(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4299860号
(P4299860)

(45)発行日　平成21年7月22日(2009.7.22)　(24)登録日　平成21年4月24日(2009.4.24)

(51)Int.Cl.		F I		
H04W 12/06	(2009.01)	H04Q	7/00	183
H04W 36/08	(2009.01)	H04Q	7/00	306
H04W 80/04	(2009.01)	H04Q	7/00	602
H04W 40/34	(2009.01)	H04L	12/56	100D
H04L 12/66	(2006.01)	H04L	12/66	B

請求項の数 19　(全 17 頁)　最終頁に続く

(21)出願番号　特願2006-522339 (P2006-522339)
(86)(22)出願日　平成16年6月25日 (2004.6.25)
(65)公表番号　特表2007-501554 (P2007-501554A)
(43)公表日　平成19年1月25日 (2007.1.25)
(86)国際出願番号　PCT/EP2004/051257
(87)国際公開番号　WO2005/015853
(87)国際公開日　平成17年2月17日 (2005.2.17)
審査請求日　平成18年2月28日 (2006.2.28)
(31)優先権主張番号　03291964.9
(32)優先日　平成15年8月6日 (2003.8.6)
(33)優先権主張国　欧州特許庁 (EP)

(73)特許権者　390009597
モトローラ・インコーポレイテッド
MOTOROLA　INCORPORATED
アメリカ合衆国イリノイ州シャンバーグ、イースト・アルゴンクイン・ロード１３０３
(74)代理人　100116322
弁理士　桑垣　衛
(72)発明者　オリーブロー、アレクシス
フランス国　Ｆ－９１１２０　パレゾー　リュ　モーリス　ベルトー　１１

最終頁に続く

(54)【発明の名称】認証済みの通信を行うための方法

(57)【特許請求の範囲】

【請求項１】

第１の移動ルータ（ＭＲ）（１２０）を介して、移動ネットワーク・ノード（ＭＮＮ）（１１０）と対応するノード（ＣＮ）（１５０）との間で認証済みの通信を行うための方法であって、

ｉ．ＭＮＮ試験開始（ＭＮＮＴＩ）メッセージがＭＲ（１２０）によって送信され、ＭＮＮ試験（ＭＮＮＴ）メッセージがＣＮ（１５０）によって送信されることによって、認証プロセス（２００）を行なうステップと、

ｉｉ．前記ＭＲ（１２０）から、前記ＭＮＮのアドレス（ＭＮＮＡ）（１１２）を含む拡張バインディング更新（ＸＢＵ）を送信するステップと、を含むことを特徴とする方法。

【請求項２】

ＭＲ（１２０）が、ＭＲ（１２０）と対応するノード（ＣＮ）（１５０）との間での認証プロセス（２００）を、移動ネットワーク・ノード（ＭＮＮ）（１１０）宛の移動ルータ（ＭＲ）（１２０）のホーム・エージェント（ＨＡ）（１３０）からトンネリングしたパケットを受信した後に開始する請求項１に記載の認証済みの通信を行うための方法。

【請求項３】

移動ルータ（ＭＲ）（１２０）と対応するノード（ＣＮ）（１５０）との間の認証プロセス（２００）が、

ＭＲ（１２０）が、ホーム・アドレス試験開始（ＨｏＴＩ）メッセージおよび気付けア

ドレス試験開始（ＣｏＴＩ）メッセージに対してランダムな値（以後「クッキー」と呼ぶ）を生成するステップ（２２６）を含み、さらに
ＭＮＮ試験開始（ＭＮＮＴＩ）メッセージのためのクッキーを生成するステップ、からなる請求項１に記載の認証済みの通信を行うための方法。
【請求項４】
移動ルータ（ＭＲ）（１２０）と対応するノード（ＣＮ）（１５０）との間の認証プロセス（２００）が、
ＭＲ（１２０）が、ＭＲのホーム・アドレス（ＨｏＡ）（１３２）およびＨｏＴＩクッキーを含むＨｏＴＩを前記ＣＮ（１５０）に送信するステップと、
ＭＲ（１２０）が、ＭＲの気付アドレス（ＣｏＡ）（１４２）およびＣｏＴＩクッキーを含むＣｏＴＩをＣＮ（１５０）に送信するステップと、を含み、さらに、
ＭＲ（１２０）が、ＭＮＮアドレス（ＭＮＮＡ）（１１２）およびＭＮＮＴＩクッキーを含むＭＮＮＴＩをＣＮ（１５０）に送信するステップ、
を含む請求項１に記載の認証済みの通信を行うための方法。
【請求項５】
ＨｏＴＩが、ＭＲのホーム・アドレス（ＨｏＡ）（１３２）を介して送信され、ＣｏＴＩが、ＭＲの気付けアドレス（ＣｏＡ）（１４２）を介して送信され、ＭＮＮＴＩが、前記ＨｏＡ（１３２）またはＣｏＡ（１４２）を介して送信される請求項４に記載の認証済みの通信を行うための方法。
【請求項６】
ＭＮＮＴＩメッセージが、さらにＭＲのホーム・アドレス（ＨｏＡ）（１３２）を含む請求項５に記載の認証済みの通信を行うための方法。
【請求項７】
移動ルータ（ＭＲ）（１２０）と対応するノード（ＣＮ）（１５０）との間の認証プロセス（２００）が、
ＣＮ（１５０）が、ＨｏＴＩから抽出したＨｏＡ（１３２）、ランダム・キー（ＫＣＮ）およびナンスからホーム・トークンを計算するステップと、
ＣＮ（１５０）が、ＣｏＴＩから抽出したＣｏＡ（１４２）、ＫＣＮおよびナンスら、気付けトークンを計算するステップと、を含み、
ＣＮ（１５０）が、ＭＮＮＴＩから抽出したＭＮＮＡ（１１２）、ＫＣＮおよびナンスから、ＭＮＮトークンを計算するステップ、をさらに含む、請求項１に記載の認証済みの通信を行うための方法。
【請求項８】
移動ルータ（ＭＲ）（１２０）と対応するノード（ＣＮ）（１５０）との間の認証プロセス（２００）が、
ＣＮ（１５０）が、ＨｏＴＩクッキー、ホーム・ナンス指数およびホーム・トークンを含むホーム・アドレス試験（ＨｏＴ）をＭＲ（１２０）に送信するステップと、
ＣＮ（１５０）が、ＣｏＴＩクッキー、気付けナンス指数および気付けトークンを含む気付けアドレス試験（ＣｏＴ）をＭＲ（１２０）に送信するステップと、を含み、さらに
前記ＣＮ（１５０）が、ＭＮＮＴＩクッキー、ＭＮＮナンス指数およびＭＮＮトークンを含むＭＮＮ試験（ＭＮＮＴ）を前記ＭＮＮ（１１０）に送信し、前記ＭＮＮＴが、
前記ＭＲのホーム・アドレス（ＨｏＡ）（１３２）を含む移動ルータ・プレゼンス・オプション（ＭＲＰＯ）をさらに含む、
請求項１に記載の認証済みの通信を行うための方法。
【請求項９】
移動ルータ（ＭＲ）（１２０）と対応するノード（ＣＮ）（１５０）との間の認証プロセス（２００）が、
ＣＮ（１５０）が、ＨｏＴＩクッキー、ホーム・ナンス指数およびホーム・トークンを含むホーム・アドレス試験（ＨｏＴ）をＭＲ（１２０）に送信するステップと、
ＣＮ（１５０）が、ＣｏＴＩクッキー、気付けナンス指数および気付けトークンを含む

