

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2012-182845

(P2012-182845A)

(43) 公開日 平成24年9月20日(2012.9.20)

(51) Int.Cl.	F I	テーマコード (参考)
H04W 8/26 (2009.01)	H04Q 7/00 161	5K067
H04W 36/14 (2009.01)	H04Q 7/00 309	
H04W 48/18 (2009.01)	H04Q 7/00 410	

審査請求 有 請求項の数 20 O L (全 26 頁)

(21) 出願番号	特願2012-134716 (P2012-134716)	(71) 出願人	504424708
(22) 出願日	平成24年6月14日 (2012.6.14)		シムトーン・コーポレーション
(62) 分割の表示	特願2008-518448 (P2008-518448) の分割		SIMTONE CORPORATION
原出願日	平成18年6月23日 (2006.6.23)		アメリカ合衆国 27713 ノースカロ
(31) 優先権主張番号	60/693,552		ライナ州 ダラム メリディアン パーク
(32) 優先日	平成17年6月23日 (2005.6.23)	(74) 代理人	100068755
(33) 優先権主張国	米国 (US)		弁理士 恩田 博宣
		(74) 代理人	100105957
			弁理士 恩田 誠
		(74) 代理人	100142907
			弁理士 本田 淳

最終頁に続く

(54) 【発明の名称】 モバイル機器に対するネットワークアドレス変更のための方法及び装置

(57) 【要約】

【課題】流動性が高い環境で通信を処理するように適応されたモビリティネットワークを提供すること

【解決手段】ネットワークアドレス変更を実行できるシステム(100)は、モバイル機器(120)と、第1のホスト(110)と、モバイルハンドラ(130)とを備える。モバイルハンドラ(130)はモバイル機器(120)から、ネットワーク(150)上のモバイル機器(120)の第2のネットワーク位置に対応する第2のネットワークアドレスを含むアドレス変更要求を受け取るように構成され、モバイルハンドラ(130)はアドレス変更要求を第1のホスト(110)に通知するように構成され、通知は第2のネットワークアドレスを含み、第1のホスト(110)は該通知を受け取り、第2のネットワークアドレスでモバイル機器(120)との接続を開始するように適応され、接続の通信経路はモバイルハンドラ(130)を含まない。

【選択図】 図1A



【特許請求の範囲】

【請求項 1】

第 1 のネットワークアドレスでネットワークに接続されているモバイル機器の第 1 のネットワークアドレスを変更するための方法であって、該モバイル機器は該ネットワークを介したホストへの接続を有し、ネットワークアドレスの該変更は、該ネットワークを介してモバイルクライアントと該ホストとの両方に接続されているモバイルハンドラによって処理される方法であって、

該モバイル機器から該モバイルハンドラに、第 2 のネットワークアドレスを含むアドレス変更要求を送信する動作と、

該モバイルハンドラから該ホストに、該第 2 のネットワークアドレスを含む該アドレス変更要求を提供する動作と、

該モバイルクライアントと通信する際に該第 2 のネットワークアドレスを使用するために、該ホストと該モバイルクライアントとの間の接続を、該ホストによって修正する動作と、

該修正された接続を介して該ホストと該モバイルクライアントとの間で通信する動作とを備え、該修正された接続の通信経路が該モバイルハンドラを含まない、方法。

【請求項 2】

該ネットワークが第 1 のネットワークと第 2 のネットワークとを含み、

該モバイル機器によって該第 1 のネットワークから該第 2 のネットワークにローミングする動作

をさらに備え、該第 2 のネットワークアドレスが該第 2 のネットワークの該モバイル機器の位置に対応する、請求項 1 に記載の方法。

【請求項 3】

該アドレス変更要求を送信する動作の前に、

該モバイル機器によって該モバイルハンドラに、該第 1 のネットワークアドレスを含む接続要求を送信する動作と、

該モバイルハンドラによって該ホストに対し、該モバイル機器の該第 1 のネットワークアドレスを含む、該接続要求の通知を提供する動作と、

該ホストによって開始される接続を、該ホストと該第 1 のネットワークアドレスにある該モバイル機器との間で確立する動作と、

をさらに備え、

該接続上の通信経路が該モバイルハンドラを含まない、請求項 2 に記載の方法。

【請求項 4】

該アドレス変更要求を該送信する動作が、識別子を含む該アドレスの変更を送信する動作を含む、該モバイルハンドラによって該モバイル機器に、該モバイルハンドラに対して該モバイル機器を識別する識別子を提供する動作と、

該モバイルハンドラによって、少なくとも部分的に該識別子に基づいて該モバイル機器を認証する動作と

をさらに備える、請求項 3 に記載の方法。

【請求項 5】

該ホストがローカルエリアネットワーク（LAN）に接続されている第 1 のサーバであって、該ネットワークから受信したネットワークアドレスを、該 LAN 上の少なくとも 1 台のサーバの位置に対応するプライベートネットワークアドレスに変換する NAT テーブルを有するネットワークアドレス変換（NAT）ルータにより、該 LAN は該ネットワークからの接続が制限され、該第 1 のサーバの該プライベートネットワークアドレスが該モバイルクライアントにとって未知である、請求項 1 に記載の方法。

【請求項 6】

該ホストと該モバイルクライアントとの間の該接続を修正する該動作が、該第 2 のネットワークアドレスから受信される通信が該第 1 のサーバに送られるように該 NAT テーブル

10

20

30

40

50

を更新する動作を含む、請求項 5 に記載の方法。

【請求項 7】

ネットワークアドレス変更を実行できるシステムであって、

複数のホストを相互接続するネットワークと、

該ネットワークに接続されており、該ネットワーク上のモバイル機器の第 1 のネットワーク位置に対応する第 1 のネットワークアドレスに関連付けられる該モバイル機器と、

該ネットワークに接続されている第 1 のホストと、

該ネットワーク上で該モバイル機器と該ホストと通信できるモバイルハンドラと、
を備え、

該モバイルハンドラが該モバイル機器から、該ネットワークの該モバイル機器の第 2 のネットワーク位置に対応する第 2 のネットワークアドレスを含むアドレス変更要求を受信するように構成され、該モバイルハンドラが該アドレス変更要求を該第 1 のホストに通知するように構成され、該通知が該第 2 のネットワークアドレスを含み、

該第 1 のホストが該通知を受け取り、該第 2 のネットワークアドレスで該モバイル機器との接続を開始するように適応され、該接続の通信経路が該モバイルハンドラを含まない、システム。

【請求項 8】

該ネットワークが少なくとも第 1 のネットワークと第 2 のネットワークとを備え、該モバイル機器が該第 1 のネットワークと該第 2 のネットワークとのどちらか一方に接続することができ、該モバイル機器が該第 1 のネットワークから該第 2 のネットワークにローミングするとき、該モバイル機器が該アドレス変更要求を送信するように構成され、該第 1 のネットワーク位置が該第 1 のネットワークと関連し、該第 2 のネットワーク位置が該第 2 のネットワークに関連する、請求項 7 に記載のシステム。

【請求項 9】

該モバイルハンドラが、該ホストに接続するために該モバイル機器から接続要求を受け取るように構成され、該接続要求を受信することに応じて、該モバイルハンドラが、少なくとも一時的に該モバイル機器を識別するために該モバイル機器に識別子を提供する、請求項 7 に記載のシステム。

【請求項 10】

該モバイル機器は、該アドレス変更要求の一部として該識別子を含むように構成され、該モバイルハンドラは少なくとも部分的に該識別子に基づいて該モバイル機器を認証するように構成される、請求項 9 に記載のシステム。

【請求項 11】

該モバイルハンドラが、該モバイル機器が認証されて初めて該アドレス変更要求を該ホストに通知するように構成される、請求項 10 に記載のシステム。

【請求項 12】

該モバイルハンドラが、該接続要求を該ホストに通知し、該モバイル機器の該第 1 のネットワークアドレスを該ホストに提供するように構成される、請求項 9 に記載のシステム。

【請求項 13】

該第 1 のホストがファイアウォールの背後に位置するプライベートローカルエリアネットワーク (LAN) に接続され、該第 1 のホストが該モバイル機器にとって未知である該 LAN 上のプライベートネットワークアドレスを有し、該ホストが該モバイルハンドラによって提供される該第 1 のネットワークアドレスを使用して該モバイル機器との接続を開始するように構成される、請求項 12 に記載のシステム。

【請求項 14】

ネットワークアドレス変換 (NAT) ルータをさらに備え、該 NAT ルータがファイアウォールの一部であり、該ネットワークから受信されたネットワークアドレスを、該プライベート LAN のそれぞれのプライベートアドレスに変換する NAT テーブルを、該 NAT ルータが含む、請求項 13 に記載のシステム。

【請求項 15】

該第 1 のホストが、該第 1 のネットワークアドレスにある該モバイル機器との接続を開始すると、該第 1 のホストと関連する仮ネットワークアドレスを発行し、該モバイル機器が該 N A T ルータを介して該第 1 のホストと通信できるように、該 N A T ルータが、該 N A T テーブルにおいて該仮ネットワークアドレスを該第 1 のホストの該プライベートネットワークアドレスに関連付ける、請求項 1 4 に記載のシステム。

【請求項 1 6】

該モバイル機器がステートレスデバイスであり、起動時に自動的に接続要求を提供するように構成される、請求項 9 に記載のシステム。

【請求項 1 7】

ネットワークでホストへの接続を有するモバイル機器の第 1 のネットワークアドレスの変更を容易にするためのネットワークデバイスであって、該接続が該モバイル機器の第 1 のネットワークアドレスを使用し、

該ネットワークデバイスが該ネットワークに接続できるようにするための少なくとも 1 つのネットワークポートと、

該少なくとも 1 つのネットワークポートに接続されており、該モバイル機器から該少なくとも 1 つのネットワークポートで受信された、第 2 のネットワークアドレスを含むアドレス変更要求を処理するように適応され、該ホストに該アドレス変更要求を通知するために該ホストに少なくとも該第 2 のネットワークアドレスを送信するようにさらに適応されたコントローラと、

を備え、

該第 2 のネットワークアドレスで確立された接続での該ホストと該モバイル機器との間の以後の通信が、該ネットワークデバイスを含まない通信経路介して行われる、ネットワークデバイス。

【請求項 1 8】

該コントローラが、該アドレス変更要求から、該モバイル機器の信頼性を検証する認証部分を含む、請求項 1 7 に記載のネットワークデバイス。

【請求項 1 9】

第 1 のコントローラが、該モバイル機器から該少なくとも 1 つのネットワークポートで受信された接続要求を処理するように適応され、該接続要求が該モバイル機器の該第 1 のネットワークアドレスを含み、該第 1 のコントローラが、該接続要求の受信に応じて、少なくとも該第 1 のネットワークアドレスを該ホストに送信し、

該第 1 のアドレスで確立される接続での該ホストと該モバイル機器との間の以後の通信が、該ネットワークデバイスを含まない通信経路を介して行われる、請求項 1 8 に記載のネットワークデバイス。

【請求項 2 0】

該コントローラが、該接続要求に応じて、識別子を生成し、該識別子を該モバイル機器に送信し、該アドレス変更要求が該識別子を含み、該認証部分が少なくとも部分的に該識別子に基づいて該モバイル機器の該信頼性を検証する、請求項 1 9 に記載のネットワークデバイス。

