ２接続７３０のＭＡＣアドレスで第１ホストのＭＡＣアドレスを第１フィールドに上書きする。処理部７１０は、最終的に、第３フィールドの第１署名において、その現在値における第１フィールドに基づいて、修正したＮＤメッセージにプロキシ７００の第２署名を挿入する。そして処理部７１０は、修正したＮＤメッセージを第２ホストへ第

２リンクで送信するよう、第２レイヤ２接続７３０に要求する。

【００３１】

図８は、本発明の一観点によって構成されたホスト例を示している。ホスト８００は、レイヤ２接続８２０と、処理部８１０と、記憶部８４０とを備える。ホスト８００は、様々な個別の装置を表したものとすることができるため、ディスプレイ、キーボード、マウス、複数の追加プロセッサ、その他多くの構成要素（図示せず）をさらに備えたものとすることができる。処理部８１０は、ＮＤ信号送信専用とすることもできるし、ホスト８００のその他のタスクもサポートするものとすることもできる。記憶部８４０は、電気的な消去およびプログラムが可能な、例えばフラッシュメモリやデータ格納モジュールとして実施することができる不揮発性メモリまたは持続性メモリである。レイヤ２接続８２０は、信号、メッセージ、データの受信（入力）および送信（出力）を行う１つの単一装置として実施することも、複数の個別の装置として実施することも可能である。ホスト８００は、１つよりも多くのレイヤ２接続を備えたものとすることも可能である。したがって、図８は図示を簡潔にするために単純化してある。

【００３２】

記憶部８４０は、ホスト８００自体に関する情報８４５を永久的または準永久的に記憶する。これには、例えば、レイヤ２接続８２０のレイヤ２アドレスＭＡＣ＿Ｈｎ、ホスト８００に割り当てられたＩＰアドレス、ＲＳＡ署名の計算に使用するホスト８００の秘密鍵および公開鍵などが含まれる。当技術分野においては周知のように、ホスト８００に割り当てられたＩＰアドレスは永久的なものとすることもできれば、ホスト８００が現在接続されているネットワークによって割り当てられるものとすることもできる。記憶部４００は、プロキシやルータやその他のホストなど、他のノードのＩＰアドレス、リンクレイヤアドレス、公開鍵もテーブル８４７に記憶することができる。記憶部４００は、当技術分野において周知の他のデータをさらに記憶することも可能である。

【００３３】

動作中、ホスト８００は、別のホストとの通信を開始する必要がある場合、そのホストとの通信で使用するリンクレイヤアドレスを取得する必要がある。ホスト８００は、ルートルックアップなどの周知手段によって、そのホストのＩＰアドレスを最初に取得しておくこともできる。他のホストへ導く当該リンクレイヤアドレス取得するためには、ホスト８００は、そのレイヤ２接続８２０でＮＤソリシテーションを送信する必要がある。ＮＤソリシテーションはＭＡＣ＿ＨｎアドレスをＭＡＣ＿Ｈｎアドレスは、今度はこの取引においてＳＬＬＡ（ソースリンクレイヤアドレス）になる。処理部８１０が、ＳＳＬＡと、このホスト８００のＩＰアドレスと、他のホストのＩＰアドレスと、ホスト８００の秘密鍵とを記憶部８４０から読み出す。処理部は、これらのパラメータおよび他のパラメータに基づいてＲＳＡ署名を構成し、レイヤ２接続８２０に対して、ＮＤソリシテーションを、それが付されるレイヤ２リンクに置くよう命令する。

【００３４】

レイヤ２接続８２０はＮＤソリシテーションメッセージを受信することができる。レイヤ２接続８２０は、このＮＤソリシテーションとそのコンテンツとを処理部８１０へ転送する。ＮＤソリシテーションがＰＳＩを含んでいる場合は、送信元ホストが発したＮＤソリシテーションはプロキシによって修正されており、ＮＤソリシテーションに含まれたリンクレイヤアドレスはプロキシのＭＡＣアドレスであり、送信元ホストの元のアドレスではないという表示として、処理部８１０がＰＳＩを検出する。処理部８１０はテーブル８４７からプロキシの公開鍵を読み出す。見つかった場合は、プロキシの公開鍵を使用して、ＰＳＩに含まれたプロキシ署名を検証する。この検証が失敗した場合、ＮＤソリシテーションは単純に破棄される。そうでない場合は、処理部８１０が、ＮＳソリシテーションを発したホストのＳＬＬＡをＰＳＩから読み出すことが好ましいことがある。ＮＤソリシテーション内でプロキシのＭＡＣアドレスを送信元ホストのＳＬＬＡで上書きすることによって、処理部８１０は、送信元ホストのＲＳＡ署名を検証することができる。ＲＳＡ署名の検証には、処理部８１０が送信元ホストの公開鍵をテーブル８４７から読み出すこと