気付けアドレス試験（ＣｏＴ）をＭＲ（１２０）に送信するステップと、を含み、さらに
ＣＮ（１５０）が、ＭＮＮＴＩクッキー、ＭＮＮナンス指数およびＭＮＮトークンを含むＭＮＮ試験（ＭＮＮＴ）をＭＮＮ（１１０）に送信し、前記ＭＮＮＴが、
気付けアドレス（ＣｏＡ）（１４２）を含む移動ルータ・プレゼンス・オプション（ＭＲＰＯ）をさらに含む、
請求項１に記載の認証済みの通信を行うための方法。
【請求項１０】
ＨｏＴが、ＭＲのホーム・アドレス（ＨｏＡ）（１３２）に送信され、ＣｏＴがＭＲの気付けアドレス（ＣｏＡ）（１４２）に送信され、前記ＭＮＮＴが、前記ＭＮＮアドレス（ＭＮＮＡ）（１１２）に送信される請求項９に記載の認証済みの通信を行うための方法。
【請求項１１】
移動ルータ（ＭＲ）（１２０）と対応するノード（ＣＮ）（１５０）との間の認証プロセス（２００）が、
ＭＲ（１２０）が、それ自身のホーム・アドレス（１３２）を、ＭＲ（１２０）が、ＭＮＮ（１１０）に経路指定するために受信するＭＮＮＴから抽出することができる任意のＭＲのホーム・アドレスと比較するステップ、
を更に含む請求項１に記載の認証済みの通信を行うための方法。
【請求項１２】
移動ルータ（ＭＲ）（１２０）と対応するノード（ＣＮ）（１５０）との間の認証プロセス（２００）が、
ＭＲ（１２０）が、それ自身の気付けアドレス（１４２）を、ＭＲ（１２０）が、ＭＮＮ（１１０）に経路指定するために受信するＭＮＮＴから抽出することができる任意のＣｏＡと比較するステップ、
を更に含む請求項１に記載の認証済みの通信を行うための方法。
【請求項１３】
ＭＲ（１２０）が、前記ＭＮＮＴを転送しないで、さらに、前記ＭＮＮＴから抽出したＭＮＮＴＩクッキーが、前記ＭＮＮＴＩ内の前記ＭＲ（１２０）が送信したＭＮＮＴＩクッキーと一致することを確認し、
一致を確認した場合に、前記ＭＮＮＴから前記ＭＮＮナンス指数およびＭＮＮトークンを抽出する請求項１２に記載の認証済みの通信を行うための方法。
【請求項１４】
移動ルータ（ＭＲ）（１２０）と対応するノード（ＣＮ）（１５０）との間の認証プロセス（２００）が、
ＭＲ（１２０）が、ＭＮＮトークンから、拡張バインディング更新（ＸＢＵ）認証鍵（ＫＢＭＮＮ）（３２４）を生成するステップ（２６６）を更に含む請求項１に記載の認証済みの通信を行うための方法。
【請求項１５】
移動ルータ（ＭＲ）（１２０）と対応するノード（ＣＮ）（１５０）との間の認証プロセス（２００）が、
ＭＲ（１２０）が、ＫＢＭＮＮ鍵（３２４）を用いて拡張バインディング更新（ＸＢＵ）署名（３２２）を生成するステップ（２７６）を更に含む請求項１に記載の認証済みの通信を行うための方法。
【請求項１６】
前記署名がＫＢＭＮＮ鍵（３２４）を用いるメッセージ認証コードをベースとする請求項１５に記載の方法。
【請求項１７】
前記拡張バインディング更新が、ＭＮＮナンス指数オプション（３２１）を更に含む請求項１５に記載の認証済みの通信を行うための方法。
【請求項１８】
前記拡張バインディング更新が、ＭＮＮアドレス（３２０）とＸＢＵ署名（３２２）のう

ちの１つからなる請求項１５に記載の方法。
【請求項１９】
移動ルータ（ＭＲ）（１２０）と対応するノード（ＣＮ）（１５０）との間の認証プロセス（２００）が、
ＣＮ（１５０）が、ＭＲ（１２０）からＣＮ（１５０）が受信したＸＢＵ（３００）から抽出したＫＢＭＮＮをベースとする署名（３２２）を認証するステップを更に含む請求項１８に記載の認証済みの通信を行うための方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、認証済みの通信を行うための方法に関し、特に、少なくとも第１の移動ルータを介しての移動ネットワーク・ノードと対応するノードとの間の認証済みの通信を行うための方法に関する。
【背景技術】
【０００２】
従来の移動体サポートの目的は、例えば、無線接続をすることができるラップトップ・コンピュータのような移動ホストに、継続的にインターネットにより接続することができるようにすることである。対照的に、ネットワークの移動体サポートは、多くの移動ホストを有する全ネットワークが、インターネット網の連結点を変更し、それによるインターネット網内の連結点に接続するルートを変更する状況に関する。移動中のこのようなネットワークは移動ネットワークと呼ぶことができる。
【０００３】
このような移動ネットワークが発生する多数のシナリオが存在する。２つだけ例を挙げると、
ｉ．パーソナル・エリア・ネットワーク（ＰＡＮ、すなわち、ある個人に取り付けられたいくつかの個人用装置のネットワーク）は、ユーザが町を歩き回っている間にインターネット網へのその連結点を変更する。
【０００４】
ｉｉ．乗客に搭載インターネット・アクセスを提供する、バスまたは航空機内にあるネットワーク。これらの乗客は、１つのデバイス（例えば、ラップトップ）を使用することもできるし、またはある移動ネットワークを訪問している移動ネットワーク（すなわち、入れ子状の移動体）の場合を示す移動ネットワーク（ＰＡＮ等）を所有することもできる。
【０００５】
それ故、移動ネットワーク（ＭＯＮＥＴ）は、一組のノード、すなわち、インターネットの残りの部分に対してユニットとして移動することができる移動ルータ（ＭＲ）に取り付けられている１つまたは複数のＩＰサブネットの一部であると定義することができる。すなわち、ＭＲおよびすべてのその連結ノード（いわゆる、移動ネットワーク・ノード、すなわちＭＮＮ）であると定義することができる。
【０００６】
ＭＮＮ自身は、所与の移動ネットワークに永久に関連するローカル固定ノード（ＬＦＮ）であってもよいし、現在の移動ネットワーク内のそのネットワーク連結点を変えることができ、他の場所に連結するために現在の移動ネットワークを離脱することができるローカル移動ノード（ＬＭＮ）であってもよいし、そのホーム・リンクが現在の移動ネットワーク上に存在しないで、その連結点を現在の移動ネットワークの外部のある場所から変更した在圏移動ノード（ＶＭＮ）であってもよい。すでに説明したように、ＭＮＮは、入れ子状の移動体になる簡単な移動ホストまたは他の移動ルータであってもよい。
【０００７】
移動ネットワークに対して使用することができる連結点の変更に関しては、このようなネットワークがデータのパケットを送受信するルートを最適化するための方法が、多くの

理由で非常に望ましいものである。

【０００８】

ｉ．ルートを最適化すると、パケット経路の長さが短くなり遅延が低減する。

ｉｉ．ルートを最適化すると、システムの使用できる全帯域幅が広くなる。何故なら、パケットがもっと短い経路を介して経路指定され、もはやトンネリングされないからである。

【０００９】

ｉｉｉ．ルートを最適化すると、通信経路上の最大送信単位のサイズを増大することができ、ペイロードの分割が少なくなる。

ＩＰｖ６（「移動ＩＰｖ６」またはＭＩＰｖ６）仕様の移動体のサポート（ｈｔｔｐ：／／ｗｗｗ．ｉｅｔｆ．ｏｒｇ／参照）は、ＭＮと対応するノード（ＣＮ）間のルートを最適化（最短経路を使用する二方向通信）することができるようにする手段を提案しているが、ＭＮＮとＣＮ間のルートを最適化することができるようにする機構はまだ提案されていない。

【００１０】

図１を参照すると、ＭＮＮとＣＮ間の通信に対する基幹ネットワーク・移動体サポート（ｈｔｔｐ：／／ｗｗｗ．ｉｅｔｆ．ｏｒｇ／の「ＮＥＭＯ基本サポート・プロトコル」）は、移動ルータ（ＭＲ）とそのホーム・エージェント（ＨＡ）間の二方向トンネリングに依存している。

