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

特許第6240273号
(P6240273)

(45)発行日　平成29年11月29日(2017.11.29)　(24)登録日　平成29年11月10日(2017.11.10)

(51)Int.Cl.		F I		
H04W 8/00	***(2009.01)***	H04W	8/00	110
H04W 12/06	***(2009.01)***	H04W	12/06	
H04W 84/18	***(2009.01)***	H04W	84/18	
H04L 9/32	***(2006.01)***	H04L	9/00	675A

請求項の数 20　(全 34 頁)

(21)出願番号　特願2016-145257 (P2016-145257)
(22)出願日　平成28年7月25日 (2016.7.25)
(62)分割の表示　特願2015-510240 (P2015-510240)の分割
原出願日　平成24年5月7日 (2012.5.7)
(65)公開番号　特開2016-208534 (P2016-208534A)
(43)公開日　平成28年12月8日 (2016.12.8)
審査請求日　平成28年8月8日 (2016.8.8)
(31)優先権主張番号　12166694.5
(32)優先日　平成24年5月3日 (2012.5.3)
(33)優先権主張国　欧州特許庁 (EP)

(73)特許権者　316013666
アイトロン　グローバル　エス　エー　アール　エル
アメリカ合衆国　９９０１９　ワシントン州　リバティー　レイク　ノース　モルター　ロード　２１１１
(74)代理人　110001243
特許業務法人　谷・阿部特許事務所
(72)発明者　ダニエル　ポーパ
アメリカ合衆国　９９０１９　ワシントン州　リバティー　レイク　ノース　モルター　ロード　２１１１　アイトロン　インコーポレイテッド内

最終頁に続く

(54)【発明の名称】メッシュネットワークにおけるＤＨＣＰサービスを使用する認証

(57)【特許請求の範囲】
【請求項１】
要求デバイスによって実行される方法であって、
前記要求デバイスの近隣において隣接デバイスを発見することであって、前記隣接デバイスは、自律ルーティングネットワークに属する、ことと、
前記自律ルーティングネットワークに参加する要求を前記隣接デバイスに送信することであって、前記要求は、前記要求が向けられる宛先アドレスを規定し、前記送信することは、前記自律ルーティングネットワークによる認証を実現するために前記要求デバイスが前記自律ルーティングネットワークとの単一のハンドシェークを実行できるようにするプロトコルを使用して前記要求を送信することを備え、前記自律ルーティングネットワークとの前記単一のハンドシェークは、前記要求デバイスに、前記自律ルーティングネットワークに関連付けられたグループキーと、前記要求デバイスが前記自律ルーティングネットワークに対してセットアップするための構成情報との受信をさらに実現させることができ、前記認証は、前記要求に含まれる前記要求デバイスの識別子および／または認証署名に基づいて行われ、前記グループキーは、前記認証の結果に関連付けられる、ことと、
前記隣接デバイスを介して前記自律ルーティングネットワークからフィードバックを受信することと
を備える方法。
【請求項２】
前記プロトコルは、インターネットプロトコルバージョン６のための動的ホスト構成プ

ロトコル（ＤＨＣＰｖ６）、またはインターネットプロトコルバージョン４のための動的ホスト構成プロトコル（ＤＨＣＰｖ４）を備える、請求項１の方法。

【請求項３】

前記発見することより前に、予め定められた周波数範囲内でブロードキャストされた前記隣接デバイスの信号を検出することをさらに備える、請求項１の方法。

【請求項４】

前記フィードバックは、前記自律ルーティングネットワークに関連付けられた前記グループキーと、前記要求デバイスが前記自律ルーティングネットワークに対してセットアップするための前記構成情報とを備える、請求項１の方法。

【請求項５】

前記フィードバックは、前記要求デバイスに割り当てられたグローバルアドレスを備え、前記グローバルアドレスのプレフィックスは、前記自律ルーティングネットワークにおけるデバイスによって共有される、請求項４の方法。

【請求項６】

前記送信することより前に、前記要求デバイスの暗号化鍵を使用して前記要求を暗号化することと、

前記受信するとすぐに、前記要求デバイスの解読鍵を使用して前記フィードバックを解読することと

をさらに備える、請求項１の方法。

【請求項７】

前記自律ルーティングネットワークは、ユーティリティメータデバイスのネットワークを備える、請求項１の方法。

【請求項８】

前記要求デバイスは、前記隣接デバイスの近隣に新たに配置されたデバイス、別の自律ルーティングネットワークから移行されたデバイス、または前記自律ルーティングネットワークに以前に参加し、離れてしまったデバイスを備える、請求項１の方法。

【請求項９】

１または複数の処理装置によって実行されるとき、前記１または複数の処理装置に、

動的ホスト構成プロトコル（ＤＨＣＰ）サーバにて、自律ルーティングネットワークに参加する参加要求を要求デバイスから受信することであって、前記参加要求に含まれる前記要求デバイスの識別子および／または認証署名は、前記要求デバイスの認証のために利用される、ことと、