【発明の詳細な説明】

【技術分野】

【0 0 0 1】

本発明はコンピュータネットワーク化に関し、さらに詳細には、モバイル機器が、例えば接続損失、ローミング、貸し出し期限終了等に起因してそのネットワークアドレスを変更することがあるネットワークに接続されているモバイル機器に関する。

(関連出願の相互参照)

本願は、全体として参照することによって本明細書に組み込まれている、2 0 0 5 年 6 月 2 3 日に出願された「信頼できる第三者機関を使用するモバイルホスト向けの安全でスケラブルな I P ネットワークアドレス変更方式 (S e c u r e a n d S c a l a b l e I P N e t w o r k A d d r e s s C h a n g e S c h e m e f o r

10

20

30

40

50

Mobile Hosts Using a Trusted Third Party)」と題される米国仮出願、出願番号第60/693552号に対して米国特許法第119(e)条の元で優先権を主張する。

【背景技術】

【0002】

無線ネットワーク技術が拡散され、これらの技術に基づく高速ネットワークの費用が低減するのに伴い、さらに多くのコンピュータデバイスが無線接続上でネットワークに接続されるようになってきている。無線技術が提供する柔軟性により、パーソナルコンピュータ（PC）、携帯電話、パーソナルデスクトップアシスタント（PDA）、及び他の携帯コンピュータデバイスを多くの異なる位置で操作することができる。

10

【先行技術文献】

【特許文献】

【0003】

【特許文献1】米国特許出願公開第10/328,660号

【特許文献2】米国特許出願公開第11/104,982号

【発明の概要】

【発明が解決しようとする課題】

【0004】

通常は恒久的または半恒久的に単一の位置と関連付けられ、多くの場合はその位置で静的に割り当てられたネットワークアドレスを有する従来の有線コンピュータデバイスとは対照的に、モバイル機器は、それが位置から位置へ変化するにつれて新しいネットワークアドレスを必要とする。つまり、モバイル機器が動作するさまざまな位置が、モバイル機器の位置を正確に突き止めるために用いるさまざまなネットワークアドレスを必要とする。例えば、異なるサービスプロバイダによって運用されるネットワークは、モバイル機器がある特定のネットワークに接続されている一方で、そのネットワークアドレスを変更することを要求する。したがって、無線モデルでは、モバイル機器は、それが使用される無線位置ごとに別のネットワークアドレスを割り当てられる。流動性の高い環境では、モバイル機器はネットワークからネットワークへローミングすることが可能であり、このようにしてネットワークアドレス変更が必要とされるときに、特に装置が現在1つまたは複数のネットワークデバイスと通信しているときに動的に実行される必要のあるネットワークアドレス変更を必要とする。

20

30

【0005】

モバイル機器によって接続されている無線ネットワークにおけるネットワークアドレス変更の問題を解決するために、伝送制御プロトコル（TCP）／インターネットプロトコル（IP）を使用してモバイル機器をサポートする一般的な解決策は、インターネットプロトコルバージョン4（IPv4）の元での移動性のためのインターネット規格を提案するインターネットエンジニアリングタスクフォースが発行するリクエストフォーコメント（RFC）2002、3220、及び3344に説明されている。この方式では、各モバイル機器はホームネットワークとして知られているものと関連付けられている。モバイル機器がホストとのエンドツーエンド通信に関与しているとき、たとえモバイル機器が本明細書では外来ネットワーク（例えば、ホームネットワークのプロバイダとは異なるプロバイダによってサービスを提供されているネットワーク）と呼ばれている別のネットワークに移動しても、ホストはつねにモバイル機器のホームネットワークに関連付けられたアドレスでモバイル機器と通信している。

40

【0006】

モバイル機器がそのホームネットワークの範囲内に位置するときには、ホストとモバイル機器との間のデータグラム（例えば、ネットワークパケット）のルーティングは通常のIPルーティングに従って機能する。例えば、IPv4では、ネットワークアドレスは、ネットワーク識別子部分とホスト識別子部分に分割される32ビットのバイナリデータを備える。ネットワーク識別子及びホスト識別子は、さまざまな数の32ビットアドレスを

50

使用する。ホスト識別子部分のために使用されるビットの数が多いほど、関連ネットワークに接続できるホストの数も多くなる。ネットワークホストはローカルネットワークに接続され、そのネットワーク上で自身を一意に識別するためにそれらのホスト識別子部分を使用する。ネットワーク識別子部分は、あるネットワークを別のネットワークから区別する。ネットワークは通常ルータと呼ばれている1台または複数の装置を介して相互接続されている。

【0007】

したがって、1つまたは複数のネットワークパケットがモバイル機器とそのホームネットワーク上のホストの間で交換されると、ネットワークパケットはそれぞれのネットワークアドレスのホスト識別子部分を使用して直接的に送られる。ネットワークパケットは、例えばモバイル装置及び／またはモバイル装置が接続されているホスト等の宛先ホストのデータリンク層に直接的に送信される。

10

【0008】

モバイル機器が外来ネットワーク（つまり、そのホームネットワーク以外の任意のネットワーク）に位置するとき、ホームネットワークはネットワークパケットまたはデータグラムを、モバイル機器が現在位置しているネットワークに転送する。ホームネットワークは、ホスト及びホストとホームネットワーク間に位置するルータに実質的に気付かれないようにこの転送動作を実行する。データパケットのリダイレクトは、さらに詳しく後に記載されるようにホストから下流で発生するために、特に、モバイル機器と通信しているホストはネットワークアドレスの変更に気付かない場合がある。モバイル機器がそのホームネットワークの外部に位置しているとき、それは外来ネットワークで、ホームネットワークがモバイル機器宛てのあらゆるパケットを転送する先の気付アドレスを与えられる。この気付アドレスは外来ネットワーク内での滞在期間中のモバイル機器の仮アドレスである。

20

【0009】

モバイル機器がそのホームネットワークからローミングできるようにするために、ホームネットワークは、モバイル機器が外来ネットワークに位置するとき、それに対してパケットを転送することに関与するホームエージェントとして知られている特殊なルータを提供しなければならない。モバイル機器が接続される、及び／または位置する各外来ネットワークでは、通常、外来エージェントとして知られている特殊なルータがモバイル機器の代わりに働くために存在している。外来エージェントは、例えば、外来ネットワークにおけるモバイル機器のデフォルトのルータとして動作する。いくつかの例では、ホームエージェントとして知られている気付アドレスは外来エージェントのネットワークアドレスである。外来エージェントは、ホームエージェントからネットワークパケットを受信すると、ネットワークパケットをモバイル機器に転送する。したがって、ホームエージェントと外来エージェント（総称的にモビリティエージェントと呼ばれている）は、ネットワークアドレスの変更に気付いているが、ホームエージェントと外来エージェントがそれぞれ旧ネットワークアドレスと新ネットワークアドレスのためのプロキシとして動作するので、ホスト及び他のルータは気付いていない。

30

【0010】

このフレームワークは、拡張である移動性サポートを使わずにIPv4で実質的な問題を克服する。特に複数のネットワークが関与するとき、ルータは、宛先ネットワークを検出するために、ネットワークに入ってきたパケットがどこに送信されなければならないのかを記述するルーティングテーブルを維持する。ルータは、多様なルーティングプロトコルを使用し、ネットワークホップルーティングとして知られているプロセスを通してさまざまなネットワークに到達する方法についての情報を交換し、互いに協力する。

40

【0011】

これらのルーティングプロトコルは、ホスト発見ではなく、ネットワークルーティング発見に関係する。IPv4アドレス空間は、すべてのホストのために個々のルートを維持することをひどく高価且つ非効率にするほど十分に広い。さらに、IPv4アドレスは非

50

常に緊密にネットワーク識別子とホスト識別子を結合し、且つ既定のネットワークで利用できるホスト識別子の数はネットワークごとに変化するため、そのホスト識別子を維持する一方で、アドレスのクライアント変更をネットワーク識別変更として伝達できるようにする方法を考案できない可能性がある。前述された携帯電話ネットワークの拡張がこの問題を解決する。

【0012】

モバイル機器は、通常、エージェント通知を通して外来エージェントの位置を突き止め、識別する。エージェント発見と呼ばれているこのプロセスは、モビリティエージェントが、モビリティエージェントがサービスを提供するネットワーク全体で、周期的に自分達のサービスをブロードキャストすることを伴う。モビリティエージェントは、エージェントが動作するネットワークにとって局所的なその通知をブロードキャストするので、モバイル機器は、それがそのホームネットワーク内にあるのか、あるいは外来ネットワーク内にあるのかを決定するだけではなく、モバイル機器がそのホームネットワークを離れたとそれが判断するとき外来エージェントの位置を突き止めることもできる。モバイル機器が、それが外来ネットワーク内にあることを発見し、外来エージェントの位置を突き止めると、モバイル機器は、モバイル機器向けのネットワークパケットの転送を可能にする通信経路を登録し、確立するためにそのホームエージェントに気付アドレス（例えば、通知から取得される外来エージェントのネットワークアドレス）を転送する。

【課題を解決するための手段】

【0013】

本発明の一実施形態は、第1のネットワークアドレスでネットワークに接続されているモバイル機器の第1のネットワークアドレスを変更するための方法を含み、モバイル機器はネットワーク上でホストに対する接続を有し、ネットワークアドレスに対する変更は、モバイルクライアントとホストとの両方にネットワークを介して接続されているモバイルハンドラによって処理されている。方法は、モバイル機器からモバイルハンドラに、第2のネットワークアドレスを含むアドレス要求の変更を送信する動作と、モバイルハンドラからホストに、第2のネットワークアドレスを含むアドレス要求の変更の通知を提供する動作と、モバイルクライアントと通信する際に第2のネットワークアドレスを使用するために、ホストによってホストとモバイルクライアントの間の接続を修正する動作と、修正された接続の上のホストとモバイルクライアントの間で通信する動作とを備え、修正された接続の通信経路はモバイルハンドラを含まない。

【0014】

本発明の別の実施形態は、ネットワークアドレス変更を実行できるシステムを含み、システムは複数のホストを相互接続するネットワークと、ネットワークに接続されており、ネットワーク上のモバイル機器の第1のネットワーク位置に対応する第1のネットワークアドレスに関連付けられたモバイル機器と、ネットワークに接続されている第1のホストと、モバイル機器とネットワーク上のホストと通信できるモバイルハンドラとを備える。ここではモバイルハンドラはモバイル機器から、ネットワークにおけるモバイル機器の第2のネットワーク位置に対応する第2のネットワークアドレスを含むアドレス変更要求を受け取るように構成され、モバイルハンドラはアドレス変更要求を第1のホストに通知するように構成され、通知は第2のネットワークアドレスを含み、第1のホストは通知を受け取り、第2のネットワークアドレスでモバイル機器との接続を開始するように適応され、接続の通信経路はモバイルハンドラを含まない。本発明の別の実施形態はネットワーク上でホストに対する接続を有するモバイル装置の第1のネットワークアドレスの変更を容易にするためのネットワークデバイスを含み、接続はモバイル機器のための第1のネットワークアドレスを使用し、ネットワークデバイスは、ネットワークデバイスをネットワークに接続できるようにするために少なくとも1つのネットワークポートと、少なくとも1つのネットワークポートに接続されるコントローラとを備え、コントローラはモバイル機器から少なくとも1つのネットワークポートで受け取られる、第2のネットワークアドレスを含むアドレス変更要求を処理するように適応され、コントローラはホストにアド