【００１１】

ｉ．（ＣＮからＭＮＮへの）入力パケットは、ＭＲのホーム・リンクに送られる。ＭＲのＨＡは、それを傍受し、ＭＲにトンネリングする。

ｉｉ．（ＭＮＮからＣＮへの）出力パケットは、ＭＲによりそのＨＡに逆トンネリングされる。

【００１２】

しかし、この方法ではＭＮＮへのルートを最適化することはできない。

ＥＰ　１　１５８　７４２　Ａ１および関連する論文、２００２年３月付けのＩＥＴＦインターネット－草案　ｄｒａｆｔ－ｅｒｎｓｔ－ｍｏｂｉｌｅｉｐ－ｖ６－ｎｅｔｗｏｒｋ－０３．ｔｘｔ掲載の、Ｔ．Ｅｒｎｓｔ、Ａ．Ｏｌｉｖｅｒｅａｕ、Ｌ．Ｂｅｌｌｉｅｒ、Ｃ．Ｃａｓｔｅｌｌｕｃｃｉａ、Ｈ．－Ｙ．Ｌａｃｈの、「移動ＩＰｖ６での移動ネットワークのサポート（プレフィックス・スコープ・バインディング・更新）」（Ｍｏｂｉｌｅ　Ｎｅｔｗｏｒｋｓ　Ｓｕｐｐｏｒｔ　ｉｎ　Ｍｏｂｉｌｅ　ＩＰｖ６（Ｐｒｅｆｉｘ　Ｓｃｏｐｅ　Ｂｉｎｄｉｎｇ　Ｕｐｄａｔｅｓ））は、ＭＲが、在圏ネットワークにローミングした場合、これらの文書がプレフィックス・スコープ・バインディング更新（ＰＳＢＵ）として参照するＭＩＰｖ６バインディング更新（ＢＵ）の修正版をそのホーム・エージェント（ＨＡ）に送信する方法を記載している。

【００１３】

古典ＭＩＰｖ６　ＢＵは、ＣＮに、１つの移動ノード（例えば、移動気付けアドレス（ＣｏＡ）と結合している移動ルータのホーム・アドレス（ＨｏＡ））宛のデータの送り先を知らせるだけである。提案のＰＳＢＵは、ＭＲ　ＨｏＡをＭＲ　ＣｏＡにバインドしないで、ＭＲプレフィックスをＭＲ　ＣｏＡにバインドするので、ＰＳＢＵを受信しているＨＡに、ＭＲに取り付けてある任意のＭＮＮ宛のデータをＭＲ　ＣｏＡに送るように通知する。

【００１４】

その宛先アドレスが、ＭＲプレフィックス（例えば、宛先がＭＮＮである）と一致するパケットを受信した場合には、ホーム・エージェント（ＨＡ）は、パケットをこのパケットを実際の受信人に送るＭＲ　ＣｏＡにトンネリングしなければならない。

【００１５】

同様に、ＭＲは、ＰＳＢＵをＣＮ／ＭＮＮルート最適化を行うＭＮＮの対応するノードに送信することができる。

しかし、この解決方法は、その受信人がＰＳＢＵの認証に成功した場合だけに使用することができる。ピア認証の範囲を超えた場合、ＰＳＢＵの送信人は、自身がＰＳＢＵを送るプレフィックス全部を有していることを実際に証明しなければならない。

【００１６】

ＰＳＢＵの受信人が、ＭＲに属するプレフィックスについて最初の知識を有していると予想されるＭＲホーム・エージェントである限りは、このことは問題にならない。しかし、受信人が任意のＣＮである場合には、そのＣＮがＰＳＢＵを認証することができるようにするある機構を発見しなければならない。この解決方法の適用範囲を大幅に低減する機構はまだ提案されていない。

【００１７】

この方法の適用範囲は、古典ＭＩＰｖ６　ＢＵ認証に対してすでに提案されていると見なすことができる。

ｉ．暗号化により生成したアドレス

この解決方法の場合、ホーム・アドレス（ＨｏＡ）は、公開鍵／秘密鍵のペアの一部である公開鍵と結合している。これにより、悪意のあるノードは、ホーム・アドレスのふりを決してすることができない。何故なら、悪意のあるノードは対応する秘密鍵を所有していないからである。

【００１８】

しかし、ＰＳＢＵに関しては、この方法を、プレフィックスの所有まで拡張することはできない。何故なら、多数のホーム・アドレスが、同じプレフィックスを共有することができるからである。さらに、ＭＩＰｖ６または任意の将来の仕様が、任意の移動ネットワークがそれ自身のアドレスまたはプレフィックスを割り当てることができるようにする可能性は少ない。所有を一意のものにするために、プレフィックスに追加のハッシュを追加するのは、ネットワーク・プレフィックス内の使用できるビット数により制限を受ける。推定では、一意性すなわちセキュリティを喪失する機会を５０％にするには、攻撃者は、2^{16}（約６５，０００）の公開鍵を試験しなければならない。

【００１９】

ｉｉ．リターンルーチング可能性チェック手段（ＲＲＰ）

ＲＲＰは、現在、ＭＩＰｖ６仕様に含まれていて、バインディング更新（ＢＵ）を受け入れる前に、指定の気付けアドレス（ＣｏＡ）のところで、指定のホーム・アドレス（ＨｏＡ）に実際に到達することができることを確認するための対応するノード（ＣＮ）によるチェックからなる。本質的には、このプロセスは下記のものを含む。

【００２０】

・ホーム試験開始（ＨｏＴＩ）メッセージおよび気付け試験開始（ＣｏＴＩ）メッセージをＣＮに送信することにより、手段を開始する移動ノード（ＭＮ）

・ＭＮのホーム・アドレスにホーム試験（ＨｏＴ）メッセージを送信し、ＭＮの気付けアドレスに気付け試験（ＣｏＴ）メッセージ）を送信するＣＮ

・ＨｏＴおよびＣｏＴの両方の内容から、ＭＮは、送信するＢＵに署名するために使用する鍵を生成する。

【００２１】

それ故、ＭＮは、有効なＢＵを生成することができるように、ＨｏＴおよびＣｏＴの両方の受信に成功しなければならない。このことは、ＣＮによりホーム・アドレスおよび気付けアドレスがそのＭＮに対して有効であるという十分な証拠であると見なされる。

【００２２】

しかし、ＰＳＢＵに関しては、全部のプレフィックスがある気付けアドレスに到達するかどうかを確認するためにこの機構を使用することはできない。プレフィックスの所有は、アドレスの所有より遥かに重要である。類似のレベルのセキュリティを入手するためには、ＣＮは、ＲＲＰにより、そのネットワーク・プレフィックスから入手することができるすべての可能なアドレスをチェックしなければならない。

【００２３】

このようなことは明らかに不可能である。何故なら、標準プレフィックスの長さの場合、可能なＩＰｖ６のアドレスの数は莫大なものになるからである。

それ故、ＰＳＢＵは、移動ネットワークに認証済みのルート最適化を提供することはできない。すなわち、ＰＳＢＵは、その内部に位置する任意の移動ネットワーク・ノードに、認証済みのルート最適化を提供することはできないという結論になる。

【発明の開示】

【発明が解決しようとする課題】

【００２４】

それ故、移動ネットワーク・ノードに対して認証済みのルートを最適化するための方法の開発が依然として待望されている。

本発明の目的は、このニーズを満たすことである。

【課題を解決するための手段】

【００２５】

本発明は、添付の特許請求の範囲に記載するように、少なくとも第１の移動ルータ（ＭＲ）を介して、移動ネットワーク・ノード（ＭＮＮ）と対応するノード（ＣＮ）との間で認証済みの通信を行うための方法を提供する。