前記要求デバイスに割り当てられるグローバルアドレスを判定することと、

前記要求デバイスのためのＤＨＣＰ応答を生成することであって、前記ＤＨＣＰ応答は、少なくともグループ鍵、前記グローバルアドレスおよび構成情報を備え、前記グループ鍵は、前記認証の結果に関連付けられる、ことと、

前記要求デバイスの現在のアドレスを規定することなく前記要求デバイスに中継するために前記ＤＨＣＰ応答を隣接デバイスに送信することと

を備える動作を実行させる実行可能命令を格納する１または複数のコンピュータ可読媒体。

【請求項１０】

前記動作は、前記自律ルーティングネットワークの状態に少なくとも一部基づいて前記参加要求を処理するかどうかを判定することをさらに備える、請求項９の１または複数のコンピュータ可読媒体。

【請求項１１】

前記自律ルーティングネットワークの状態に少なくとも一部基づいて前記参加要求を処理するかどうかを前記判定することは、前記自律ルーティングネットワークでの現在の負荷が予め定められた閾値よりも大きい、または等しいかどうかを判定することを備える、請求項１０の１または複数のコンピュータ可読媒体。

【請求項１２】

前記参加要求は、前記自律ルーティングネットワークに属し、かつ前記要求デバイスから１ホップ離れた隣接デバイスから中継される、請求項９の１または複数のコンピュータ可読媒体。

【請求項１３】

前記要求デバイスのためのＤＨＣＰ応答を生成することより前に、前記動作は、

前記要求デバイスのメッセージを得るために前記参加要求を解析することと、

前記メッセージを認証サーバに送信することと、

認証応答を前記認証サーバから受信することであって、前記認証応答は、前記自律ルーティングネットワークの前記グループ鍵を備える、ことと

をさらに備える、請求項９の１または複数のコンピュータ可読媒体。

【請求項１４】

前記要求デバイスのためのＤＨＣＰ応答を生成することより前に、前記動作は、

登録要求をネットワーク管理システムに送信することであって、前記登録要求は、前記要求デバイスの識別情報を含む、ことと、

前記ネットワーク管理システムから応答を受信することであって、前記応答は、前記要求デバイスの構成情報を備える、ことと

をさらに備える、請求項９の１または複数のコンピュータ可読媒体。

【請求項１５】

前記グローバルアドレスは、前記ＤＨＣＰサーバによって割り当てられた各デバイスで共有されるプレフィックスを備える、請求項９の１または複数のコンピュータ可読媒体。

【請求項１６】

システムであって、

無線機と、

前記無線機に通信可能に結合され、かつ

前記システムの近隣において隣接デバイスを発見することであって、前記隣接デバイスは、自律ルーティングネットワークに属する、ことと、

前記無線機を介して、前記自律ルーティングネットワークに参加する要求を、前記要求が向けられる宛先アドレスを規定することなくプロトコルを使用して前記隣接デバイスに送信することであって、前記プロトコルは、要求デバイスに前記自律ルーティングネットワークとの単一のハンドシェークを実行させて、前記要求デバイスの認証、および前記自律ルーティングネットワークに関連付けられたグループキーと、前記要求デバイスが前記自律ルーティングネットワークに対してセットアップするための構成情報との受信を実現させることができ、前記要求デバイスの認証は、前記要求に含まれる前記要求デバイスの識別子および／または認証署名に基づいて行われ、前記グループキーは、前記認証の結果に関連付けられる、ことと、

前記隣接デバイスを介して前記自律ルーティングネットワークからフィードバックを受信することと

を備える動作を実行するように構成された処理装置と

を備えたシステム。

【請求項１７】

前記グループキーは、前記要求デバイスと、前記要求デバイスが参加することを要求している１または複数の自律ルーティングネットワークに関連付けられる認証サーバとにのみ知られている前記要求デバイスの対称鍵を使用して暗号化され、前記プロトコルはさらに、前記要求デバイスが前記自律ルーティングネットワークを認証できるようにする、請求項２の方法。