レス変更要求を通知するためにホストに少なくとも第2のネットワークアドレスを送信するようにさらに適応されている。ここでは第2のネットワークアドレスで確立された接続でのホストとモバイル機器との間の以後の通信は、ネットワークデバイスを含まない通信経路を介して行われる。

【図面の簡単な説明】

【0015】

【図1A】本発明の一実施形態に従ってモビリティデバイスのためのネットワークアドレスの変更を容易にするモビリティネットワークを実現するためのシステムを示す。

【図1B】本発明の一実施形態に従ってモビリティデバイスのためのネットワークアドレスの変更を容易にするモビリティネットワークを実現するためのシステムを示す。

【図1C】本発明の一実施形態に従ってモビリティデバイスのためのネットワークアドレスの変更を容易にするモビリティネットワークを実現するためのシステムを示す。

【図1D】本発明の一実施形態に従ってモビリティデバイスのためのネットワークアドレスの変更を容易にするモビリティネットワークを実現するためのシステムを示す。

【図1E】本発明の一実施形態に従ってモビリティデバイスのためのネットワークアドレスの変更を容易にするモビリティネットワークを実現するためのシステムを示す。

【図1F】本発明の一実施形態に従ってモビリティデバイスのためのネットワークアドレスの変更を容易にするモビリティネットワークを実現するためのシステムを示す。

【図1G】本発明の一実施形態に従ってモビリティデバイスのためのネットワークアドレスの変更を容易にするモビリティネットワークを実現するためのシステムを示す。

【図1H】本発明の一実施形態に従ってモビリティデバイスのためのネットワークアドレスの変更を容易にするモビリティネットワークを実現するためのシステムを示す。

【図1I】本発明の一実施形態に従ってモビリティデバイスのためのネットワークアドレスの変更を容易にするモビリティネットワークを実現するためのシステムを示す。

【図2A】本発明の別の実施形態に従って、ファイアウォールの背後に位置するサーバと通信するモバイル機器のためにネットワークアドレス変更を容易にするモビリティネットワークを実現するためのシステムを示す。

【図2B】本発明の別の実施形態に従って、ファイアウォールの背後に位置するサーバと通信するモバイル機器のためにネットワークアドレス変更を容易にするモビリティネットワークを実現するためのシステムを示す。

【図2C】本発明の別の実施形態に従って、ファイアウォールの背後に位置するサーバと通信するモバイル機器のためにネットワークアドレス変更を容易にするモビリティネットワークを実現するためのシステムを示す。

【図3A】本発明の別の実施形態に従ってモバイルステートレスデバイスのためのネットワークアドレスの変更を容易にするモビリティネットワークを実現するためのシステムを示す。

【図3B】本発明の別の実施形態に従ってモバイルステートレスデバイスのためのネットワークアドレスの変更を容易にするモビリティネットワークを実現するためのシステムを示す。

【図3C】本発明の別の実施形態に従ってモバイルステートレスデバイスのためのネットワークアドレスの変更を容易にするモビリティネットワークを実現するためのシステムを示す。

【図3D】本発明の別の実施形態に従ってモバイルステートレスデバイスのためのネットワークアドレスの変更を容易にするモビリティネットワークを実現するためのシステムを示す。

【発明を実施するための形態】

【0016】

前に記載されたように、従来の装置の移動性は、各携帯電話ネットワークに、モバイル機器の代わりに動作するホームエージェントを有するホームネットワークが割り当てられるフレームワークを介して達成される。加えて、モバイル機器は、モバイル機器が、ホー

10

20

30

40

50

ムエージェントから受信される通信を外来ネットワーク上のその位置でモバイル機器に転送するプロキシとして動作するためにローミングしてよい各外来ネットワーク内の外来エージェントを必要とする。出願人は、ネットワーク移動性に対する従来の解決策に多くの欠点があることを認識している。

【0017】

特に、モバイル機器が指定されたホームネットワークを有するという要件は融通が利かないことがある。ホームネットワークフレームワークは、モバイル機器がその指定されたホームネットワーク内に通常位置することを前提としてモデル化されている。ネットワーク移動性及びネットワーク間ローミングがますます普及し、当たり前になるにつれ、ある特定のモバイル機器にとってどのネットワークがホームネットワークと考えられなければならないのかが明確ではなく、フレームワークを管理及び使用することを難しくしている。

10

【0018】

加えて、ネットワークパケット（例えば、データグラム）のホームネットワークを介したルーティングは非効率的である。特に、エンドツーエンド通信に参与している既定のホストとモバイル機器は互いにさらに近くなることがあり、ネットワークの観点から、それらは指定されたホームネットワークにさらに近くなる。したがってホストとモバイルクライアント間で交換されるネットワークパケットは、ホームエージェントを介してホームネットワークを通して非効率的に経路が再選択されなければならない可能性がある。これはネットワーク移動性の解決策のスケラビリティに悪影響を及ぼす。例えば、モバイル機器の数が増加するにつれ、従来のフレームワークの要件によってもたらされる非効率がネットワーク帯域幅にマイナスの影響を及ぼす。ホームエージェントと外来エージェントを通してデータパケットを送ることは、多大且つ不必要なネットワークトラフィックを生じさせる可能性があり、非効率的なルーティングはエンドポイント間で不必要な待ち時間を生じさせ、このようにして伝送の質に悪影響を及ぼす。

20

【0019】

モビリティエージェント（つまりホームエージェントと外来エージェント）の実施には、通知を提供し、登録を承認し、多様な転送機能を実行し、及び／またはモバイル機器の代わりに他のプロキシサービスを処理するように構成された追加のルータ及び特殊ルータが必要になる。この追加のネットワークインフラストラクチャは、ホームネットワーク内で、及びモバイル機器がローミングすることが期待されるあらゆる外来ネットワーク上で配備されなければならない、広く行き渡った高移動性のネットワークの実現を費用のかかるものにし、管理、維持を高価にする。例えば、ネットワークローミングは、前に記載されたモビリティエージェントフレームワークを実現し、モビリティエージェントフレームワークに準拠するネットワークに制限される。

30

【0020】

前に記載された従来のネットワークモビリティ技法の適用性をさらに制限するために、現在の解決策はIPネットワークの実施の拡張部分として策定され、このようにしてこれらの技法が実現されるネットワークのタイプを制限している。モバイル機器が非IPベースのネットワークにアクセスする、及び／または（定義により、IPをベースにしていなければならない）そのホームネットワークの外部からだけしかアクセスできないネットワークに接続することを希望する場合がある。あらゆる接続側ネットワークがIPをベースにしていらない場合、モバイルクライアントは、少なくとも準拠したIPをベースにしたネットワーク上で接続されているホストと同時に通信している間にはなく、それらのネットワークにローミングすることはできない。ホームネットワークと、モバイル機器が接続する可能性のある任意の外来ネットワークの両方ともがIPをベースにしているという要件は、モバイル機器のためのネットワークの可用性を削減する。

40

【0021】

前に記載されたように、モバイル機器がローミングしているとき、モバイル機器は新規に参入したネットワークのための新しいネットワークアドレスを要求する、あるいは割り

50

当てられる必要がある。従来のモビリティネットワークでは、これは外来エージェントからの通知に応答すること、またはそれ以外には外来エージェントの支援を要請し、（例えば、ホームエージェントを介して）ホームネットワークに新しいアドレスを登録することを伴う。装置が単に外来ネットワークに接続しているだけではなく、1つまたは複数のネットワーク化されたホストと通信しているのと同時にローミングしているときに状況は複雑になる。これらの例では、現在モバイル機器と通信しているホストは、以前のモバイル機器のネットワークアドレスにパケットを送信し続けるであろう。

【0022】

ホストまたはモバイル機器及び／またはホストの代わりに働くルータのような何らかの他の装置のどちらかが、好ましくはホストとモバイル機器の間の接続を停止、再確立／再開し、且つ／またはすでに実行された認証プロセスを繰り返す必要なく新しいアドレスへの通信のリダイレクトを可能にするためには、モバイル装置のアドレスの変更を知らされなければならない。その結果として、従来のアドレス変更手順はセキュリティ違反を受けやすい。例えば、悪意のあるネットワークデバイスが、ホスト（複数の場合がある）がまだ以前のアドレスにパケットを送信している時間的間隔の間に、及び／または悪意のあるネットワークデバイスへの通信をリダイレクトするためにアドレス変更手順を偽造することによって、ホスト（複数の場合がある）とモバイル機器間の通信をハイジャックしようと試みることがある。

【0023】

出願人は、前記欠点の1つまたは複数が、モバイル機器がおそらく相対的に頻繁にネットワークアドレスの変更を必要とする可能性がある流動性が高い環境で通信を処理するように適応されたモビリティネットワークを実現することによって排除できると認識している。例えば、一実施形態では、2002年12月23日に出願された「汎用ステレスデジタルサービス及びコンピューティングサービスをプロビジョニングするためのシステム及び方法（System and Method for Provisioning Universal Stateless Digital and Computing Services）」と題される特許文献1（第‘660号）に説明されているネットワークアーキテクチャは、モバイル機器がパケット指向型の信頼できないネットワーク上での別のホストコンピュータとのすでに確立されているエンドツーエンド通信に関与し、ネットワークアドレス変更を通して通信を維持する一方で、モバイル機器が自動的に、安全に、スムーズに、及び動的にそのネットワークアドレスを変更できるようにモビリティデバイスの移動性を促進するためのモデルとして使用される。第‘660号出願は、全体として参照することにより本明細書に組み込まれている。

【0024】

一実施形態では、ホストとモバイル機器の両方ともがモバイルハンドラ（MH）と呼ばれているサードパーティデバイスに接続されている、あるいは接続できるように構成されている。一般的には、MHはモバイル機器とホストの両方に信頼されている。例えば、ホストはMHからの通信を認識し、情報が悪意のあるネットワークデバイスから送信されなかったことを信用してよい。モバイル機器とホストは、モバイル機器を認証し、モバイル機器のためのネットワークアドレス変更を実行し、このようにしてホストが新しいネットワークアドレスでモバイル機器と通信できるようにするために情報を交換するためにMHと通信する。ネットワークアドレスの変更は、例えばモバイル機器が別のネットワークの間でローミングした、及び／または別のネットワークに接続した結果生じるネットワークハンドオーバー、及び／または現在のネットワークとの接続の損失が発生した場合等、多数の理由のどれかについて発生する。

【0025】

以下は本発明による方法及び装置に関連する多様な概念、及び本発明による方法及び装置の実施形態のさらに詳細な説明である。本書に説明されている多様な態様が多数の方法のどれかで実現されてよいことが理解される必要がある。特定の実施の例は説明のためだけに本書に示されている。本発明の態様は任意の特定のタイプのネットワーク、ネットワ

10

20

30

40

50

ーク構成、及び／またはネットワークデバイスに制限されないので、特に、多様なネットワーク、ネットワークプロトコル等のどれかを使用する多様なネットワークの実装及び構成のどれかが使用される。

【0026】

図1は、本発明の一実施形態によるモビリティネットワークを実現するためのシステムを示している。システム100は、ルータ115を介して信頼できないネットワーク（例えば、インターネット）に接続されているホスト110を含んでいる。システム100は、ルータ125を介して信頼できないネットワーク150に接続されているモバイル機器120も含んでいる。モバイル機器120は無線リンクを介してネットワーク150に接続してよい。例えば、ルータ125はモバイル機器をネットワーク150に無線で接続する1つまたは複数の無線アクセスポイントを含む。モバイル装置120はホスト110にとって未知であり、ホスト110によって信用されないことがある。しかしながら、モバイル機器120は既知であるか、信用されているか、あるいは両方の可能性があるので、これは本発明の態様に対する制限ではない。システム100は、信用できないネットワーク150に接続されており、モバイル機器120とホスト110間に通信リンクを確立することを容易にするMH130も含む。ホスト及び／またはMHは無線リンクを介してネットワーク150にも接続される。