【００２６】

第１の態様においては、本発明は、請求項１に記載するように、認証済みの通信を行うための方法を提供する。

第２の態様においては、本発明は、請求項３２に記載するように、認証済みの通信のための装置を提供する。

【００２７】

第３の態様においては、本発明は、請求項３３に記載するように、認証済みの通信を行うために動作することができる移動ルータを提供する。

第４の態様においては、本発明は、請求項３４に記載するように、認証済みの通信を行うために動作することができる対応するノードを提供する。

【００２８】

本発明の他の特徴は、従属請求項に定義してある。

添付の図面を参照しながら以下に本発明の実施形態について説明するが、これは単に例示としてのものに過ぎない。

【発明を実施するための最良の形態】

【００２９】

本発明は、認証済みの通信を行うための方法を提供する。下記の説明において、本発明を完全に理解してもらうために、多数の特定の詳細について説明する。しかし、当業者であれば、これらの特定の詳細は、本発明を実行するために使用する必要がないことを理解することができるだろう。他の例の場合には、本発明が分かりにくくなるのを避けるために、周知の方法、手順および構成要素の詳細な説明は省略してある。

【００３０】

図１を参照すると、この図は、少なくとも第１の移動ルータ（ＭＲ）１２０を介しての移動ネットワーク・ノード（ＭＮＮ）１１０と対応するノード（ＣＮ）１５０との間で認証済みの通信を行うための方法を示す。

【００３１】

図１は、移動ルータ（ＭＲ）１２０およびそのホーム・アドレス１３２から在圏リンク上のあるアドレス１４２に移動したそのネットワークであって、移動ネットワーク・ノード（ＭＮＮ）（１１０）を認証済みのルートを最適化する方法を必要としているネットワークを示す。

【００３２】

ここで図２についても説明すると、本発明のある実施形態においては、この方法は、拡張リターンルーチング可能性チェック手順（ＸＲＲＰ）２００を使用する。この場合、ＭＮＮ試験開始（ＭＮＮＴＩ）メッセージが、ＭＲ１２０により送信され（２３６）、ＭＮ

Ｎ試験（ＭＮＮＴ）メッセージがＣＮ１５０により送信される（２５６）。
【００３３】
これは、３つのＨｏＴ、ＣｏＴおよびＭＮＮＴ試験メッセージの任意のものまたはすべての上での受信に基づいて、バインディング更新認証鍵の生成を可能にすることにより、標準ＲＲＰのところですでに説明したように、ホーム・アドレスおよび気付けアドレスが同じでなければならないセキュリティの一助になる。
【００３４】
さらに、図３を参照すると、本発明のこの実施形態の方法は、また、ＭＲ１２０からのＭＮＮのアドレス（ＭＮＮＡ）１１２を含む（３２０）拡張バインディング更新（ＸＢＵ）（３００）を送信するステップを含む。
【００３５】
このようにＭＮＮＡを含むようにバインディング・更新を拡張することにより、認証済みＣＮ／ＭＮＮルートの最適化を行うことができる。より詳細に説明すると、認証済みＣＮ／ＭＮＮルートの最適化は、セキュリティ・コンテキストを予め確立しなくても行うことができる。
【００３６】
さらに、このことは、移動ネットワーク・ルート最適化に適当なレベルのセキュリティを提供する。より詳細に説明すると、悪意のあるノードは、ＭＮＮのアドレスを装うことができず、データを他の宛先に送ることができず、またはＭＲの気付けアドレスのフリをすることもできず、それに対するサービス攻撃を拒否することもできない。
【００３７】
さらに、このことは、ＭＮＮに対して透明であるので、ノードを変更する必要がなく、そのため現在の装置は、本発明の利点を使用することができる。
拡張リターンルーチング可能性チェック手順２００については、以下に詳細に説明する。
【００３８】
ＭＲ１２０は、ＭＮＮ１１０が、そのＭＮＮ１１０に対するそのホーム・エージェントからのトンネリングしたパケットを受信した場合にはいつでも、ルート最適化が、ＭＮＮ１１０に対して使用されていないことを検出する。
【００３９】
それ故、ＭＲ１２０と対応するノードＣＮ１５０との間の認証プロセス２００は、移動ネットワーク・ノードＭＮＮ１１０宛のＭＲ１２０のホーム・エージェントＨＡ１３０からのトンネリングしたパケットをＭＲ１２０が受信した場合に開始する。
【００４０】
しかし、これは下記の一組の条件のうちの少なくとも１つの適用を受ける。すなわち、
ｉ．ＭＮＮ１１０は、指定のサービスに加入する。
ｉｉ．ＣＮ１５０は、前のＸＢＵ３００のしきい値数を無視したことがない。
【００４１】
ｉｉｉ．ＣＮ１５０は、認証プロセス２００のしきい値数を無視したことがない。
ｉｖ．ＭＮＮ１１０は、使用ポリシーを満足する。
認証プロセス２００が開始すると、ＭＲ１２０は、当業者であれば周知のように、ホーム・アドレス試験開始（ＨｏＴＩ）メッセージおよび気付けアドレス試験開始（ＣｏＴＩ）メッセージに対してランダムな値（以後「クッキー」と呼ぶ）を生成する。
【００４２】
しかし、さらに、ここで、追加の移動ネットワーク・ノード試験開始（ＭＮＮＴＩ）メッセージに対してもう１つのクッキーを生成することを提案する。
本発明の発明者は、現在のＭＩＰｖ６仕様の制約により、追加のメッセージを使用しなければならないことを理解している。ＭＲ１２０は、バインドしているＭＲ　ＨｏＡ１３２／ＭＲ　ＣｏＡ１４２が正しいことを証明しなければならないが、この証明の他に、ＭＮＮ１１０を含む第３のチェックが、所望のレベルの認証に対して必要である。それ故、

本質的には、ＭＮＮ１１０が、そのパケットを経路指定するためにＭＲ１２０を信頼することを証明することができなければならないか、またはＭＲ１２０が、ＭＮＮ１１０宛のパケットを経路指定することができることを証明することができなければならない。

【００４３】

ＭＮＮ１１０に対して透明であるという利点を保持するために、本発明の発明者は、第２の機構を選択する。ＣＮ１５０が要求した場合には、ＭＲ１２０は、自身がＭＮＮ１１０に実際にサービスを提供していることを証明しなければならない。ＭＩＰｖ６は、ホーム・アドレス所有の証明を、それぞれ、ＭＲ　ＨｏＡ１３２からＣＮ１５０へ送った、およびＣＮ１５０からＭＲ　ＨｏＡ１３２に送ったＨｏＴＩ（ホーム試験開始）メッセージおよびＨｏＴ（ホーム試験）メッセージにより行うように指定する。同様に、気付けアドレス所有の証明が、それぞれＭＲ　ＣｏＡ１４２からＣＮ１５０へ、およびＣＮ１５０からＭＲ　ＣｏＡ１４２に送ったＣｏＴＩ（気付け試験開始）メッセージおよびＣｏＴ（気付け試験）メッセージにより行われる。

【００４４】

それ故、認証プロセス（２００）は、当業者であれば周知のように、ＭＲ１２０が、ＭＲのホーム・アドレス（ＨｏＡ）１３２およびＣＮ１５０へのＨｏＴＩクッキーを含むＨｏＴＩを送るステップと、ＭＲ１２０が、ＭＲの気付けアドレス（ＣｏＡ）１４２およびＣＮ１５０へのＣｏＴＩクッキーを含むＣｏＴＩを送るステップ（２３６）を含み、さらに、ＭＲ１２０が、ＭＮＮアドレス（ＭＮＮＡ）１１２およびＣＮ１５０へのＭＮＮＴＩクッキーを含むＭＮＮＴＩを送るステップを含む。

【００４５】

ＨｏＴＩは、ＭＲのホーム・アドレス（ＨｏＡ）１３２を介して送られ、ＣｏＴＩは、ＭＲの気付けアドレス（ＣｏＡ）１４２を介して送られる。

しかし、ＨｏＴＩメッセージおよびＣｏＴＩメッセージとは異なり、ＭＮＮＴＩメッセージは、移動体・オプション（ＭＩＰｖ６内に定義されている）を含み、このオプションはＭＮＮアドレス１１２を含む。