【請求項１８】

前記送信することは、前記要求をビーコンメッセージの中で送信することを備える、請求項１の方法。

【請求項１９】

前記動作は、

前記送信することより前に、前記要求デバイスの暗号化鍵を使用して前記要求を暗号化することと、
前記受信するとすぐに、前記要求デバイスの解読鍵を使用して前記フィードバックを解読することと
をさらに備える、請求項１６のシステム。
【請求項２０】
前記動作は、前記発見することより前に、予め定められた周波数範囲内でブロードキャストされた前記隣接デバイスの信号を検出することをさらに備える、請求項１６のシステム。
【発明の詳細な説明】
【背景技術】
【０００１】
スマートデバイス技術の到来とともに、今日、ますます多くのスマートデバイスが住宅用途、商業用途および軍事用途のために展開されている。これらのデバイスの例には、スマートユーティリティメータ、センサ、制御装置、ルータ、レギュレータ等が含まれる。一般に、新たなデバイスが展開される際、技術者が、新たなデバイスが展開される現場に行き、その現場で新たなデバイスを手作業でセットアップする。その技術者は、例えば、ネットワークに対して新たなデバイスを構成し、認証することができる。その技術者は、その新たなデバイスを、ネットワークに登録することができ、場合により、ネットワークにおける各デバイスの情報を保持する中央サーバに登録することができる。
【０００２】
無線ネットワークに登録し、および参加する標準の方法は、無線ネットワークに重い負荷をかけ、さらに既に重い負荷のかかったネットワーク上の輻輳につながる可能性がある。無線ネットワークに参加する標準のアプローチは、３つのステップから成る。すなわち、まず、参加ノードが８０２．１ｘ認証を完了しなければならず、次に、そのノードが、ＤＨＣＰ（Dynamic Host Configuration Protocol）サーバと通信してＩＰアドレスを獲得し、最後に、そのノードが、ネットワーク管理サーバ（ＮＭＳ）と連絡をとって、要求される構成情報を獲得する。これら３つのステップは、多量の終端間パケット交換を要求し、このことが、要求を課せられる無線通信ネットワークに相当な負荷をもたらす。
【図面の簡単な説明】
【０００３】
詳細な説明は、添付の図を参照して示される。これらの図において、参照符号の左端の数字は、その参照符号が最初に現れる図を識別する。異なる図における同一の参照符号の使用は、同様の、または同一のアイテムを示す。
【図１】ネットワークにおけるデバイスの登録および／または移行を実施するのに使用可能な例示的な環境を示す図である。
【図２】図１の例示的なデバイスをより詳細に示す図である。
【図３】ネットワークにおけるデバイス登録の例示的な方法を示す図である。
【図４】デバイスの、ネットワークに参加する要求を許可するか、または拒否するかを判定する例示的な方法を示す図である。
【図５】１のネットワークから別のネットワークへのデバイス移行の例示的な方法を示す図である。
【発明を実施するための形態】
【０００４】
（概要）
前述したとおり、新たなデバイスの既存の展開は、一般に、技術者が、現場でネットワークに対して新たなデバイスを手作業で構成し、認証し、さらに新たなデバイスをネットワークに接続することを要求する。この接続および認証プロセスは、厄介であるとともに、時間がかかる可能性がある。この状況は、ネットワークが、ネットワークの容量に、またはその容量近くに達している（例えば、その新たなデバイスをサポートするのに限られ

た帯域幅しか残っていない、または全く帯域幅が残っていない）場合、より複雑になる。その時点で、技術者は、その新たなデバイスを、利用可能な別のネットワークが存在する場合、そのネットワークに接続しようと試みることができる。これらの状況は、新たなデバイスを展開する際、および１のネットワークから別のネットワークにノードを移行させる際の困難をもたらすだけでなく、ネットワーク内で、またはネットワークをまたいで異なるデバイスを同期させることに問題を生じさせもする。

【０００５】

本開示は、自律的ルーティングネットワークにおける自動化されたデバイス登録およびデバイス移行の方法を説明する。これらの方法は、ネットワークに対する新たなデバイスの自動的登録を、その新たなデバイスとそのネットワークの間の最小限の回数の交換を介して可能にする。さらに、これらの方法は、ネットワークの条件、および／またはネットワークに展開されるべき新たなデバイスの条件による、デバイスの、１のネットワークから別のネットワークへの移行またはハンドオーバを可能にする。

【０００６】

一般に、デバイスは、ネットワークに参加することを要求することができる。一部の実施形態において、要求側デバイスは、そのネットワークに関連するどのデバイスが、そのネットワークに参加するように新たなデバイスにアドレス指定すること、またはそのようなデバイスの受け付けを制御することを担うかを知っていることも、知らないこともある。一部の実施形態において、要求側デバイスは、ネットワークに参加する要求をブロードキャストすることができ、この要求は、隣接デバイス（すなわち、その要求側デバイスの伝送範囲のデバイス）によって聞かれることが可能である。さらに、または代替として、要求側デバイスは、隣接デバイスからの伝送が聞こえてくる（overhear）ことによってネットワーク内の隣接デバイスを発見してもよい。要求側デバイスは、例えば、メッセージまたはビーコンを介して隣接デバイスにその要求を直接に送信することができる。

【０００７】

その要求を受信したことに応答して、隣接デバイスは、その要求を構文解析し、要求側デバイスがネットワークに参加することを要求することを知ることができる。一実施形態において、隣接デバイスは、要求側デバイスの要求を、ネットワークに参加する新たなデバイスにアドレス指定すること、またはそのようなデバイスの受け付けを制御することを担う制御側デバイスに中継することができる。代替として、隣接デバイスは、その要求を、隣接デバイスの親であるネットワークにおけるデバイスに中継して、その要求を制御側デバイスに中継するよう親デバイスを誘導してもよく、または親デバイスよりも、制御側デバイスに階層的により近い別のデバイスに中継してもよい。一実施形態において、隣接デバイスは、例えば、隣接デバイスが、どのデバイスがネットワークに参加する新たなデバイスにアドレス指定すること、またはそのようなデバイスの受け付けを制御することを担うかを知らない場合、その要求を隣接デバイスの親デバイスに中継することができる。