10

【0027】

ネットワーク150が、任意のタイプ及び構成の多数のネットワークを含んでよいことが理解される必要がある。例えば、ネットワーク150は、各ネットワークがネットワークに接続されている多様なネットワークデバイスによって発行されるネットワークアドレスの別のネットワーク識別子部分によって特定される多数のネットワークを含む。本発明の態様はこの点に制限されていないので、ネットワーク150は1つまたは複数のプライベートネットワーク、ローカルエリアネットワーク（LAN）、広域ネットワーク（WAN）、インターネット等を含んでよい。ネットワーク150は、さまざまなネットワーク間でネットワークトラフィックを導き、ネットワークに接続されているモバイル機器によるローミングを容易にする1台または複数の協調するルータを含む。

20

【0028】

一般的に、MH130はホスト110に既知であり、ホスト110によって信用されており、それによってMHがホストに情報を通信できる信用できるリンクをホストと確立させる。例えば、ホストは、トランスポート制御プロトコル（TCP）接続を介して、あるいはセキュアソケットレイヤ（SSL）内でMHに接続される。図1Bに示されているように、ホスト110はMHとの通信リンクを開始し、確立する。代替えとして、MH130はリンクを開始する。しかしながら、ホストにプロセスを開始させることによって、ホスト110はMH130が信用されていることを確実にするためにプロセスをさらに大きく制御できる。ホスト110は、それが満足したいと思う、MHの信頼性及び信用性の任意のタイプのセキュリティ手段または認証手順を実行する。

30

【0029】

同様に、一般的にMH130はモバイル機器120に既知であり、モバイル機器120によって信用されている。モバイル機器120は、それがホスト110との通信を所望するときに、MH130に接続し、MH130と対話するように構成される。モバイル機器120はホスト110によって提供されている1つまたは複数のサービスを使用することを望む。その結果として、MH130はモバイル機器120とホスト110の間の信頼される仲介として動作する。本発明の態様はこの点で制限されていないので、MH130が任意の数の信頼されている、及び／または信頼できないモバイル機器／ホストの組の間で概して信頼される仲介として動作するために複数のホスト及び複数のモバイル機器に接続されてよいことが理解される必要がある。

40

【0030】

図1Cに示されているように、モバイル機器はネットワーク接続117（例えば、及びSSLのような暗号化された接続、あるいは任意の他のタイプの接続）を介してMH13

50

0に接続してよい。モバイル機器がMH130と接続すると、モバイル機器の仮の識別子が認証のために確立される。仮の識別子は秘密識別子(ID)と一意のネットワーク識別子(例えば、モバイル機器のIPアドレス)から構成される。本発明の態様はこの点で制限されていないので、仮の識別子はモバイル機器を安全に特定するために役立つさまざまなまたは追加の識別子から構成されてよい。つまり、MHはモバイル機器を一意に特定でき、(例えば、有害因子が、1つまたは複数のサービスへのアクセスを獲得するためにそれ自体を認証されたモバイル機器であると自称するのを防ぐために、及び/またはデータまたは他の秘密情報を取得するために)悪意のある装置がモバイル機器の識別子になりますことの防止を容易にする多様な認証方式のどれかが使用される。

【0031】

MH130は、接続を確立するために使用されるモバイル機器のネットワークアドレスを取得し、モバイル機器の一意の識別子を形成するために秘密ID127を生成する。例えば、MHは秘密IDとして乱数を生成する。いくつかの実施形態では、秘密IDは、秘密IDがモバイル機器の識別子になりますことを試みる悪意のある攻撃者によって容易に推測できないことを確実にするために、無作為に、及びMHまたはモバイル機器のどちらかに関連する公知の属性または知り得る属性とは無関係に生成される。例えば、MHは、整数値がMHまたはモバイル機器のIPアドレス、ハードウェアアドレス、地理的な位置等に関連していない、少なくとも128ビットの無作為な整数値を生成する。秘密ID及びネットワークIDは、MHにとってモバイル機器の識別子の証拠としてともに動作する。

【0032】

図1Dに示されているように、MH130はモバイル機器とMHの間で確立されたリンク上で秘密ID127を転送する。MH及びモバイル機器は、モバイル機器が再開する、リブートする、またはそれ以外の場合秘密IDを期限切れにさせる操作を受けるまで、認証のために両方によって保持される秘密IDを所有する唯一のエンティティである。ネットワークアドレスと秘密IDは認証機構として動作するが、本発明の態様はこの点で制限されていないので、モバイル機器を安全に識別する認証の任意の方法が使用される。

【0033】

図1Eでは、MH130はホスト110に、モバイル機器120がホストとの接続を希望していることを通知する。MH130からの通知は、モバイル機器のネットワークアドレスを含み、ホスト110によって必要とされる、及び/または所望される追加の情報を含む(例えば、モバイル機器が要求している1つまたは複数のサービス)。次にホスト110は、図1Fに示されているように、MH130によってそれに供給された情報(例えば、ネットワークアドレス)を使用してモバイル機器との通信リンクを開始し、確立する。その結果、モバイル機器及びホストはこの確立されたリンクで自由に通信できる。ホスト110とモバイル機器120間の接続がいったん確立されると、MHは確立リンクリンク上での以後の通信にもはや関与しない。すなわち、信頼できないネットワークを通る通信経路はMH130を含まない。したがって、MHは接続を確立するための仲介として動作するが、接続上の結果として生じる通信の間には動作しない。

【0034】

ホスト110とモバイル機器120間の通信中のなんらかの時点で、モバイル機器はネットワークアドレスの変更を要求してよい。例えば、モバイル機器が、現在のネットワークアドレスが、もはや有効ではない別のネットワークの中に既にローミングした、あるいはローミングしかかっている可能性があり、したがってネットワークハンドオーバを必要とする。現在の無線ネットワークが現在到達できず、別のネットワークによって提供される信号強度または料金請求方式がさらに優れているために、あるいは任意の他のこのような要因のために、このネットワークハンドオーバが生じることがある。加えて、ネットワークアドレスの変更は、モバイル機器が一時的に現在のネットワークとの接続を失ったために発生した可能性もある。いずれにせよ、モバイル機器120はもう到達できない可能性がある、あるいはすぐにモバイル機器の旧ネットワークアドレスで到達できなくなるで

あろう。

【0035】

ネットワークアドレスの変更を開始するために、モバイル機器120は、図1Gに描かれているように、アドレス変更要求129を介してMH130にアドレスの変更を通知する。モバイル装置120は、確立されたリンク上でMH130に対して秘密ID、その旧ネットワークアドレス、及びネットワーク上のモバイル機器の新しい位置に対応する新しいネットワークアドレス（例えば、モバイル機器がローミングしたネットワークに、それによっていま到達できるネットワークアドレス）を提供することによってアドレス変更要求を行う。例えば、ネットワーク150は、第1のネットワークによってサービスを受ける第1のネットワークと、第2のネットワークプロバイダによってサービスを受ける第2のネットワークとを含む。モバイル機器は、第1のネットワークから、旧ネットワークアドレスがもはや有効ではなく、新しいネットワークアドレスが必要とされる第2のネットワークにローミングする。その結果、MHはモバイル機器の識別子を認証し、アドレスの変更をホストに通知するためにモバイル機器によって提供される情報を使用する。

10

【0036】

モバイル機器とMHの間でアドレス変更トランザクションが実施される多くの方法がある。特に、モバイル機器が自主的にネットワークアドレス変更を要求しているのか、あるいは一般的なネットワーク状態（例えば、モバイル機器はローミング、低信号強度、及び／または他のこのような要因に起因して旧ネットワークに対するその接続を不注意に失った可能性がある）に起因して変更せざるをえないのか、MHとモバイル機器間のアドレス変更トランザクションがどのようにして達成されるのかを決定する。

20

【0037】

一実施形態では、モバイル機器はその旧ネットワークアドレスを使用してMHに接続されたままであり（あるいは再接続し）、MHとの毀損の接続の上でアドレスの変更を行う。このトランザクションは自主的なシナリオに制限されていないが、通常、このトランザクションは、モバイル機器がアドレスの変更を自主的に行うときに実施される。別の実施形態では、モバイル機器はMH130から切断し、そのアドレスを局所的に変更してから、新しいネットワークアドレスを使用してMHに再接続し、新しいネットワークアドレスを使用して確立された新しい接続上でアドレス変更要求を行う。

【0038】

次にMH130は、要求を認証し、モバイル機器が要求されたアドレス変更を行うことを許可されていることを検証する。いったん要求が検証されると、図1Hに描かれているように、MH130はホスト110に対し、ホストとモバイル機器の間で現在確立されている接続が変更した、あるいは変更しそうである旨を通知し、新しいネットワークアドレス119をホストに転送する。MH130とホスト110の間の通知トランザクションは、多数の方法で実施されてよい。例えば、通知プロセスは、モバイル機器によるアドレス変更要求が自主的であるのか、あるいは不本意であるのかに依存する。モバイル機器120がMH130から切断する場合、MHはホスト110に、間違ったアドレスにパケットを送信するのを避けるために、モバイル機器とホストの間に確立された接続上でネットワークパケットまたはデータグラムを配信するのを一時的に停止するように信号で伝達する。その結果、ホストはMH130が、ネットワークパケットをモバイル機器に送信するのを再開する前に、MH130が新しいネットワークアドレスとともに転送するのを待機する。

30

40

【0039】

図1Iで示されるように、ホスト110は、MH130によって提供される新しいネットワークアドレスを使用してモバイル機器110との接続を確立する、あるいはその接続状態を調整する。いったんアドレスの変更が完了すると、ホスト110及びモバイル機器120は、モバイル機器によって別のアドレス変更が要求されるまで、及び要求される場合に、MH130からの介入なしに直接的に通信する。すなわち、以後の通信はMHを含まない通信経路上で送られる。したがって、MHは初期接続の確立の間、及びネットワー

50

クアドレス変更を成立させるときにだけ仲介として動作する。

【0040】

したがって、モバイル機器とホスト間の接続は直接的、したがってモバイル機器がネットワークアドレスをどれほど頻繁に変更するのかとは関係ない、及びモバイル機器がどのネットワークにローミングするのかに関係ないことが理解される必要がある。その結果、ホストとモバイル装置間の情報の配信はモバイル機器とホスト間の最小コストのルートについて最適化され、サードパーティネットワーク及び／またはホストを通して送られる必要はない（例えば、ホームネットワーク／ホームエージェント、外来エージェント等を通して送られる）。したがって、ネットワーク効率は最適化され、ネットワーク移動性に対するきわめてスケーラブルな解決策が提供される。