【００４６】

本発明の好ましい実施形態の場合には、ＭＮＮＴＩは、ＭＲ　ＨｏＡ１３２を介して送られる。

本発明の他の実施形態の場合には、ＭＮＮＴＩは、ＭＲの気付アドレス（ＣｏＡ）１４２を介して送られる。次に、ＭＮＮＴＩメッセージは、さらにＭＲのホーム・アドレス（ＨｏＡ）１３２を含む。

【００４７】

本発明のある実施形態の場合には、関連試験開始メッセージを受信した場合には、ＣＮ１５０は、当業者であれば周知のように、ランダム・キー（ＫＣＮ）およびナンス（時間依存値）と一緒に、ＨｏＴＩから抽出したＨｏＡ１３２からホーム・トークンを計算し、およびＣｏＴＩ、ＫＣＮおよびナンスから抽出したＣｏＡ１４２からの気付けトークンを計算するステップ２４６を実行する。

【００４８】

さらに、ＭＮＮＴＩを受信した場合には、ＣＮ１５０は、ＫＣＮおよびナンスと一緒に、ＭＮＮＴＩから抽出したＭＮＮＡ１１２からＭＮＮトークンを計算する。

各初期化試験に応じてトークンを生成した後で、当業者であれば周知のように、ＣＮ１５０は、ＨｏＴＩクッキー、ホーム・ナンス指数およびＭＲ１２０へのホーム・トークンを含むホーム・アドレス試験（ＨｏＴ）を送信し、ＣｏＴＩクッキー、気付けナンス指数およびＭＲ１２０への気付けトークンを含む気付けアドレス試験（ＣｏＴ）を送信するステップ２５６を実行する。ナンス指数を使用すれば、ＣＮは、セキュリティを危うくするので、ナンス自身を送信しないで、トークンを生成するために使用したナンスを検索することができる。

【００４９】

さらに、ＣＮ１５０は、ＭＮＮＴＩクッキー、ＭＮＮナンス指数、ＭＮＮ１１０へのＭ

ＮＮトークンを含む移動ネットワーク・ノード・アドレス試験（ＭＮＮＴ）を送信する。ＭＮＮＴは、さらに、ＭＲのホーム・アドレス（ＨｏＡ）１３２を含む移動ルータ・プレゼンス・オプション（ＭＲＰＯ）を含む。

【００５０】

ＨｏＴは、ＭＲ　ＨｏＡ１３２に送られ、ＣｏＴは、ＭＲ　ＣｏＡ１４２に送られる。ＭＮＮＴは、ＭＮＮアドレス（ＭＮＮＡ）１１２に送られる。

その目的は、ＨｏＴおよびＣｏＴの場合には、両方ともＭＲに到達することであり、ＭＮＮＴの場合には、ＭＮＮに到達することである。

【００５１】

ＭＮＮトークンは、依然として秘密のままである場合には認証プロセス２００内でもっと高いレベルのセキュリティを提供することに留意されたい。この目的のために、ホーム・エージェント（ＨＡ）１３０は、ＣＮ１５０がそれを暗号化しない場合には、ＭＲ１２０に上記ＭＮＮＴをトンネリングする場合にＭＮＮＴを暗号化することができる。

【００５２】

移動ルータ・プレゼンス・オプション（ＭＲＰＯ）は、受信人の経路上のすべてのルータにそれをチェックするように指示するＩＰホップ・バイ・ホップ・オプションである。しかし、実際には、移動ルータだけが、通常このオプションをチェックする。

【００５３】

本発明の発明者は、このことが必要であることを理解している。何故なら、それが正しい場所に確実に経路指定されるようにするためにＭＮＮＴをＭＮＮ１１０宛に送るからである。しかし、それが正しい位置の有効なＭＲである場合には、ＭＲ１２０は、それによる認証鍵を生成するために、ＭＮＮＴを傍受できることが望ましい。そうするには、ＭＲＰＯ内のＭＲ　ＨｏＡ１３２のようなＭＮＮＴのある特徴のある部分をチェックすることができるＭＲ１２０のための施設が必要である。

【００５４】

それ故、ＭＲ１２０は、それ自身のホーム・アドレス１３２を、ＭＮＮ１１０に経路指定するために受信するＭＮＮＴから抽出するＭＲのホーム・アドレスと比較する。

他の実施形態の場合には、ＭＲＰＯは、ＭＲ　ＨｏＡではなくＭＲの気付アドレス（ＣｏＡ）を含み、ＭＲは、それ自身のＣｏＡ１４２をＭＮＮ１１０に経路指定するために受信するＭＮＮＴから抽出するＭＲ　ＣｏＡと比較する。

【００５５】

上記ＨｏＡまたはＣｏＡの場合には、アドレスが一致する場合には、ＭＲ１２０は、ＭＮＮＴをさらにＭＮＮには転送しない。代わりに、ＭＲ１２０は、ＭＮＮＴから抽出したＭＮＮＴＩクッキーがＭＮＮＴＩ内のＭＲ１２０が送信したものと一致するかどうかを確認し、一致を確認した場合には、ＭＮＮＴからＭＮＮナンス指数およびＭＮＮトークンを抽出する。

【００５６】

それ故、クッキーは、悪意により構成されたＭＮＮＴに対してフェイルセーフとなる。

ＭＲ１２０は、この時点で、有効なＸＢＵを生成することができる。

図３を参照すると、ＭＲ１２０は、ＭＮＮＴ、ＨｏＴおよびＣｏＴを受信した後で、ＣＮ１５０が生成したホーム・トークン、気付けトークンおよびＭＮＮトークンを含む。次に、当業者であれば周知のように、ＭＲは、ＣＮ１５０が有効なＭＲ１２０に属していることを認識するホーム・トークンおよび気付けトークンからバインディング・更新認証鍵（ＫＢＭ）３１４を生成することができる。

【００５７】

さらに、ＭＲ１２０は、また、ＭＮＮトークンから拡張バインディング・更新（ＸＢＵ）認証鍵（ＫＢＭＮＮ）を生成（２６６）することができる。

本発明のある実施形態の場合には、拡張を理解することができないＣＮ１５０により受信された場合には、ＸＢＵは、標準ＢＵとして解釈されるように構成されている。

【００５８】

それ故、ＸＢＵは、ＭＩＰｖ６　ＢＵに新しいオプションを追加することにより入手される。それ故、拡張バインディング・更新は、少なくとも下記の２つのオプションを含む。

【００５９】

ｉ．ＭＮＮアドレス３２０

ｉｉ．ＸＢＵ署名３２２

任意のより好適な追加オプションｉｉｉは、ＭＮＮナンス指数３２１である。

【００６０】

ＭＮＮアドレス・オプション３２０は、ＸＢＵが送られるＭＮＮ１１２のアドレスを含み、一方、ＸＢＵ署名オプション３２２は、全ＸＢＵ上で行われたＫＢＭＮＮ鍵３２４を使用するメッセージ認証コード（ＭＡＣ）に基づいて生成（２７６）することが好ましい。

【００６１】

次に、ＭＲは、通常はＣＮ１５０であるその受信人にＸＢＵを送信する。

署名３２２内のＣＮ１５０からのＭＮＮトークンに基づいてＫＢＭＮＮ鍵３２４を含むことにより、ＣＮ１５０は、ＭＲ１２０からＣＮ１５０が受信したＸＢＵ３００から抽出したＫＢＭＮＮをベースとする署名３２２を認証することができる。

【００６２】

本発明のある実施形態の場合には、ＣＮ１５０がＸＢＵ３００を受信し、認証に成功すると、ＣＮ１５０は、認証済みのＸＢＵ３００からのそのバインディング・キャッシュ（ＢＣ）に２つの入力を追加する。