【０００８】

その要求が制御側デバイスに中継されるか、または親デバイスに中継されるかに関わらず、隣接デバイスは、その要求が向かう宛先を示す宛先アドレス（例えば、制御側デバイスまたは親デバイスのＩＰアドレス）をその要求の中に挿入することができる。

【０００９】

その要求を受信したことに応答して、ネットワークに関連付けられた制御側デバイスは、要求側デバイスの、ネットワークに参加する要求を許可するか、または拒否するかを判定することができる。一実施形態において、制御側デバイスは、要求側デバイスの条件に基づいて、要求側デバイスの要求を許可するか、または拒否するかを判定することができる。例として、限定としてではなく、制御側デバイスは、受信された要求の中に含められた情報に基づいて、要求側デバイスが孤立したデバイスであるかどうかを判定することができる。一実施形態において、要求側デバイスは、要求側デバイスが制御側デバイスのネットワーク以外のネットワークに参加することができない場合、孤立していると決定され得る。さらに、または代替として、要求側デバイスは、要求側デバイスが位置するエリア

を範囲に含む他のネットワークを要求側デバイスが全く検出しない場合、孤立していると決定され得る。さらに、または代替として、要求側デバイスは、要求側デバイスが、別のネットワークから制御側デバイスのネットワークに移行しようと試み、またはそうするように強制され、さらに要求側デバイスが位置するエリアを範囲に含むネットワークが、この別のネットワークと制御側デバイスのネットワークだけに限られる場合、孤立していると決定され得る。さらに、または代替として、要求側デバイスは、要求側デバイスが、制御側デバイスのネットワークを除いて、要求側デバイスのエリア内の検出される全てのネットワークについて残らず成功しなかった（すなわち、参加できなかった）場合、孤立していると決定され得る。さらに、または代替として、要求側デバイスは、制御側デバイスのネットワークが、要求側デバイスと、ネットワークに関連付けられた認証、許可および／またはアカウンティング（ＡＡＡ）サーバなどのサーバとの間で接続をもたらすことができる唯一のネットワークである場合、孤立していると決定され得る。

【００１０】

さらに、または代替として、制御側デバイスは、要求側デバイスの、ネットワークに参加する要求を、ネットワークの条件に基づいて、許可するかまたは拒否するかを判定してもよい。例えば、制御側デバイスは、ネットワークにおける現在のデバイス数、現在のトラフィック、現在もしくは平均のパケットドロップ率、現在もしくは平均の帯域幅使用率などの、ネットワークにかかる負荷が、所定の閾値以上であるかどうかを判定することができる。さらに、または代替として、制御側デバイスは、ネットワークについての負荷統計またはネットワーク統計（現在もしくは平均のパケットドロップ率、現在もしくは平均の帯域幅使用率などの）を格納して、または取り出して、その負荷統計またはネットワーク統計（例えば、現在の帯域幅使用率）が、所定の閾値以上であるかどうかを判定してもよい。

【００１１】

この判定に基づいて、制御側デバイスは、要求側デバイスの要求を許可する、または拒否することができる。例えば、要求側デバイスが孤立したデバイスであると決定したことに応答して、制御側デバイスは、要求側デバイスの、ネットワークに参加する要求を許可することができる。制御側デバイスが、ネットワークにかかっている負荷（または統計）、例えば、現在の帯域幅使用率が、それぞれの閾値以上であるとさらに判定した場合、制御側デバイスは、ネットワークにおける１または複数のデバイスを、そのネットワークを離れるよう、またはそのネットワークから別のネットワークに移行するよう強制することができる。例として、限定としてではなく、制御側デバイスは、ネットワークにおけるどのデバイスが別のネットワークに移行すること、または参加することができるかの知識に基づいて、１または複数のデバイスを選択することができ、さらに制御側デバイスのネットワークを離れるようその１または複数のデバイスを強制することができる。このようにして、制御側デバイスは、要求側の孤立したデバイスがネットワークに参加することを許す十分なレベルまたは所定のレベルまで負荷を低減することができる。

【００１２】

要求側デバイスの、ネットワークに参加する要求を許可すると決定したことに応答して（ネットワークの条件に関わらず）、制御側デバイスは、要求側デバイスのためのネットワークに参加することと関係する情報をさらに準備することができる。この情報には、そのネットワークに関連付けられたグループ鍵、そのネットワークに対して要求側デバイスがセットアップすべき構成情報、および／または要求側デバイスに割り当てられた新たなアドレス（ＩＰアドレスなどの）が含まれ得るが、それらには限定されない。制御側デバイスは、隣接デバイスを介して要求側デバイスに情報を送信することができる。