10

【0041】

図1に関連して前述されたモビリティ機構は、きわめて信頼でき、安全である。モバイル機器及びホストは、モバイル機器とホストの間でアドレス変更が起こる前に安全な方法でMHに接続されており、悪意のある攻撃の可能性をあり得なくする。例えば、従来のモビリティネットワークでは、ホスト及び／またはモバイル機器が、特定のネットワークでの外来エージェント通知について何も知らない可能性がある。対照的に、MHは両方の関係者によって信用されて、接続を確立し、且つ／またはアドレス変更を実施することが必要であるときに介入する。したがって、任意のレベルのセキュリティ／認証がこのようなトランザクションの間に実施される。安全且つスムーズな接続の確立及びネットワークアドレス変更の手順は、既知の信頼されている仲介にこのようなトランザクションを実行させることによって達成される。

20

【0042】

加えて、本発明の多様な態様によるモビリティネットワークは、ネットワークインフラストラクチャに対する多大な追加を必要とせず実現される。特に、ホームエージェント及び外来エージェントは、異なるネットワーク全体でローミングするときにモバイル装置が通信を続行できることを保証することを必要とされていない。さらに、本発明の態様によるモビリティネットワークはIPプロトコルまたは任意の特定の根本的なプロトコルに準拠するが、依存する必要はない。したがって、このようなモビリティネットワークは普遍的に実現される。モビリティエージェントが実現される必要がないため、モバイル機器は任意のネットワーク、つまり従来のフレームワークに準拠していないネットワークにもローミングできる。

30

【0043】

前述された利点は本発明の特定の実施形態の所望されている影響にすぎないことが理解される必要がある。言及された利点のどれかまたはすべてが実現されてよいが、本発明の態様は、意図されている利点のどれか1つまたは組み合わせを達成するモビリティネットワークとの使用のために制限されていない。

【0044】

ホストもモバイル機器であってよいことが理解される必要がある。特に、仲介として動作するMHの支援を受けて確立される接続は、2つのモバイル機器間、モバイル機器と信頼できないネットワークに無線で接続されているホストの間、モバイル機器と信頼できないネットワークに結線されているホストの間、あるいはその任意の組み合わせの間である。一実施形態では、モバイル機器は複数のホストに接続され、MHは、モバイル機器によってアドレス変更要求がなされると複数のホストのそれぞれに通知する。本発明の態様はこの点で制限されていないので、モバイル機器、ホスト、サーバ等の任意の構成が使用される。

40

【0045】

本発明の多様な態様は、1つまたは複数のホストがファイアウォールの背後に位置しているネットワーク構成で使用されてよい。特に、MH仲介は、モバイル機器と、ファイアウォールによって保護されているプライベートネットワーク上のその位置のために直接的に接触されない可能性のあるホスト（例えばサーバ）との間で通信を達成するために使用

50

される。例えば、2005年4月12日に出願された「ファイアウォールで保護されているサーバとファイアウォールで保護されているクライアントの間で安全なインターネット接続を自動的に開始し、動的に確立するためのシステム及び方法 (System and Method for Automatically Initiating and Dynamically Establishing Secure Internet Connections Between a Fire-walled Server and Fire-walled Client)」と題される特許文献2 (第'982号) は、ネットワークアドレス変換 (NAT) ルータを含む、1台または複数のサーバがファイアウォールを介して信頼できないネットワークに接続されているプライベートネットワークの一部である多様なネットワーク構成を説明している。特に、第'982号出願に説明されているセッション制御サーバ (SCS) は、図1に描かれているように、MHとして動作し、アドレス変更要求を受け取り、1台または複数のサーバにアドレス変更要求を通知する。第'982号出願に説明されている実施形態は制限的ではなく、本発明の態様がともに使用されてよい例示的なネットワーク構成にすぎないことが理解される必要がある。

【0046】

図2Aは、本発明の一実施形態に従ってネットワーク移動性を達成するためのシステムを示している。システム200は、図1に示されているシステム100に類似する。しかしながら、ホスト110はファイアウォールの背後に位置するサーバ210であり、一般的にはサーバ210のプライベートネットワークアドレスはプライベートネットワーク205の外部の装置にとっては未知である。プライベートネットワーク205は、例えば、企業イントラネット、またはLANの外部から直接的にはアドレス指定できない何らかの他のローカルエリアネットワーク (LAN) である。プライベートネットワーク205は、NATルータ215を通して信頼できないネットワーク (例えば、インターネット) に接続されている。プライベートネットワークの外部の1台または複数のモバイルクライアントが、プライベートネットワーク205を何らかの限られた、安全な基準で利用できるようになることが所望される。例えば、企業LANが、従業員が事務所の外におり、企業LANに直接的に接続していないときに従業員にeメールサービスまたは他のサービスを提供することを望む。NAT215は、MH230と組み合わせられて、さらに詳しく後に記載されるように、安全な外部アクセスを達成するために、及びプライベートネットワークに接続されているモバイルクライアントのための相対的にスムーズ且つ安全なネットワークモビリティを容易にするために使用される。

【0047】

通常、NATルータ215は、プライベートネットワークの外部からルータで受信されたネットワークアドレスを、プライベートネットワーク上の宛先サーバのプライベートネットワークアドレスに変換するNATテーブルを記憶している。したがって、NATルータはサーバのプライベートネットワークアドレスを、プライベートネットワーク上で非表示にし、ゲートキーパとして動作し、他を無視する一方で、特定のネットワークパケットをプライベートネットワーク上のサーバに送ることを可能にする。この立場で、NATルータはファイアウォールの一体化した部分として機能する。NATルータ自体が、一般 (例えば、信頼できないネットワークに接続している他のホストと装置) にとって既知である、あるいは既知でないネットワークアドレスを有する。いずれにせよ、プライベートネットワークとの通信はNATルータを通過する。

【0048】

図2の構成では、MHは、モバイルクライアント220とサーバ210の間に安全な通信を確立することを容易にするために、及び安全且つ動的なネットワークアドレスの変更を達成するために信頼されている仲介として動作する。例えば、モバイルクライアント220とサーバ210の間に初期の接続を確立するために、図1Bから図1Dに関連して説明されている動作が実行される。特に、サーバ210及びモバイルクライアント220は、それぞれMH230との接続を確立する。MH230及びモバイルクライアント220

は、クライアントを一意に且つ安全に特定するために情報を交換する。次にMH 230は、NATルータ215を介してサーバ210に対して、モバイルクライアント220が、例えばサーバ210によって提供されている1つまたは複数のサービスにアクセスするためにサーバ210に接続することを所望している旨を通知する。MH 230は、プライベートネットワークによって信用されているため、それはモバイルクライアントに対して1つまたは複数のサービスを提供することに合意する。しかしながら、プライベートネットワークは内部プライベートネットワークアドレスを非公開にしておくことに関心があるため、サーバ210は、内部ネットワークアドレス情報を公表することなくクライアントと接続を確立するためにNATルータ215と連動して動作する。

【0049】

図2Bに示されているように、サーバ210は、サーバとモバイルクライアント220の間で接続を確立するためのトランザクションを開始する。モバイルクライアントはサーバのプライベートネットワークアドレスを知らないので、モバイルクライアントは独力でサーバと接続を確立することはできない。よって、サーバは、サーバが連絡されてよい仮のネットワークアドレスを用いてモバイル機器に連絡する。NATルータ215は、次に、仮のネットワークアドレスをサーバのプライベートネットワークアドレスと関連付ける。さらに、情報が(MHによって提供されるような)モバイルクライアント220のネットワークアドレスから受信された場合に、NATルータは仮のネットワークアドレスで受信された情報だけをプライベートネットワークアドレスに送るように命令される。このようにして、モバイルクライアントがサーバのプライベートアドレスを一度も学習することなく、サーバとモバイルクライアントの間に接続が設立される。

【0050】

サーバ210とモバイルクライアント220の間に接続が確立された後のなんらかの時点で、モバイルクライアント220は、MHに対してアドレス変更要求を行う。MHを用いるアドレス変更のトランザクションは、図1に関連して説明されたように実施される。すなわち、モバイルクライアントは、モバイルクライアントに連絡できる新しいネットワークアドレスとともに、MHによって提供される秘密のIDを提供する。代わりに、モバイルクライアントがすでにネットワークを切り替え、現在のネットワークとの接続を失い、及び／またはそれ以外の場合ネットワークから不本意に追われた場合、モバイルクライアントはその新しいネットワークアドレスを使用してMHに再接続する。MHは、モバイルクライアントを認証後、アドレス変更要求をサーバに通知し、サーバにモバイルクライアントの新しいネットワークアドレスを提供する。

【0051】

図2Cに示されているように、サーバは接続を再確立するため、あるいはモバイルクライアントとの接続を調整するためのトランザクションを開始する。例えば、サーバ210はモバイルクライアントの新しいネットワークアドレスを使用して図2Bに関連して前に記載された手順を繰り返す。サーバは、NATルータのためのモバイルクライアントの新しいネットワークアドレスと関連するための新しい仮アドレスを発行することを選ぶ。代替えとして、NATテーブルは新しいネットワークアドレスを通知され、新しいネットワークアドレスからサーバ210のプライベートネットワークアドレスにただ通信の経路を決めるためだけに修正される。本発明の態様はこの点で制限されていないので、他の機構はサーバとモバイルクライアントの間の接続を再確立する、及び／または調整するために使用される。

【0052】

本発明の態様は特定のネットワーク構成との使用に制限されていないので、モバイルクライアントは、信頼できないネットワークとそれを通して接続するNATルータを有し、それ自体プライベートネットワークの一部であり、且つ／またはファイアウォール等によって保護されることが理解される必要がある。前に記載されたように、モバイル機器(例えば、モバイルクライアント)は任意の数のホスト(例えばサーバ)と通信する。本発明の態様はこの点で制限されていないので、これらのサーバは、直接的に接続され、信頼で

10

20

30

40

50

きないネットワークを介してアクセス可能なプライベートネットワークの一部であり、あるいは任意の他のネットワーク構成にある。

【0053】

ネットワーク層（ISOスタックの第3層）で実現される、背景に説明されている従来のフレームワークとは異なり、前に記載された技法は、（IPプロトコルを含む）根本的なプロトコルとは関係なくアプリケーション層で実現され、本発明の態様を任意のタイプのネットワークと関連して使用できるようにする。例えば、前に記載されたアドレス変更技法は、NATを介してトランスポート層の下で実現され、あるいは明示的なトランスポート層を介してアプリケーション層で、モバイル機器によるアドレス変更に続いて再接続する。しかしながら、本発明の態様はこの点で制限されていないので、アドレス変更は他の層で実現されてもよい。

10

【0054】

出願人は、本発明の態様が、携帯ステートレスデバイスについて移動性を容易にすることを理解している。ステートレスデバイスは、本明細書では、実質的にネットワークとして動作し、管理装置を表示できる装置を指している。特に、ステートレス装置は、その処理状態を把握しない立場で動作しているときには、おもにネットワークに対するヒューマンインタフェース装置として動作する。ステートレスデバイスは、通常、ネットワーク機能性を実行し、ネットワーク上で受信される情報を表示するソフトウェア以外のアプリケーションを実行しない。その結果、ステートレスデバイスは（その処理状態を把握しない立場で動作しているときには）実質的なユーザ機能性を実行する必要はない、及び／または重要な及び／または恒久的なユーザデータを記憶している（contain）必要はない。

20

【0055】

ステートレスデバイスが、他のネットワークデバイスからのサービスにアクセスする、他のネットワークデバイスからのサービスと対話する、及び／または受け取るようにすることで、従来のネットワークコンピューティングにまつわる1つまたは複数の問題が軽減され、且つ／または排除される。例えば、処理状態を把握するコンピュータデバイスは、おもに、ハッキングを容易にする機能性をユーザに提供する、ホストと拡散されるウィルスの両方にとって計算環境を確立し、且つ／またはそれ以外の場合、ユーザがセキュリティに違反し、ネットワーク環境における脆弱性を攻撃し、及び／またはさもなければ処理状態を把握する装置の機能性を利用できるようにする等の多くのセキュリティの問題に大きく関与している。