が必要である。ＲＳＡ署名が有効であると仮定すると、処理部８１０は、プロキシのＭＡＣアドレスと、送信元ホストのＩＰアドレスとをテーブル８４７に記憶して、テーブル８４７内に送信元ホストのキャッシュエントリを作成する。そして処理部は、ホスト８００自体のレイヤ２アドレスＭＡＣ＿Ｈｎを記憶部８４０から読み出し、ＴＬＬＡ（ターゲットリンクレイヤアドレス）フィールド内において、ＮＤアドバタイズメントメッセージに配置する。プロキシのＭＡＣアドレス、ホスト８００のＩＰアドレス、その他のパラメータも、ＮＤアドバタイズメントに配置される。処理部８１０はＲＳＡ署名を計算し、ＮＤアドバタイズメントに挿入する。そして処理部８１０は、レイヤ２リンクにＮＤアドバタイズメントを配置するようレイヤ２接続８２０に要求する。

【００３５】

レイヤ２接続８２０はＮＤアドバタイズメントを受信することができる。レイヤ２接続８２０は、このＮＤアドバタイズメントとそのコンテンツとを処理部８１０へ転送する。ＮＤアドバタイズメントがＰＳＩを含んでいる場合は、応答ホストが発したＮＤアドバタイズメントはプロキシによって修正されており、ＮＤアドバタイズメントに含まれたＭＡＣアドレスまたはリンクレイヤアドレスはプロキシのアドレスであり、応答ホストの元のＴＬＬＡではないという表示として、処理部８１０がＰＳＩを検出する。処理部８１０はテーブル８４７からプロキシの公開鍵を読み出す。見つかった場合は、プロキシの公開鍵を使用して、ＰＳＩに含まれたプロキシ署名を検証する。この検証が失敗した場合、ＮＤアドバタイズメントは単純に破棄される。そうでない場合は、処理部８１０が、ＮＳアドバタイズメントを発したホストのＴＬＬＡをＰＳＩから読み出すことが好ましいことがある。プロキシのＭＡＣアドレスを応答ホストのＴＬＬＡで上書きすることによって、処理部８１０は、応答ホストのＲＳＡ署名を検証することができる。ＲＳＡ署名の検証には、処理部８１０が応答ホストの公開鍵を記憶部８４０から読み出すことが必要である。ＲＳＡ署名が有効であると仮定すると、処理部８１０は、プロキシのＭＡＣアドレスと、応答ホストのＩＰアドレスとを記憶部８４０に記憶する。

【００３６】

本発明の方法およびプロキシの好ましい実施形態のいくつかを添付図面に示し、上述の発明を実施するための形態において説明したが、本発明は、開示した実施形態に限定されるものではなく、添付の特許請求の範囲において掲載および限定がなされた本発明の本異質から逸脱せずに、多くの再構成、修正、代替が可能である、ということが理解されよう。

【図１】

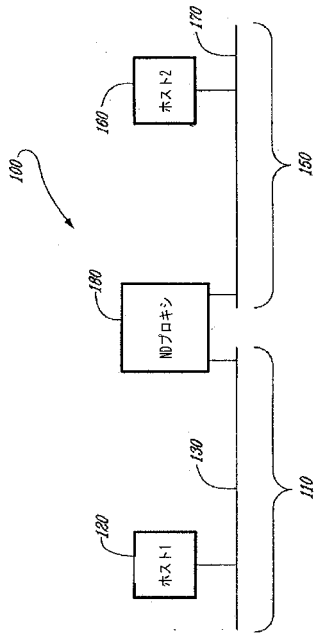

Fig. 1 (PRIOR ART)

【図２】

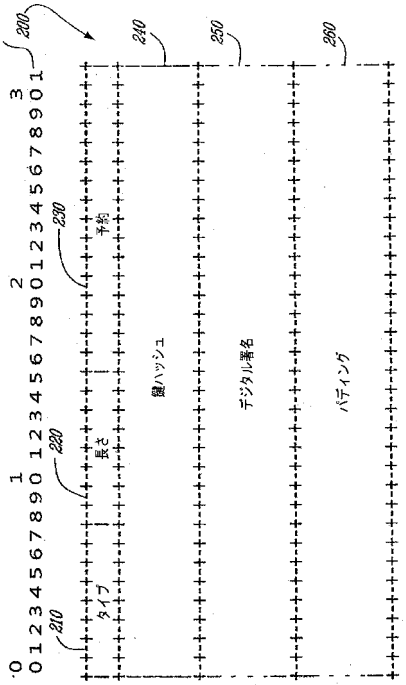

Fig. 2 (PRIOR ART)