【００１３】

説明される方法は、ネットワークに参加することを所望する要求側デバイスが、ネットワークを相手に単一回のハンドシェークを実行して、ネットワークに参加することを可能にする。一部の実施形態において、要求側デバイスの近隣に位置しており、要求側デバイスから１ホップ離れている隣接デバイスは、要求側デバイスに代行して要求を制御側デバ

イスに中継して、これにより、要求側デバイスがネットワークに要求をランダムに、またはあてもなく送信することをせずに済むようにすることができる。説明される方法は、ネットワークにおける既存のデバイスの別のネットワークへのスムーズな移行をさらに可能にして、これにより、ネットワークが、ネットワークのリソースを過負荷にすること、過密化させること、または使い果たすことを回避する。さらに、制御側デバイスは、ネットワークに関連する帯域幅使用率のパーセンテージ、全てのデバイスのなかの孤立したデバイスのパーセンテージなどの他の統計を格納し、または取り出し、さらにこれらの他の統計のうちの１または複数がそれぞれの所定の閾値に達した場合、管理者に警報またはアラートを送信することができる。このことは、管理者が、ネットワークの帯域幅を改善するために新たなサポートするハードウェアを追加すること、および／またはネットワークにおけるデバイスのうちのいくつかを物理的に並べ替える、または再配置することを決定するのを容易にする。

【００１４】

本明細書で説明される実施例において、制御側デバイスが、要求を受信し、要求を許可するか、または拒否するかを判定し、ネットワークにおける１または複数のデバイスを、ネットワークを離れるよう強制するか否かを判定し、さらに要求側デバイスがネットワークに参加することを可能にすることと関係する情報を準備する。しかし、他の実施形態において、他の１または複数のデバイスまたはサービスが、これらの機能のうちのいくつか、または全てを実行してもよい。例えば、制御側デバイスが、ネットワークの条件の情報を、ネットワークにおけるデバイスの一部または全てに定期的に、または必要に応じて送信する、またはブロードキャストすることができる。制御側デバイスは、送信される、またはブロードキャストされる情報の中で、ネットワークが、孤立したデバイス以外の新たなデバイスの受け付けを承認しないことを示すことができる。従って、一実施形態において、デバイス（例えば、隣接デバイス）またはサービスが、要求側デバイスの、ネットワークに参加する要求を許可するか、または拒否するかを判定することが可能である一方で、別のデバイスまたは別のサービスが、ネットワークにおける１または複数のデバイスを、ネットワークを離れるように強制するかどうかを判定することが可能であり、さらに別のデバイスまたはさらに別のサービスが、要求側デバイスがネットワークに参加することを可能にすることと関係する情報を準備することが可能である。

【００１５】

本出願は、複数の様々な実施形態を説明する。以下のセクションは、様々な実施形態を実施するのに適した例示的な環境を説明する。次に、本出願は、デバイス登録およびデバイス移行を実施するための例示的なシステム、デバイス、およびプロセスを説明する。

【００１６】

（例示的な環境）

図１は、デバイス登録およびデバイス移行を実施するのに使用可能な例示的なアーキテクチャ１００の概略図である。アーキテクチャ１００は、直接通信経路、つまり、「リンク」を介して互いに通信可能に結合された複数のノードまたはデバイス１０２－１、１０２－２、１０２－３、１０２－４、１０２－５、．．．、１０２－Ｎ（まとめてデバイス１０２と呼ばれる）を含む。この実施例において、Ｎは、ワイドエリアネットワーク（ＷＡＮ）、メトロポリタンエリアネットワーク（ＭＡＮ）、ローカルエリアネットワーク（ＬＡＮ）、ＮＡＮ（neighborhood area network）、パーソナルエリアネットワーク（ＰＡＮ）などの自律的ルーティングエリア（ＡＲＡ）内に構成されたデバイスの数を表す。１だけのＡＲＡしか図１に示されないが、実際には、複数のＡＲＡが存在することが可能であり、集合的に、ＡＭＩ（advanced metering infrastructure）ネットワークなどの、より大きいネットワークを規定することが可能である。任意の所与の時点で、個別の各デバイスは、特定のＡＲＡのメンバであり得る。しかし、時が経つにつれ、デバイスは、ＡＲＡにかかるそれぞれの負荷、干渉などの様々な要因に基づいて、１のＡＲＡから、地理的に近い、または重なり合う別のＡＲＡに移行する可能性がある。

【００１７】

前述したとおり、「リンク」という用語は、２つのデバイス間の直接通信経路（別のデバイスを経由せず、別のデバイスによって伝搬されることもない）を指す。リンクは、有線通信経路を介しても、無線通信経路を介してもよい。各リンクは、デバイスがデータを送信する、または受信することができる複数のチャネルを表し得る。複数のチャネルのそれぞれは、複数のチャネルのそれぞれに関して同一な、または異なる周波数範囲によって規定され得る。一部の事例において、複数のチャネルは無線周波数（ＲＦ）チャネルを備える。複数のチャネルは、制御チャネルと、複数のデータチャネルとを備え得る。一部の事例において、制御チャネルは、データチャネルのうちの１のデータチャネルを、データを転送するのに利用されるように指定する１または複数のメッセージをデバイス間で通信するために利用される。一般に、制御チャネル上の伝送は、データチャネル上の伝送と比べて、より短い。