30

【0056】

対照的に、ステートレス装置は、前述された多様な能力を容易にする機能性を大部分剥奪されている。しかしながら、前述されたアーキテクチャと連動するステートレスデバイスは、ステートレスデバイスがいわゆる「ダム端末」として動作するが、依然としてネットワーク上で入手可能なリソースから恩恵を受けることができるようにする。特に、ステートレスデバイスは、装置自体が関連する機能性で有効にされる必要なく、任意のコンピュータ環境をシミュレーションしてよい。例えば、ネットワークサービスと対話しているステートレスデバイスは、WindowsTMオペレーティングシステムをステートレスデバイスにインストールする必要なく、WindowsTM装置として動作してよい。ステートレスデバイスはネットワークに対するインタフェースとして動作しているので、それは、機能性がステートレスデバイス上に常駐しているという要件にまつわる付随する欠点を必要としなくても、それが任意の装置または機能性をシミュレーションできるようにする情報をネットワーク上で提示されてよい。

40

【0057】

ステートレスデバイスは、計算の、及び機能上の負担がネットワーク（例えば、ラップトップまたはPC）に接続している装置上にあるパラダイムから、機能性と計算がおもにネットワークに接続されているサーバによって実行されてよいパラダイムへのネットワークコンピューティングにおけるシフトを容易にする。前述された優位点のいくつかの内で

50

、この新しいパラダイムが、従来ネットワーク機能を享受しない、あるいは限られたネットワーク機能を享受する装置（例えば、テレビ、またはディスプレイを有する他の装置）が完全にネットワーク可能な装置になることを可能にする。ステートレスデバイスは、ステートレスデバイスが対話している／接続しているホスト／サーバによって維持されているデータの完全性を保つ一方で、1つまたは複数のネットワークでサービスと完全に対話し、サービスにアクセスするための相対的に安価な手段を提示する。

【0058】

（例えば、パーソナルコンピュータ、パーソナルデジタルアシスタント等の）ステートフルデバイスが処理状態を把握しない立場で動作してよいことが理解される必要がある。つまり、ステートフル装置は、例えばアプリケーションを実行する、ユーザデータと情報を記憶する等のステートフルデバイスとしてのその完全な能力をある程度まで抑制することによってステートレスデバイスとして動作する。純粋に処理状態を把握しない装置は実質的には、ユーザがどこかに記憶されているネットワーク上の情報と接続する、及び／または（例えば、ネットワーク機器が接続されている1つまたは複数のホストまたはサーバによって）ネットワーク上の他の位置から計算され、実行され、提供されるサービスと機能性を受け取ることができるようにするネットワーク機器として動作する。

【0059】

出願人は、ますます高まる携帯電話ネットワーク、在宅勤務、及びモバイル環境のどこからの情報へのスムーズなアクセスに対する願望及び／または必要性に対する傾向が、処理状態を把握しないモバイル機器が明らかに有益である環境を作り出すことを認識している。例えば、本発明の多様な態様は、ネットワークに対するインタフェースとしてモバイルステートレスデバイスを使用することを容易にする。モバイルステートレスデバイスのユーザは、ステートレスデバイスがプライベートネットワーク内で（例えば、ファイアウォールの背後で）接続されているかのように、ネットワーク、例えばプライベートネットワークと対話する。このようにして、モバイルステートレスデバイスのユーザは、実質的にはあたかもユーザがサーバに局所的に接続されているかのように、ある特定のネットワークのサーバによって提供されるサービスを使用できる。前に記載されたモビリティネットワークは、さらに詳しく後で記載されるようにスムーズで、安全で、スケーラブルにモバイルステートレスデバイスの実施を容易にする。

【0060】

図3は、本発明の一実施形態によるモバイルステートレスデバイスを含むモビリティネットワークを示している。モビリティネットワーク300は、図2に説明されているネットワーク200に類似している。しかしながら、モビリティネットワーク300は、処理状態を把握しないネットワーク機器（SNAP）320を含んでよい。SNAP320は純粋に処理状態を把握しない装置であり、あるいは実質的に処理状態を把握しない立場で動作できるステートフルネットワークデバイスである。特に、SNAP320は、例えば信頼できないネットワーク350上でネットワークパケットを受信し、送信する、及びネットワーク上で（例えば、MH330、サーバ310等から）受信された情報を表示する等のネットワーク活動を実行できる任意の装置である。

【0061】

一実施形態では、SNAP320は、中央演算処理装置（CPU）、メモリ、フレームバッファ、ネットワークポート、キーボード、キーパッド、マウス、タッチセンシティブスクリーン等の入力装置、及びネットワークから受信された情報をユーザに提示するためのディスプレイ等の1台または複数のプロセッサを含む。前に記載されたように、SNAPはステートフルデバイスで使用されている他の構成要素を含むが、前記に一覧された構成要素は、SNAPがモバイル環境の信頼できないネットワークで通信するのに十分である。特に、構成要素は、SNAPがネットワーク情報を交換し、ネットワークから受信される情報を表示できるようにし、ユーザが（例えば、1台または複数の入力装置を介して）ディスプレイと対話できるようにするほど十分でありさえすればよい。

【0062】

図 3 B に示されているように、S N A P は、サーバ 3 1 0 との接続を要求するために M H 3 3 0 に連絡する。例えば、S N A P 3 2 0 は、ネットワーク上での装置との通信を可能にするためにネットワークスタックを実現するソフトウェアを含む。S N A P 3 2 0 が純粋に処理状態を把握しない実施形態では、（ネットワークとは別に、純粋に処理状態を把握しない S N A P はほとんどまたはまったく機能性を有さないで）S N A P 3 2 0 は、起動時に M H 3 3 0 に自動的に連絡し、接続するように構成される。

【0063】

図 1 と図 2 に関連して説明されたのとほぼ同じように、ネットワーク接続（例えば、S S L または T C P / I P 接続等の暗号化リンク）が S N A P 3 2 0 と M H 3 3 0 の間に確立され、一意の識別子がセキュリティを容易にするために交換される（例えば、S N A P 3 2 0 はそのネットワークアドレスを提供し、M H は秘密 I D を生成し、S N A P に送信する）。次に M H 3 3 0 はサーバ 3 1 0 に対して、S N A P 3 2 0 が、図 3 C に示されているようにサーバに接続することを希望し、S N A P 3 2 0 のネットワークアドレスをサーバに与えることを通知する。サーバ 3 1 0 は、次に、（例えば、図 3 D に示されているように、S N A P があたかもプライベートネットワーク 3 0 5 に直接的に接続されているかのように）S N A P がファイアウォールの背後でサーバと通信できるようにサーバと S N A P の間にリンクを確立するために使用できる仮アドレスを S N A P に送信する。

【0064】

このようにして、ステートレスデバイスは、プライベートネットワーク（例えば、ファイアウォールの背後で保護されている企業 L A N）の中に位置するサーバによって提供される 1 つまたは複数のサービスにアクセスするために使用されてよい。S N A P が何らかの理由から（例えば、それが新しいネットワークプロバイダを有する新しいネットワークにローミングした、別のネットワークの信号強度または料金請求方式が好ましい位置にローミングした、ネットワークとの接続を一時的に失った等のために）そのネットワークアドレスを変更する必要がある場合、S N A P 3 2 0 はアドレス変更要求を、次に、新しいネットワークアドレスで S N A P と通信を開始するサーバ 3 1 0 への要求を中継する M H 3 3 0 に提供する。したがって、S N A P は、ユーザの介入なしで新しいネットワークアドレスを自動的に、安全に、スムーズに、そして動的に取得する。その結果、ステートレスデバイスは 1 つまたは複数のサービスを受け、且つ／または任意の位置から、及び／または高移動性の環境においてプライベートネットワーク 3 0 5 と対話する。

【0065】

S N A P 3 2 0 が、例えばパーソナルコンピュータ、携帯電話等の従来のステートフルデバイスと関連する特徴及び／または構成要素に依存する必要がないことが理解される必要がある。例えば、S N A P 3 2 0 は、クライアントに特殊な情報、アプリケーション状態情報等を保存する固定記憶機能を含む必要はない。唯一の関連性のある状態情報は、ネットワーク接続性に関する一時状態情報に関する（例えば、T C P 接続状態等）。S N A P は、ネットワークにデータをダウンロードするまたはデータをアップロードすることができる必要はない（そして場合によってはデータをダウンロードまたはアップロードしないようにされている場合がある）。例えば、S N A P によって使用されるサービスは（例えば、第 6 6 0 号出願と第 9 8 2 号出願に説明されているように）完全にサーバ側で提供され、サーバは S N A P に純粋にディスプレイ情報を送信する。したがって、S N A P はプライベートネットワークに属する任意の情報を記憶する、及び／またはそれ自体修正する必要はなく、S N A P にサービスを提供しながらも、プライベートネットワーク内で入手できる情報を保護することによって S N A P とサーバの間の安全な移動性対話を可能にする。

【0066】

加えて、機構とユーザの識別子の間で必要とされている関連がないため、S N A P のユーザとの関連がある必要ない。さらに、サーバの識別子またはそれらから受信されるデータを含む、それが通信するサーバのどれかとの関連は必要とされていない。

【0067】

10

20

30

40

50

モバイルステートレスデバイスが、図 1 に関連して説明されたホスト 110 等の、信頼できないネットワークに直接的に接続されているホストに接続することが理解される必要がある。本発明の態様はこの点で制限されていないので、前述されたモビリティネットワークの構成要素のどれかは、任意の組み合わせ、数、及び／または構成で使用される。

【0068】

本発明の前に記載された実施形態は、多くの方法のどれかで実現できる。例えば、実施形態は、ハードウェア、ソフトウェア、またはその組み合わせを使用して実現される。ソフトウェアで実現されるとき、ソフトウェアコードは、単一のコンピュータで提供されているのか、あるいは複数のコンピュータの間で分散されているのかに関係なく、任意の適切なプロセッサ、またはプロセッサの集合体で実行される。前に記載された機能を実行する任意の構成要素または構成要素の集合体が、一般的には、前に記載された機能を制御する 1 台または複数のコントローラと見なすことができることが理解される必要がある。1 台または複数のコントローラは、例えば専用のハードウェアを用いる、あるいは前に列挙された機能を実行するようにマイクロコードまたはソフトウェアを使用してプログラミングされる汎用ハードウェア（例えば、1 台または複数のプロセッサ）を用いる等の多数の方法で実現される。

【0069】

本明細書に概略されている多様な方法が、種々のオペレーティングシステムまたはプラットフォームのどれか 1 つを利用する 1 台または複数のプロセッサで実行可能であるソフトウェアとして符号化されることが理解される必要がある。加えて、このようなソフトウェアは、多くの適切なプログラミング言語及び／または従来のプログラミングツールまたはスクリプトツールのどれかを使用して作成され、実行可能な機械語コードとしてコンパイルされる。