【図３】

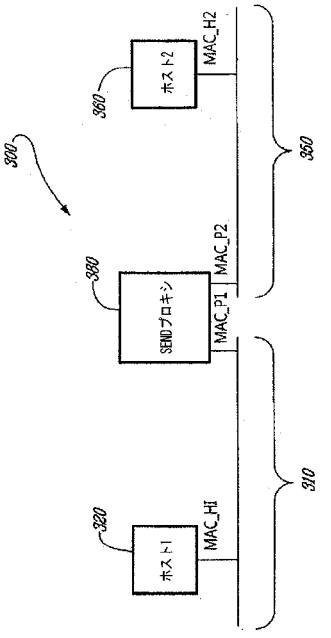

Fig. 3

【図４ａ】

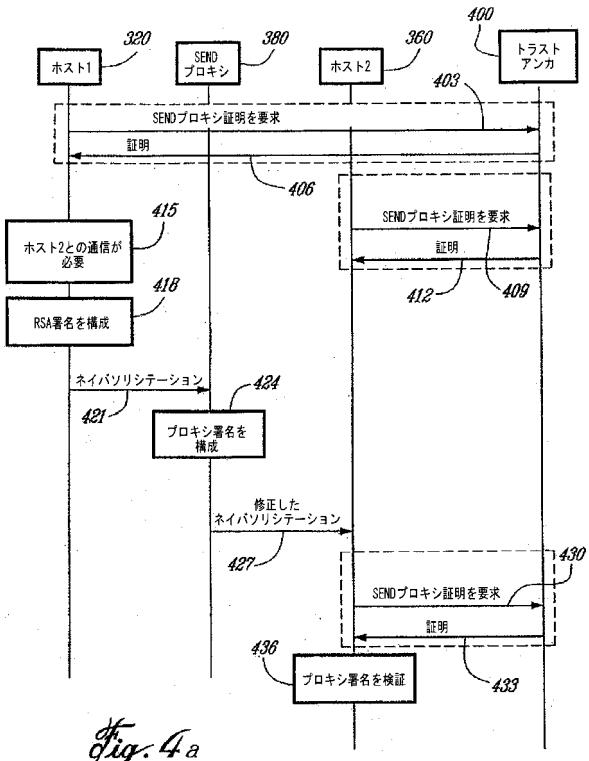

Fig. 4a

【図４ｂ】

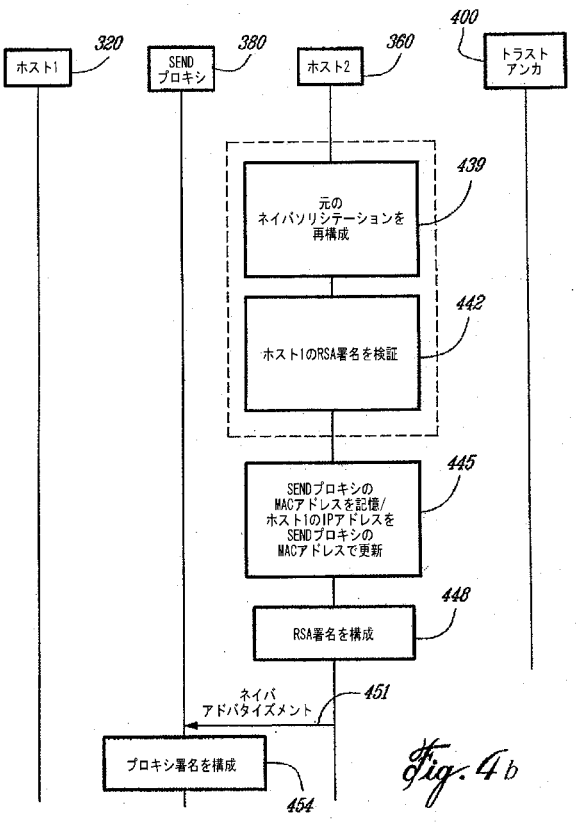

Fig. 4b

【図４ｃ】

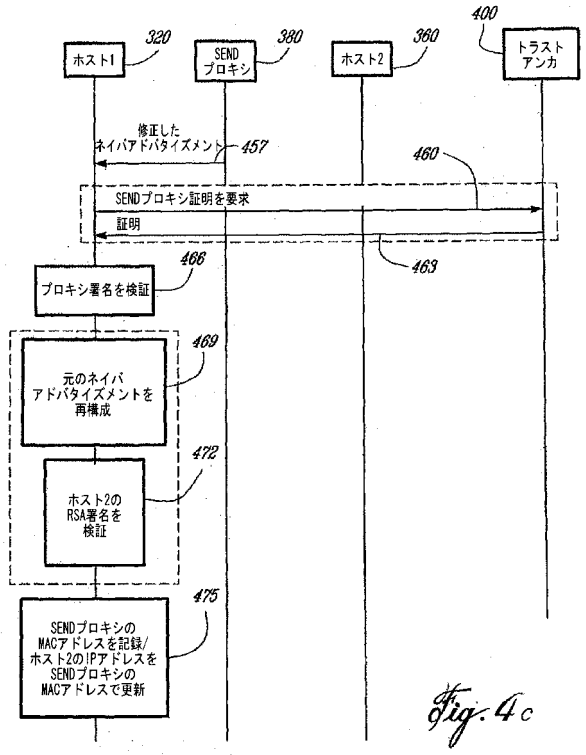

Fig. 4c

【図５】

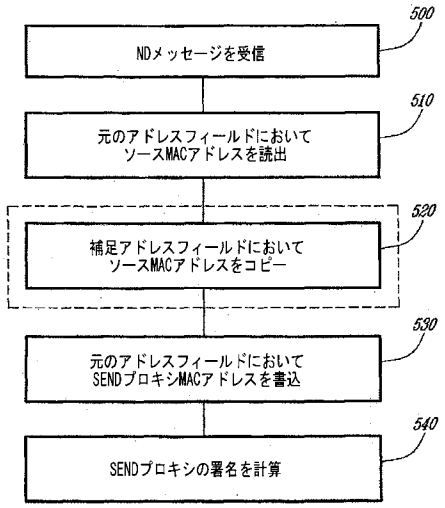

Fig. 5

【図６】

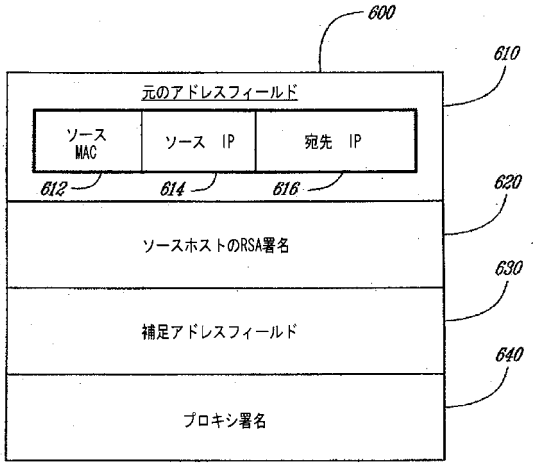

Fig. 6

【図７】

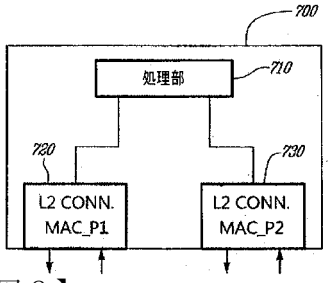

Fig. 7

【図８】

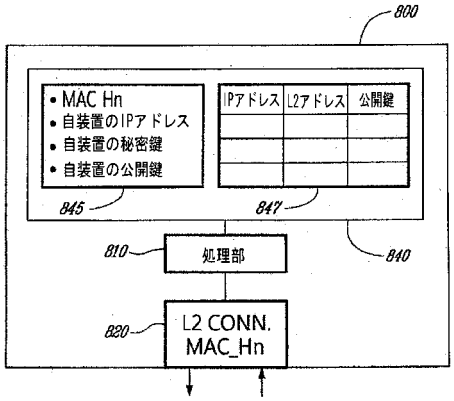

Fig. 8

フロントページの続き

(72)発明者　クリシュナン、スレッシュ
カナダ　エイチ３シー　６エス３　ケベック州　モントリオール　リューノートルダムウェスト
１２２５　アパートメント８２０

審査官　中里　裕正

(56)参考文献　特開２００４－４０７６２（ＪＰ，Ａ）
国際公開第２００６／１１９３５８（WO，Ａ２）
国際公開第２００７／０２７２４１（WO，Ａ２）
Daley, G., Securing Proxy Neighbour Discovery Problem Statement, Internet-Draft, IETF, ２００５年　2月１８日，ＵＲＬ，http://tools.ietf.org/html/draft-daley-send-spnd-prob-01
Arkko, J. et al., SEcure Neighbor Discovery (SEND), RFC 3971, IETF, ２００５年　3月，ＵＲＬ，http://datatracker.ietf.org/doc/rfc3971/
Thaler, D. et al., Neighbor Discovery Proxies (ND Proxy), RFC 4389, IETF, ２００６年　4月，ＵＲＬ，http://datatracker.ietf.org/doc/rfc4389/

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　１２／４６
Ｈ０４Ｌ　９／３２
ＪＳＴＰｌｕｓ／ＪＭＥＤＰｌｕｓ／ＪＳＴ７５８０（ＪＤｒｅａｍＩＩ）