【００１８】

一実施形態において、デバイス１０２のいくつか、または全てが、例えば、スマートユーティリティメータ（電気メータ、ガスメータおよび／または水道メータ）、センサ（例えば、温度センサ、気象観測所、周波数センサなど）、制御装置、トランス、ルータ、サーバ、中継器（例えば、セルラ中継器）、スイッチ、バルブ、以上の組み合わせ、または通信ネットワークに結合可能であり、データを送受信することができる任意デバイスなどの、様々なデバイスのいずれとして実装されることも可能である。

【００１９】

一部の実施形態において、デバイス１０２のいくつか、または全てが、さらに、または代替として、例えば、ノートブックコンピュータもしくはポータブルコンピュータ、ハンドヘルドデバイス、ネットブック、インターネット機器、ポータブル読み取りデバイス、電子ブックリーダデバイス、タブレットコンピュータもしくはスレートコンピュータ、ゲームコンソール、モバイルデバイス（例えば、モバイル電話機、携帯情報端末、スマートフォンなど）、メディアプレーヤなど、または以上の組み合わせを含む様々な従来のコンピューティングデバイスのいずれとして実装されてもよい。

【００２０】

この例において、デバイス１０２は、インターネットなどのバックホールネットワーク１０６に対するＡＲＡの接続ポイントの役割をするエッジデバイス（例えば、デバイス１０２－４）経由で中央局１０４と通信するようにさらに構成され得る。一実施形態において、エッジデバイスには、セルラ中継器、セルラルータ、エッジルータ、ＤＯＤＡＧ（Destination Oriented Directed Acyclic Graph）ルート、ＡＲＡネットワークのルートデバイスもしくはルートノード等が含まれ得るが、以上には限定されない。この図示される実施例において、デバイス１０２－１は、ＡＲＡにおける他のノードのためのセルラ中継器および／または転送デバイスの役割をして、例えば、ＡＲＡのその他のデバイス１０２－２～１０２－Ｎからの通信を、ネットワーク１０６を介して中央局１０４との間で中継する。

【００２１】

一実施形態において、デバイス１０２のいくつか、または全てが、処理装置１０８を含み得る。処理装置１０８は、メモリ１１２と通信可能に結合された１または複数のプロセッサ１１０を含み得る。メモリ１１２は、様々な機能を実施するようにプロセッサ１１０上で実行可能である、１または複数のソフトウェアモジュールおよび／またはファームウェアモジュールを格納するように構成され得る。これらのモジュールは、メモリの中に格納され、プロセッサ上で実行可能なソフトウェアおよび／またはファームウェアとして本明細書で説明されるが、他の実施形態において、これらのモジュールのうちの任意のモジュールまたは全てのモジュールが、全体として、または部分的に、説明される機能を実行するようにハードウェアによって（例えば、ＡＳＩＣ、専用の処理装置などとして）実装されてもよい。

【００２２】

メモリ１１２は、コンピュータ可読媒体を備えることが可能であり、さらにランダムア

クセスメモリ（ＲＡＭ）などの揮発性メモリ、および／または読み取り専用メモリ（ＲＯＭ）またはフラッシュＲＡＭなどの不揮発性メモリの形態をとることができる。コンピュータ可読媒体には、コンピューティングデバイスの１または複数のプロセッサによって実行されるようにコンピュータ可読命令、データ構造、プログラムモジュール、または他のデータなどの情報を格納するために任意の方法または技術で実装された揮発性媒体および不揮発性媒体、リムーバブルメディアおよび非リムーバブルメディアが含まれる。コンピュータ可読媒体の例には、相変化メモリ（ＰＲＡＭ）、スタティックＲＡＭ（ＳＲＡＭ）、ＤＲＡＭ、他のタイプのＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリもしくは他のメモリ技術、ＣＤ－ＲＯＭ、ＤＶＤもしくは他の光ストレージ、磁気カセット、磁気テープ、磁気ディスクストレージもしくは他の磁気ストレージデバイス、またはコンピューティングデバイスによってアクセスされるように情報を格納するのに使用され得る他の任意の非伝送媒体が含まれるが、以上には限定されない。本明細書で定義されるコンピュータ可読媒体は、変調されたデータ信号および搬送波などの通信媒体を含まない。