【0070】

この点で、本発明の一実施形態が、1 台または複数のコンピュータまたは他のプロセッサで実行されるときに、前述された本発明の多様な実施形態を実現する方法を実行する 1 つまたは複数のプログラムで符号化されているコンピュータ可読媒体（または複数のコンピュータ可読媒体）（例えば、コンピュータメモリ、1 枚または複数のフロッピーディスク（登録商標）、コンパクトディスク、光ディスク、磁気テープ等）を目的としていることが理解される必要がある。1 つまたは複数のコンピュータ可読媒体は可搬型であり、その結果その上に記憶されている 1 つまたは複数のプログラムは、前に記載されたように本発明の多様な態様を実現するために 1 台または複数の異なるコンピュータまたは他のプロセッサの上にロードされる。

【0071】

用語「プログラム」は、前に記載されたように本発明の多様な態様を実現するためにコンピュータまたは他のプロセッサをプログラムするために利用できる任意のタイプのコンピュータコードまたは命令のセットを指すために、本明細書では一般的な意味で使用されていることが理解される必要がある。加えて、本実施形態の一態様に従って、実行時に本発明の方法を実行する 1 つまたは複数のコンピュータプログラムが単一のコンピュータまたはプロセッサに常駐する必要はないが、本発明の多様な態様を実現するために多くの異なるコンピュータまたはプロセッサにおいてモジュラー様式で分散されることが理解される必要がある。

【0072】

本発明の多様な態様は単独で、組み合わせられて、あるいは前記に説明された実施形態で特に説明されていない種々の配置で使用される、その適用性において、前記説明に記載された、あるいは図面中に示された構成要素の詳細及び配置に制限されない。本発明は他の実施形態を可能にし、多様な方法で実践できる、実施できる。特に、本発明の多様な態様は、任意のタイプ、集合体、またはネットワーク構成に関連して実現されてよい。ネットワーク実装には制限は課されていない。したがって、前記説明及び図面は、ほんの例証としてのものである。

【0073】

請求項要素を修正するための請求項における「第1の」、「第2の」、「第3の」等の序数用語の使用は、ある請求項要素の、方法の動作が実行される別のまたは時間的な順序に優る優先順位、優位、または順序を独力で暗示するのではなく、単位特定の名称を有するある請求項要素を、（序数用語の使用を別にすれば）同じ名称を有する別の要素と区別するためのラベルとして使用されているにすぎない。

【0074】

また、本明細書に使用されている表現及び専門用語は説明のためであり、制限的と見なされてはならない。「含む」、「備える」または「有する」、「記憶している」、「伴う」及び本書でのその変形の使用は、追加項目だけではなくそれ以降一覧されている項目及び同等物も包含することを意図されている。