【００６３】

ｉ．当業者であれば周知のように、ＭＲ　ＨｏＡ１３２には、ＭＲ　ＣｏＡ１４２を介して到達できるというマークが付けられる。

ｉｉ．さらに、ＭＮＮＡ１１２には、ＭＲ　ＨｏＡ１３２を介して到達できるというマークが付けられる。

【００６４】

ＥＰ　０２２９１３３１．３（Ｍｏｔｏｒｏｌａ）に詳細に記載されているように、ＣＮは、そのバインディング・キャッシュの再帰的パーズを使用していると仮定することができる。

【００６５】

それ故、ＣＮが入力点としてＭＮＮアドレス１１２によりそのＢＣをパーズした場合には、ＭＲ　ＨｏＡ１３２が最初に返送される。ＢＣの再帰的パーズのおかげで、次に、ＢＣ内でＭＲ　ＨｏＡ１３２が探索され、ＭＲ　ＣｏＡ１４２を返送する。

【００６６】

本発明の他の実施形態の場合には、ＣＮ１５０のバインディング・キャッシュに追加された２つの入力は、

ｉ．当業者であれば周知のように、ＭＲ　ＣｏＡ１４２を介して到達できるというマークがつけられたＭＲ　ＨｏＡ１３２、および

ｉｉ．さらに、ＭＲ　ＣｏＡ１４２を介して到達できるというマークがつけられたＭＮＮＡ１１２である。

【００６７】

それ故、ＣＮが、入力点としてのＭＮＮアドレス１１２でそのＢＣをパーズした場合には、ＭＲ　ＣｏＡ１４２が最初に返送される。

次に、どちらの実施形態の場合にも、ＣＮ１５０は、その宛先が、例えば、ＭＲ　ＣｏＡ１４２のような第１の中間アドレスである１つのＩＰヘッダを含み、その後に、ＭＲ　ＨｏＡ１３２およびＭＮＮＡ１１２のような他の中間アドレスを有するルーティング・ヘッダが続き、その後に最後に、ペイロードが続くパケットを組立てることができる。

【００６８】

もっと一般的にいうと、入れ子状の移動ルータの場合には、ＣＮ１５０は、トップ・レ

ベルの移動ルータ気付けアドレスのＩＰヘッダ宛先を含み、少なくとも以降の移動ルータの気付けアドレスおよびＭＮＮＡ１１２を含み、その後に最後にペイロードが続くルーティング・ヘッダを含むＭＮＮ１１０宛のパケットを経路指定する。

【００６９】

ＣＮ１５０が、ＸＢＵ３００により、そのバインディング・キャッシュ（ＢＣ）内で生成した期限切れＭＮＮ　ＢＣ入力をリフレッシュしたい場合には、ＣＮ１５０は、古典ＭＩＰｖ６バインディング要求メッセージの修正版を送信しなければならないことに留意されたい。その拡張バインディング要求（ＸＢＲ）は、ＭＲに送られ、それが発行されるＭＮＮ１１０のアドレス１１２を含む。期限切れおよびＢＣ内のデータのリフレッシュのような目的のために、ＭＮＮ　ＢＣ入力（「ＭＮＮアドレスはＭＲ　ＨｏＡのところに到達することができる」）をＭＲ　ＢＣ入力（「ＭＲ　ＨｏＡは、ＭＲ　ＣｏＡのところに到達することができる」）から区別することができることに留意されたい。しかし、両方ともＣＮ１５０が認証済みＸＢＵ３００を受信した場合に生成される。通常、これら２つの入力は、同じ寿命を有していてはならない（ＭＮＮ　ＢＣ入力の寿命の方が遥かに長い）。ＣＮ１５０がこの区別をすることができるようにするために、ＣＮ　ＢＣの構造を若干修正しなければならない（例えば、ＭＮＮ入力であるかないかを指定する各入力にフラグを追加することにより）。

【００７０】

本発明のある実施形態の場合には、移動ルータがある移動ルータ（入れ子状の移動体）を訪問した場合のために、移動ルータは、そのホーム・エージェントからトンネリングしたパケットを受信した場合には、内部パケットの宛先アドレスに対して内部パケットのソース宛先へＸＢＵを送信する。

【００７１】

図４Ａおよび図４Ｂを参照すると、第２の移動ルータをホストしている第１の移動ルータの場合のために：

第１の移動ルータ（ＭＲ１）４２０のネットワークは、第２の移動ルータ（ＭＲ２）４６０を有し、ＭＲ２　４６０のネットワークはＭＮＮ４１０を有する。

【００７２】

ＣＮ１５０をＭＮＮ１１０にリンクするＣＮバインディング・キャッシュ内のバインドのシーケンスをコンパイルするために、認証プロセス２００は２回始動される。１回目の始動は、（ＭＲ２のＨＡ４７０によりトンネリングされた）ＭＲ２　４６０により第１のパケット（図４Ａ）を受信した場合行われ、２回目の始動は、（ＭＲ２　ＣｏＡ４８２へ直接送信され、ＭＲ１のＨＡ４３０によりトンネリングされた）ＭＲ１　４２０により、第２のパケット（図４Ｂ）を受信した場合に行われる。図４Ａおよび図４Ｂの丸で囲んだ数字は、２つのパケットの各ルータを示す。

【００７３】

図４Ａを参照すると、第１のトンネリングしたパケットを受信した場合には、ＭＲ１　４２０は、ＭＲ２　ＣｏＡ４８２に対するＭＲ２のホーム・エージェント（ＨＡ２）４７０にＸＢＵ４０１を送信する。何故なら、ＨＡ２のアドレスおよびＭＲ２　ＣｏＡは、それぞれ、内部パケットのソース・フィールドおよび宛先フィールド内に位置するからである。（内部パケットは、パケット内のシリーズ内の次のＩＰヘッダで始まると定義される。図５を参照すると、パケット５１０は、ＩＰヘッダ５０１で開始し、５２０で別に示すその内部パケットは、ヘッダ５０２で開始する）。

【００７４】

ＨＡ２　４７０は、通常、ＸＢＵ４０１を無視する。その目的は、認証プロセスと同じ方法で内部パケットを「アンラップ」することである。

ＭＲ１　４２０は、内部パケットをＭＲ２　４６０に転送する。ＭＲ２　４６０は、パケットを受信した場合、（第２の）内部パケットをデトンネリングし、ＸＢＵ４０２をＭＮＮＡ４１２に対するＣＮ４５０に送信する。何故なら、ＣＮアドレスおよびＭＮＮアドレスは、それぞれ内部パケットのソース・フィールドおよび宛先フィールド内に位置する

からである。ＭＲ２　４６０は、最後に内部パケットをＭＮＮ１１０に転送する。

【００７５】

その結果、ＣＮは、間接的にＭＮＮＡ１１２をＭＲ２　ＣｏＡ４８２にリンクするために、そのバインディング・キャッシュを更新する。

図４Ｂを参照すると、ＭＲ２　ＨｏＡ４７２およびＭＮＮＡ４１２を含むルーティング・ヘッダを有するＭＲ２　ＣｏＡ４８２に直接送信された第２のトンネリングしたパケットを受信した場合には、ＨＡ１　４３０は、それを傍受し、それをＭＲ１　ＣｏＡ４４２にトンネリングする。

【００７６】

それを受信した場合、ＭＲ１　４２０は、ＸＢＵ４０３をＭＲ２　ＣｏＡ４８２に対するＣＮ４５０に送信する。何故なら、ＣＮおよびＭＲ２の気付けアドレスは、それぞれ、内部パケットのソース・フィールドおよび宛先フィールド内に位置するからである。

【００７７】

その結果、ＣＮは、ＭＲ２　ＣｏＡ４８２をＭＲ１　ＣｏＡ４４２に間接的にリンクするためにバインディング・キャッシュを更新する。

それ故、ＣＮ　ＢＣ内でこのように生成された４つすべての入力は、再帰的にパーズした場合、ＭＲ１　ＣｏＡ４４２のＩＰヘッダ宛先、および（ＭＲ１　ＨｏＡ４３２、ＭＲ２　ＣｏＡ４８２、ＭＲ２　ＨｏＡ４７２、ＭＮＮＡ４１２）のルーティング・ヘッダを含むＭＮＮ４１０にパケットを経路指定する。