【００２３】

一実施形態において、デバイス１０２のいくつか、または全てが、無線機１１４をさらに含み得る。無線機１１４は、複数のチャネル／周波数のうちの１または複数を介してＲＦ信号を送信するように、かつ／または受信するように構成された無線周波数（ＲＦ）トランシーバを備える。一部の実施形態において、デバイス１０２のいくつか、または全てが、各通信リンクの制御チャネルおよび複数のデータチャネルなどの異なる複数のチャネル上でデータを送受信するように構成された単一の無線機１１４を含む。無線機１１４は、異なる複数の変調技法、データレート、プロトコル、信号強度および／または電力レベルを実施するようにさらに構成され得る。アーキテクチャ１００は、デバイス１０２に、様々なタイプのデバイス（例えば、スマートメータ、セルラ中継器、センサなど）、様々な世代もしくはモデルのデバイス、および／またはそれ以外で様々なチャネル上で伝送することができるとともに、様々な変調技法、データレート、プロトコル、信号強度および／または電力レベルを使用することができるデバイスが含まれ得るという点で、デバイスの異種のネットワークを表すことが可能である。

【００２４】

さらに、または代替として、一部の実施形態において、デバイス１０２のいくつか、または全てが、ネットワークインターフェース１１６、および／または入出力インターフェース１１８を含んでもよい。処理装置１０８は、ネットワークインターフェース１１６からのデータ、入出力インターフェース１１８から受け取られたデータ、および／またはメモリ１１２の中に格納されたデータを受け取り、操作するようにさらに構成され得る。

【００２５】

一方、ネットワーク１０６は、無線ネットワークもしくは有線ネットワーク、または無線ネットワークと有線ネットワークの組み合わせを自らが備え得るバックホールネットワークを表す。ネットワーク１０６は、相互接続され、単一の大型ネットワーク（例えば、インターネットまたはイントラネット）として機能する個々のネットワークを集めたものであり得る。さらに、それらの個々のネットワークは、無線ネットワークもしくは有線ネットワーク、または無線ネットワークと有線ネットワークの組み合わせであり得る。

【００２６】

中央局１０４は、サーバ、パーソナルコンピュータ、ラップトップコンピュータ、ルータ、スイッチなどの１または複数のコンピューティングデバイスによって実装され得る。この１または複数のコンピューティングデバイスは、メモリに通信可能に結合された１または複数のプロセッサを備え得る。一部の実施形態において、中央局１０４は、デバイス１０２のうちの１または複数から受信されたデータの処理、解析、格納、および／または管理を実行する集中メータデータ管理システムを含む。例えば、中央局１０４は、スマートユーティリティメータ、センサ、制御装置、ルータ、レギュレータ、サーバ、中継器、スイッチ、バルブ、および／または他のデバイスから獲得されたデータを処理すること、解析すること、格納すること、および／または管理することができる。中央局１０４は、

さらに、または代替として、ＡＭＩネットワークのデバイスのレジストリ、デバイス構成設定、バージョン情報などを保持するためのネットワーク管理システム（ＮＭＳ）を含んでもよい。図１の例は、単一のロケーションにおける中央局１０４を示すものの、一部の実施形態において、中央局は、複数のロケーションに分散していてもよく、かつ／または完全に無くされてもよい（例えば、極めて非集中化された分散コンピューティングプラットフォームの事例において）。

【００２７】

一実施形態において、このアーキテクチャは、ＡＲＡネットワークにおけるデバイス１０２のＩＤを認証することを担う認証サーバ１２０をさらに含み得る。一部の実施形態において、アーキテクチャ１００は、ＡＲＡネットワークに対する新たなデバイスの受け付けを制御する、またはサポートすることが可能な他のサーバ１２２をさらに含み得る。一実施形態において、それらの他のサーバ１２２には、ＡＲＡネットワークに対してセキュリティサービスを維持すること、および／または提供することを担うセキュリティサーバが含まれ得る。

【００２８】

（例示的なデバイス）

図２は、図１のデバイス１０２（例えば、代表的デバイス１０２－２）の詳細を示す概略図である。この実施例において、無線機１１４は、ＲＦフロントエンド２０２およびベースバンドプロセッサ２０４に結合されたアンテナ２００を含む。ＲＦフロントエンド２０２は、送信機能および／または受信機能をもたらすことができる。ＲＦフロントエンド２０２は、アンテナによってもたらされた信号、およびデバイス１０２のうちの１または複数から獲得された信号に調整する（tune）こと、および／または当該信号を減衰させることなどの機能をもたらす高周波数アナログ構成要素および／またはハードウェア構成要素を含み得る。ＲＦフロントエンド２０２は、ベースバンドプロセッサ２０４に信号を供給することができる。

【００２９】

一実施例において、ベースバンドプロセッサ２０４の全て、または一部が、ソフトウェア（ＳＷ）無線機として構成され得る。一実施例において、ベースバンドプロセッサ２０４は、無線機１１４に周波数選択機能および／またはチャネル選択機能をもたらす。例えば、ＳＷ無線機は、プロセッサ、または特定用途向け集積回路（ＡＳＩＣ）、または他の組み込まれたコンピューティングデバイスによって実行されるソフトウェアとして実装されたミキサ、フィルタ、増幅器、変調器および／または復調器、検出器などを含み得る。ＳＷ無線機は、プロセッサ１１０、およびメモリ１１２の中で定義された、またはメモリ１１２の中に格納されたソフトウェアを利用することができる。代替として、無線機１１４は、少なくとも部分的に、アナログ構成要素を使用して実装されてもよい。