10

【符号の説明】

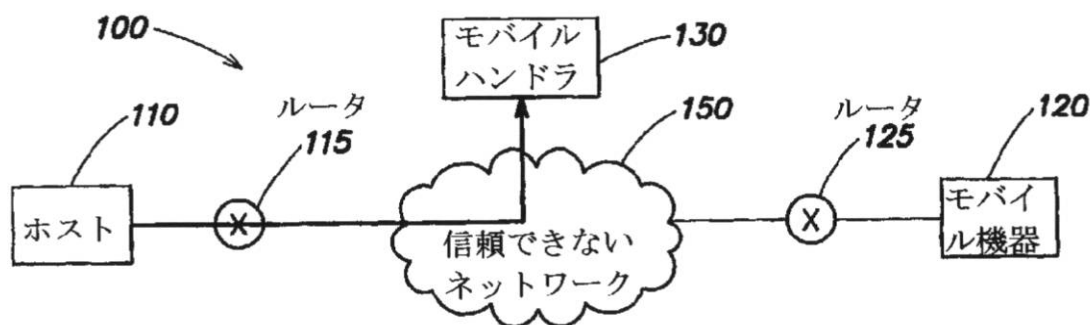
【0075】

110：ホスト，120：モバイル機器，130：モバイルハンドラ，150：ネットワーク。

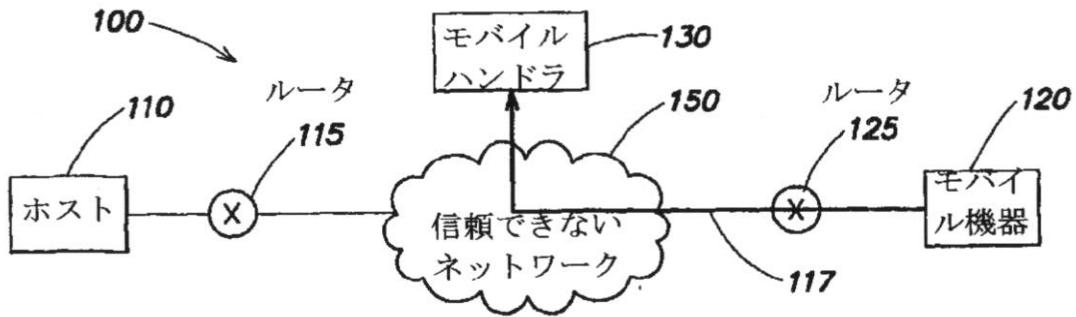
【図1A】



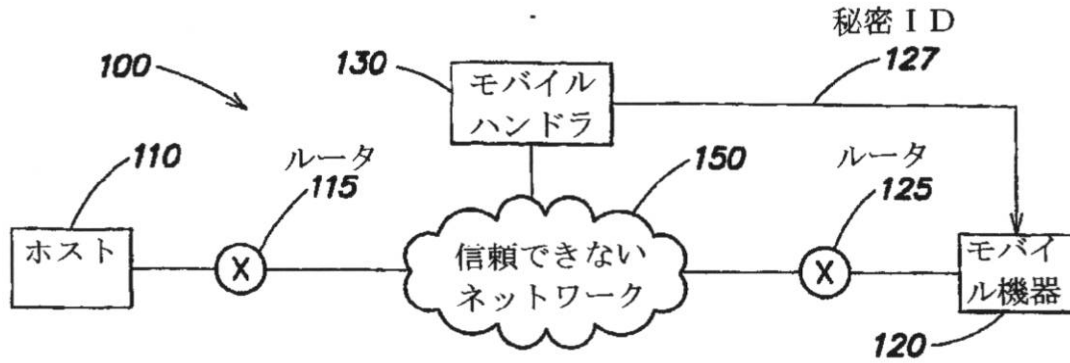
【図1B】



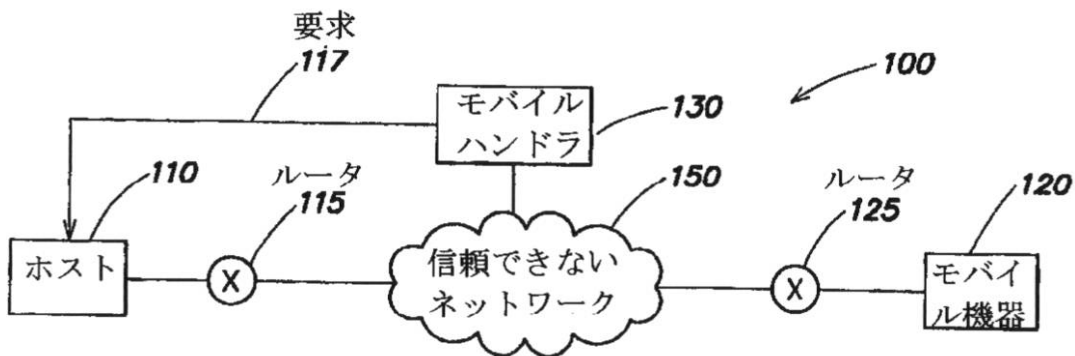
【図 1 C】



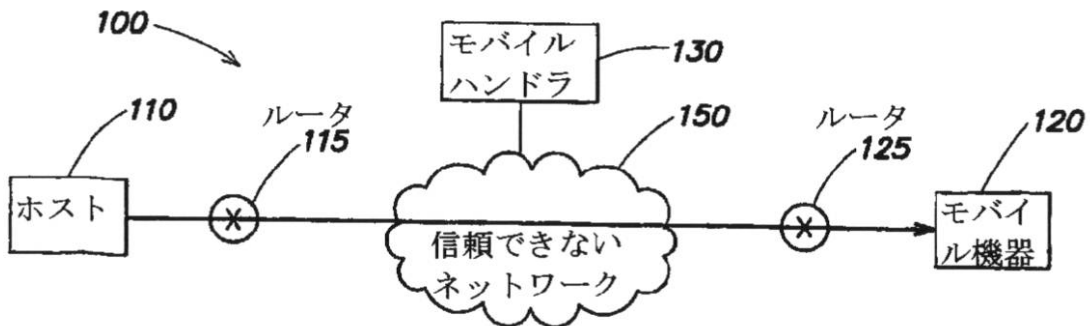
【図 1 D】



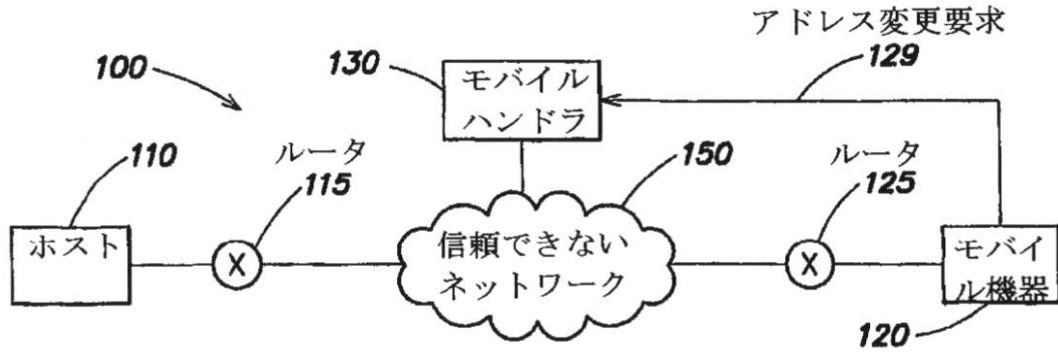
【図 1 E】



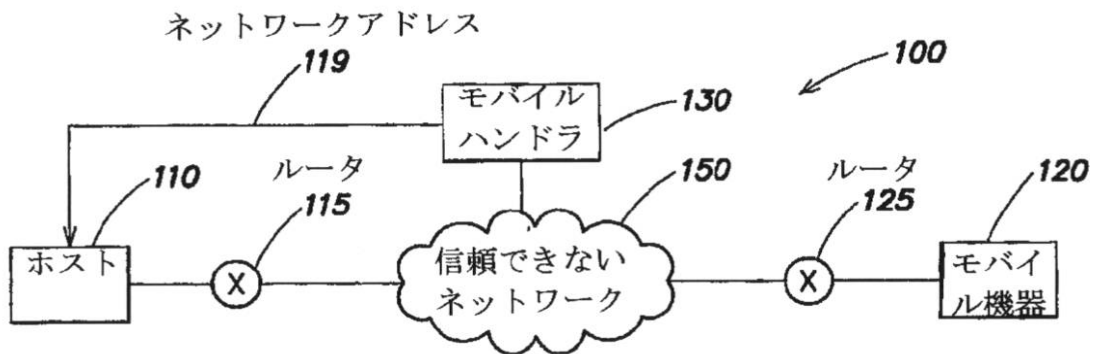
【図 1 F】



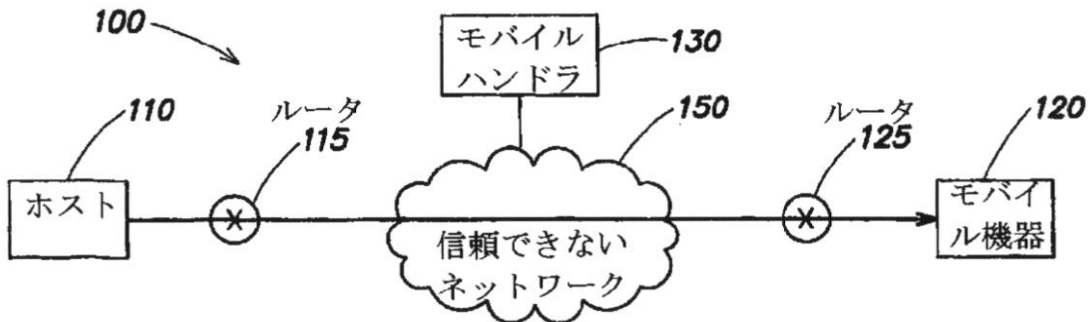
【図 1 G】



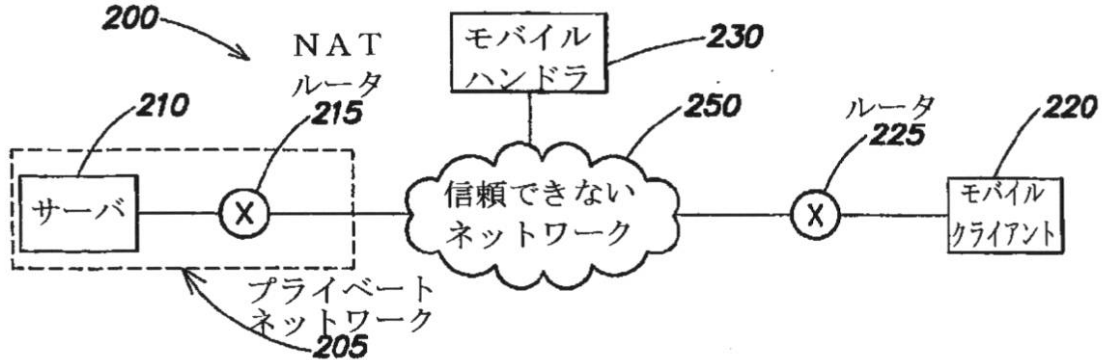
【図 1 H】



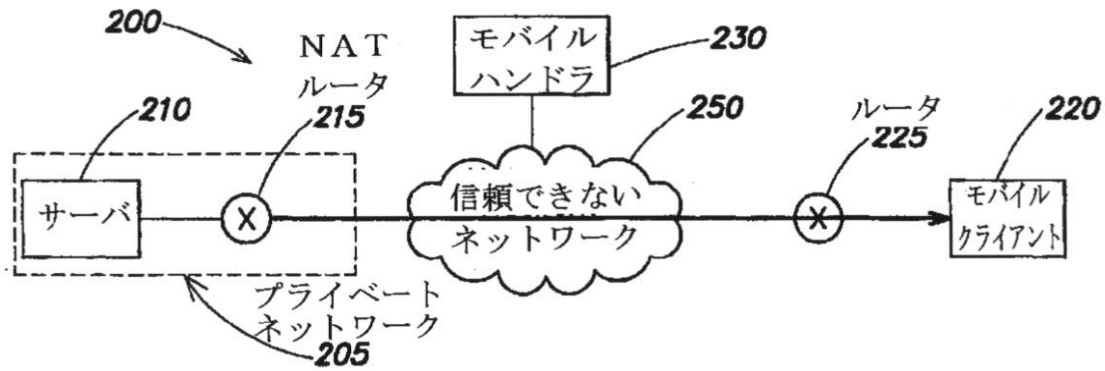
【図 1 I】



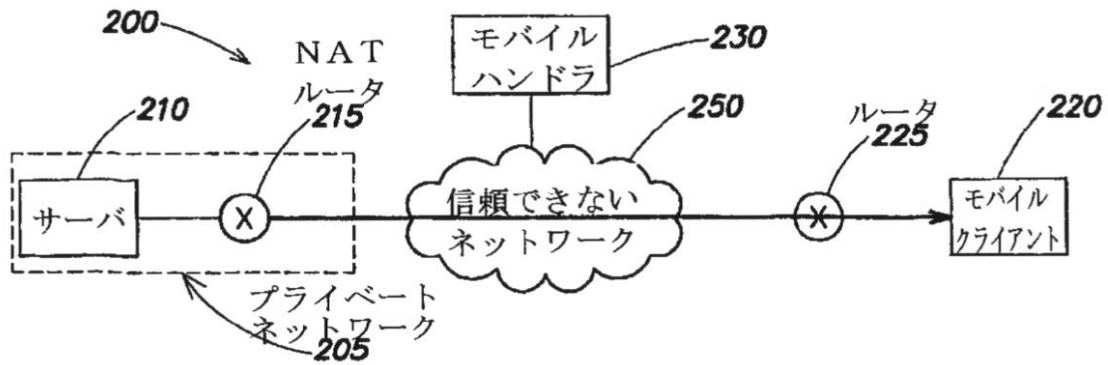
【図 2 A】



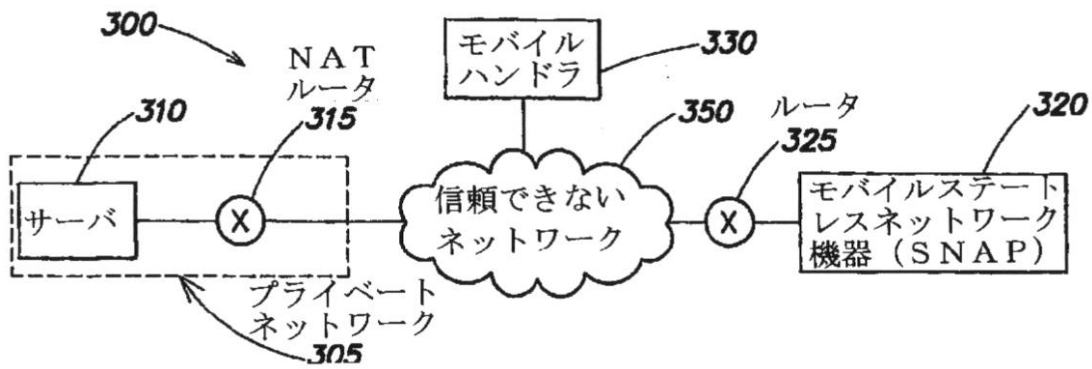
【図 2 B】



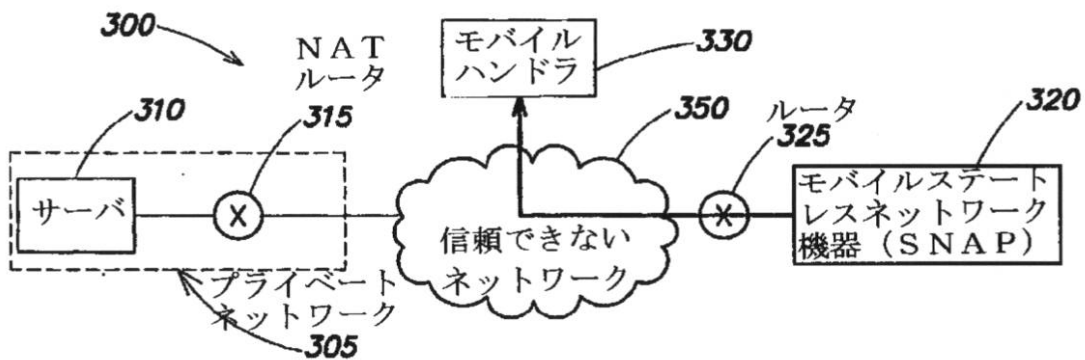
【図 2 C】



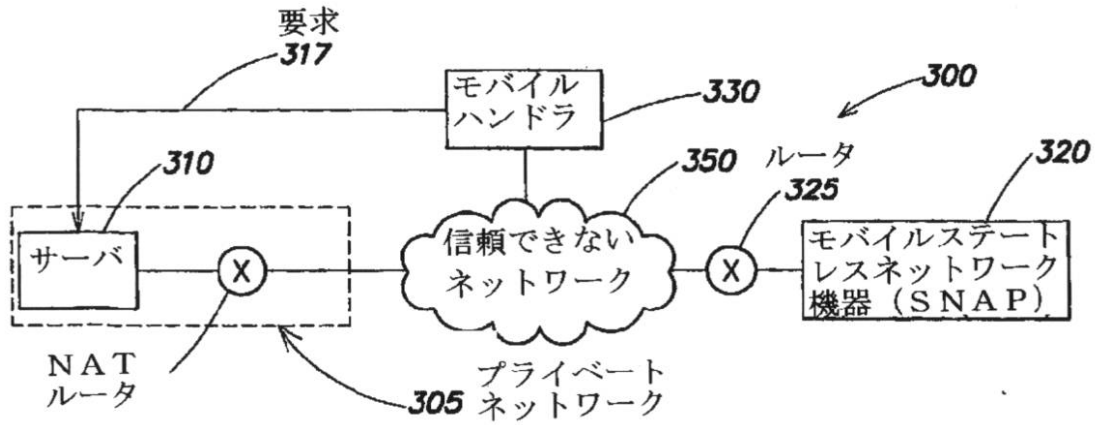
【図 3 A】



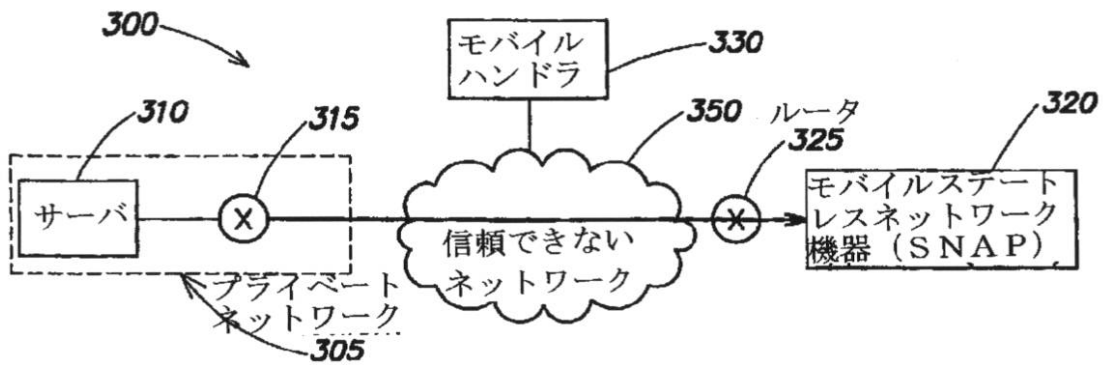
【図 3 B】



【図 3 C】



【図 3 D】



フロントページの続き

(72)発明者 ギレスピー、ブライアン
アイルランド国 9 ダブリン ドラムコンドラ アルフォンサス アベニュー 3 ストリート

(72)発明者 サルメン、ヘルムート
アメリカ合衆国 95032 カリフォルニア州 ロス ガトス ユニバーシティ アベニュー
439ーシー

(72)発明者 トレイシー、デイビッド
アイルランド国 シーオー．ラウズ アイルランド ドロヘダ モナスターボイス ニュータウン
“ ラークフィールド ”

Fターム(参考) 5K067 BB01 BB21 DD17 EE02 EE10 EE16 JJ71