【００７８】

当業者であれば、上記例は、移動ネットワークの入れ子状の１つのレベルに限定されないことを理解することができるだろう。

本発明の高度の実施形態の場合には、移動ネットワークがある移動ネットワーク（入れ子状の移動体）を訪問した場合のために、上記のように第１のＸＢＵ４０１を送信するのを避けることができる。このことは、移動ネットワークのｎレベルが入れ子状になっている場合、ＸＢＵが無駄にならないというもう１つの利点を有する。このことは、また、トンネリング方法により送信するパケットの数を低減する。

【００７９】

この実施形態の場合には、移動ルータは、そのホーム・エージェントからトンネリングしたパケットを受信した場合、ＸＢＵを内部パケットの宛先アドレスに対する最も内側のパケットのソース・アドレスに送信する。

【００８０】

図５および図６を参照すると、トンネリングしたパケット５１０は、ＭＮＮへのルートの各ステップに対するＩＰヘッダを含む前に添加されたペイロードを示す。図を見やすくするために、パケット５１０内の各ＩＰヘッダは、任意の以降のパケットおよびそれ故ペイロードを含むパケットのヘッダと見なすことができる。それ故、この場合、第１のパケット５０１は、ＭＲ１　ＣｏＡ４４２に向けられ、一方、最も内側のパケット５０６は、ＭＮＮＡ１１２に向けられる。

【００８１】

第１のトンネリングしたパケット５１０を受信した場合には、ＭＲ１　４２０は、ＸＢＵ５１６を第２の（または「内側の」）パケット５０２、すなわち、ＭＲ２　ＣｏＡ４８２の宛先５１４に対する最も内側のパケット（ＣＮ）５１２のソース・アドレスに送信する。

【００８２】

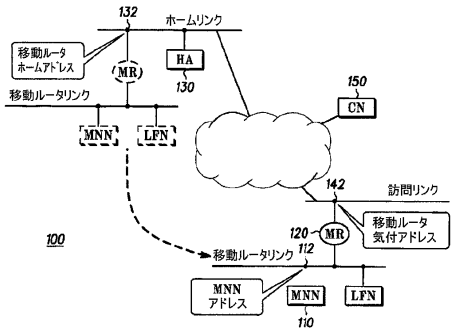
これにより、ＣＮは、ＭＲ２　ＣｏＡ４８２へＭＲ１　ＣｏＡ４４２をリンクするために、そのバインディング・キャッシュ（ＢＣ）を更新することができる。

パケットをＭＲ２　４６０に送った場合、ＭＲ２　４６０は、第２のパケット５２０を受信する。上記プロセスを反復することにより、ＭＲ２　４６０は、ＸＢＵ５２６を宛先５２４宛の最も内側のパケット（ＣＮ）５２２のソース・アドレスに送信する。万一存在する場合には、ＭＲ３　ＣｏＡへ送信する。

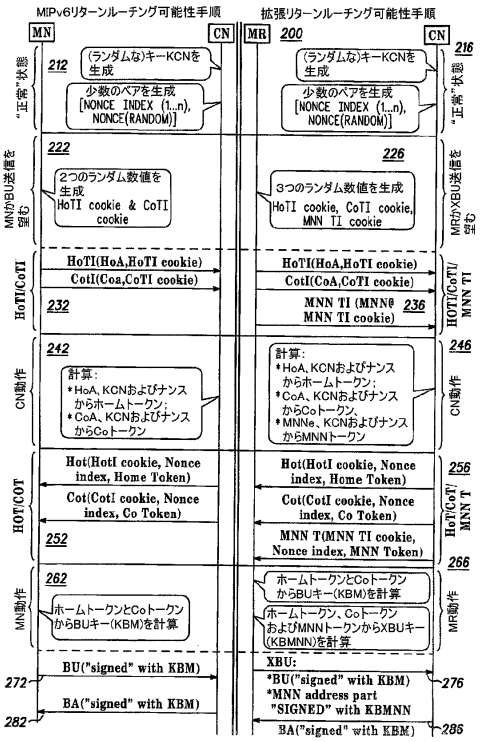
【００８３】
このプロセスは、ＭＲｎが、ＸＢＵ５５６をＭＮＮ４１０に対する最も内側のパケットＣＮ５５２のソース・アドレスに送信した場合には、ＭＮＮ４１０が取り付けられているＭＲｎに到達するまで反復して行われる。
【００８４】
再帰的にパーズした場合、ＣＮ　ＢＣ内でこのように生成した２ｎの入力は、ＭＲ１　ＣｏＡ５４２のＩＰヘッダ宛先を含むＭＮＮ５１０に対するパケットを経路指定する。図６の場合には、ＢＣの内容は、見やすくするために順序を変えてあることに留意されたい。
【００８５】
図６のアーキテクチャの場合には（図４Ａおよび図４Ｂのアーキテクチャをコピーした）、第１の移動ルータ（ＭＲ１）４２０のネットワークは、第２の移動ルータ（ＭＲ２）４６０を有し、ＭＲ２　４６０のネットワークは、ＭＮＮ４１０を有する。
【００８６】
第１のトンネリングしたパケットを受信した場合には、ＭＲ１　４２０は、ＸＢＵ６０１をＭＲ２　ＣｏＡ４８２に対する最も内側のパケット（ＣＮ）のソース・アドレスへ送信する。
【００８７】
ＭＲ１は、このパケットをＭＲ２　４６０に送信する。
このパケットを受信した場合には、ＭＲ２　４６０は、再帰的にパーズした場合、ＣＮ　ＢＣ内でこのように生成した４つの入力が、ＭＲ１　ＣｏＡ４４２のＩＰヘッダ宛先、および（ＭＲ１　ＨｏＡ４３２、ＭＲ２　ＣｏＡ４８２、ＭＲ２　ＨｏＡ４７２、ＭＮＮＡ４１２）のルーティング・ヘッダを含むＭＮＮ４１０に対してパケットを経路指定するように、ＸＢＵ６０２をＭＮＮに対する最も内側のパケット（ＣＮ）のソース・アドレスに送信する。
【００８８】
本発明の他の実施形態の場合には、ホーム・アドレス試験開始（ＨｏＴＩ）および移動ネットワーク・ノード試験開始（ＭＮＮＴＩ）を結合することができ、結果として得られる試験開始は、ホーム／ＭＮＮ　ＴＩクッキー、ＭＲ　ＨｏＡ１３２およびＭＮＮアドレスを含む。当業者であれば、本明細書に記載するプロセスは、容易にこのような結合試験開始に適応させることができることを理解することができるだろう。
【００８９】
本発明のもう１つの他の実施形態の場合には、ＭＮＮＴＩメッセージは、ＭＲ　ＣｏＡ１４２を介して送信される。
本発明の他の実施形態の場合には、気付けアドレス試験開始（ＣｏＴＩ）および移動ネットワーク・ノード試験開始（ＭＮＮＴＩ）を結合することができる。結果として得られる試験開始は、気付け／ＭＮＮ　ＴＩクッキー、ＭＲ　ＣｏＡ１４２およびＭＮＮアドレスを含む。当業者であれば、本明細書に記載するプロセスは、容易にこのような結合試験開始に適応させることができることを理解することができるだろう。
【００９０】
本発明の上記２つの他の実施形態のいずれの場合でも、ＭＲ　ＣｏＡ１４２を介して送信したＭＮＮＴＩメッセージは、さらにＭＲ　ＨｏＡ１３２を含むことができる。
対応するノード１５０の役割に対する装置は、本明細書に記載する方法による使用のために動作することができる任意のＩＰネットワーク対応可能な装置であってもよい。
【００９１】
移動ルータ１２０の役割を行う装置は、本明細書に記載する方法による使用のために動作することができるもう１つのＩＰネットワーク対応可能な装置と接続することができる、任意のＩＰネットワーク対応可能な装置であってもよい。
【図面の簡単な説明】
【００９２】

【図１】対応するノードと移動ネットワーク・ノードとの間の通信の略図。
【図２】当業者にとって周知のリターン・ルーチング可能性・チェック手順と、本発明のある実施形態による拡張リターンルーチング可能性チェック手順との間の違いを詳細に示す比較プロセス・チャート。
【図３】本発明のある実施形態による拡張バインディング・更新・メッセージに対する移動体・オプションのブロック図。
【図４】本発明のある実施形態による対応するノードと移動ネットワーク・ノードとの間の通信の略図。
【図５】本発明のある実施形態によるデータ・パケットの連続的パーズを詳細に示すブロック図。
【図６】本発明のある実施形態による対応するノードと移動ネットワーク・ノード間の通信の略図。

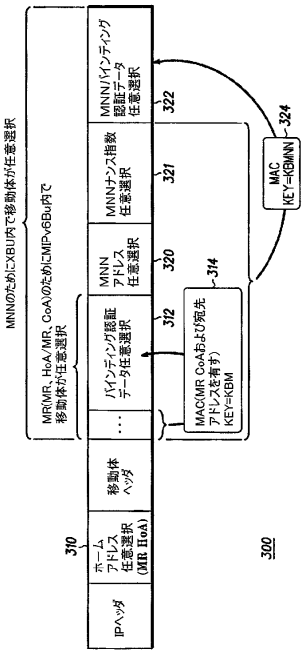
【図１】



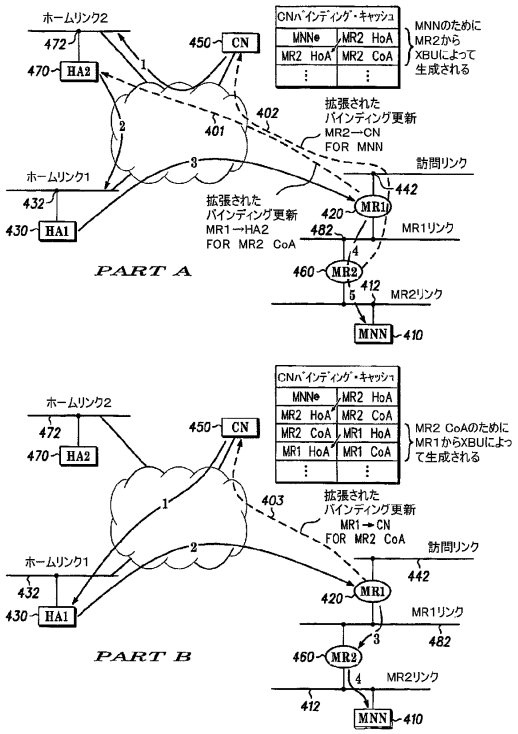
【図２】



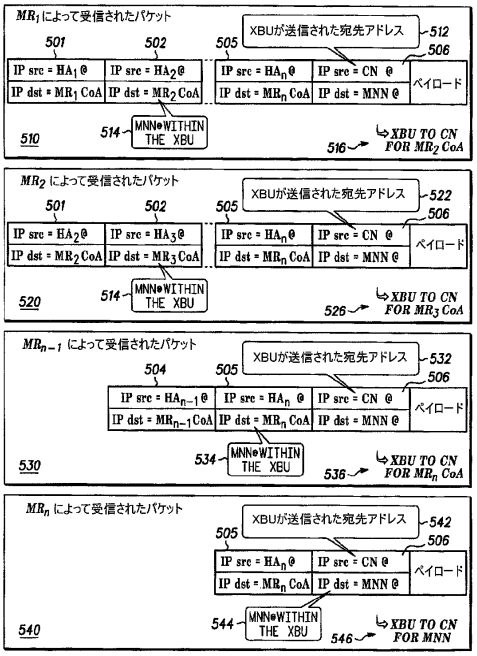
【図３】


MNNのためにXBU内で移動体が任意選択
MR(MR, HoA/MR, CoAへのためにMIPv6Bu内で
移動体が任意選択
MNN/バインディング
認証データ
任意選択
322
MNNナンス指数
任意選択
321
MNN
アドレス
任意選択
320
バインディング認証
データ任意選択
312
…
MAC(MR CoAおよび宛先
アドレス含有;
KEY=KBM
314
MAC
(KEY=KBMN
324
移動体
ヘッダ
ホーム
アドレス
任意選択
(MR HoA)
310
IPヘッダ
300

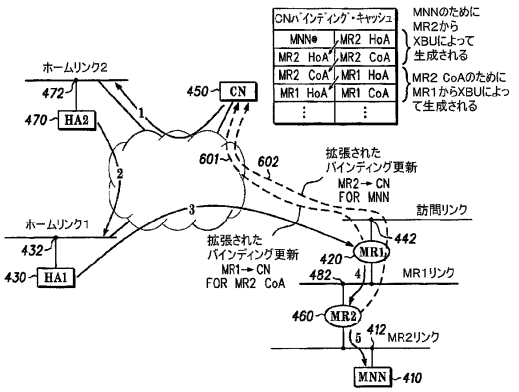
【図４】


ホームリンク2
472
470
HA2
450
CN
CNバインディング・キャッシュ
MNNo
MR2 HoA
MR2 CoA
MNNのために
MR2から
XBUによって
生成される
拡張された
バインディング更新
MR2→CN
FOR MNN
401
402
訪問リンク
ホームリンク1
432
430
HA1
拡張された
バインディング更新
MR1→HA2
FOR MR2 CoA
442
420
MR1
MR1リンク
482
460
MR2
412
MR2リンク
MNN
410
PART A
MR1 HoA
MR1 CoA
MR2 CoAのために
MR1からXBUによって
生成される
403
拡張された
バインディング更新
MR1→CN
FOR MR2 CoA
PART B

【図５】


MR1によって受信されたパケット
501
502
505
XBUが送信された宛先アドレス
512
506
IP src = HA1@
IP src = HA2@
IP src = HAn@
IP src = CN @
IP dst = MR1 CoA
IP dst = MR2 CoA
IP dst = MRn CoA
IP dst = MNN @
ペイロード
510
514
MNNoWITHIN
THE XBU
516
XBU TO CN
FOR MR2 CoA
MR2によって受信されたパケット
IP src = HA2@
IP src = HA3@
IP dst = MR2 CoA
IP dst = MR3 CoA
522
520
526
XBU TO CN
FOR MR3 CoA
MRn-1によって受信されたパケット
504
IP src = HAn-1@
IP dst = MRn-1CoA
532
530
534
536
XBU TO CN
FOR MRn CoA
MRnによって受信されたパケット
542
540
544
546
XBU TO CN
FOR MNN

【図６】


ホームリンク2
472
470
HA2
450
CN
CNバインディング・キャッシュ
MNNo
MR2 HoA
MR2 CoA
MR1 HoA
MR1 CoA
MNNのために
MR2から
XBUによって
生成される
MR2 CoAのために
MR1からXBUによって
生成される
601
602
拡張された
バインディング更新
MR2→CN
FOR MNN
訪問リンク
ホームリンク1
432
430
HA1
拡張された
バインディング更新
MR1→CN
FOR MR2 CoA
442
420
MR1
MR1リンク
482
460
MR2
412
MR2リンク
MNN
410

フロントページの続き

(51)Int.Cl. F I
H04L 12/22 (2006.01) H04L 12/22

(72)発明者 ジャンヌトー、クリストフ
フランス国 Ｆ－７８３９０ ボワ ダルシー リュ オーギュスト ルノワール １０
(72)発明者 ペトレスキュ、アレクサンドリュ
フランス国 Ｆ－９１４００ オルセー リュ シャルル ド ゴール ４３

審査官 衣鳩 文彦

(56)参考文献 特開２００４－２８２７５１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl., ＤＢ名)
H04W 12/00
H04W 36/08
H04W 40/34
H04L 12/00