【００３０】

処理装置１０８は、時刻を保持するように構成されたクロック２０６をさらに含み得る。クロック２０６は、１または複数のカウントアップタイマまたはカウントダウンタイマをもたらすようにさらに構成され得る。そのようなタイマは、複数の通信チャネルの間で周波数ホッピングする際に使用され得る。

【００３１】

周波数ホッピングモジュール２０８が、ベースバンドプロセッサ２０４およびクロック２０６と通信するように構成され得る。一実施例において、周波数ホッピングモジュール２０８は、時刻情報を獲得し、さらに／またはクロック２０６における周波数ホッピングタイマを設定するように構成される。そのような時刻情報および／またはタイマは、異なるチャネルまたは異なる周波数をいつ「ホップ」すべきか、または異なるチャネルまたは異なる周波数にいつ調整すべきかを周波数ホッピングモジュール２０８に示す。さらに、周波数ホッピングモジュール２０８は、実際の周波数変更を実行するよう無線機１１４のＳＷ無線機または他の構成要素を誘導するように構成され得る。従って、周波数ホッピングモジュール２０８は、合意された周波数の間で、合意された時刻に繰り返し移り、合意

された期間にわたって、合意されたプロトコルで別のデバイスと通信することができる。
【００３２】
一部の実施形態において（例えば、デバイスがユーティリティメータである場合）、メモリ１１２は、１または複数のリソース（例えば、電気、水道、天然ガスなど）の消費データを収集するように構成された計測モジュール２１０をさらに含むことが可能であり、次に、この消費データが、中央局１０２または他の宛先に最終的に伝搬されるように他の１または複数のデバイス１０２に送信されることが可能である。
【００３３】
デバイス１０２は、さらに、または代替として、ＡＲＡネットワークにおけるデバイス１０２の役割または機能に依存して、発見モジュール２１２、ブロードキャストモジュール２１４、送信モジュール２１６、暗号化／解読モジュール２１８、受信モジュール２２０、解析モジュール２２２、中継モジュール２２４、制御モジュール２２６、認証モジュール２２８、および／またはアドレス割り当てモジュール２３０を含んでもよい。これらのモジュールの機能の詳細は、後段で説明される。
【００３４】
（例示的なデバイス登録）
一実施形態において、デバイス１０２（例えば、デバイス１０２－３）が、中央局１０４におけるＮＭＳに登録すること、および／またはＡＲＡネットワークのメンバになることに先立って、最初に、ＡＲＡネットワークにアタッチされることが可能である。例として、限定としてではなく、要求側デバイス１０２－３はまず、ＡＲＡネットワークに、要求側デバイス１０２－３がＡＲＡネットワークに参加する要求を送信することができるポイント、例えば、ＩＰレベルまたはＩＰレイヤでアタッチされることが可能である。例えば、要求側デバイス１０２－３はまず、ＡＲＡネットワークにＭＡＣ（すなわち、媒体アクセス制御）レベルまたはＭＡＣレイヤでアタッチされることが可能である。一実施形態において、要求側デバイス１０２－３は、ＡＲＡネットワークを含むエリアに新たに展開されたスマートユーティリティメータなどのデバイスに対応することが可能である。代替として、要求側デバイス１０２－３は、図１に示されるとおり、別のＡＲＡネットワークからそのＡＲＡネットワークに移行しようと試みているデバイスに対応してもよい。
【００３５】
一実施形態において、要求側デバイス１０２－３の発見モジュール２１２は、要求側デバイス１０２－３の近隣に存在する１または複数の隣接デバイス１０２（例えば、デバイス１０２－２）を能動的に、または受動的に発見することができる。要求側デバイス１０２－３の隣接デバイスには、例えば、要求側デバイス１０２－３から通信可能に１ホップ離れたデバイスが含まれ得る。つまり、隣接デバイスは、要求側デバイスが通信リンクを介して直接に通信することができるデバイスである。一実施形態において、要求側デバイス１０２－３は、ＭＡＣレイヤにおいて近隣発見サービスを実行することができる。さらに、または代替として、発見モジュール２１２は、要求側デバイス１０２－３が参加することを所望するＡＲＡネットワークのために指定された所定の周波数または所定の周波数範囲で検出された、または受信された信号を調べることを介して、発見モジュール２１２の近隣に存在する１または複数の隣接デバイスを発見してもよい。
【００３６】
さらに、または代替として、一部の実施形態において、要求側デバイス１０２－３は、要求側デバイス１０２－３の近隣の範囲内の１または複数のデバイスが要求を受信し、さらに要求側デバイス１０２－３に代行してその要求を処理し、さらに／または要求側デバイス１０２－３と接続を確立することができるように、要求側デバイス１０２－３の近隣に存在する任意のデバイスをまず知るもしくは発見して、またはまず知るもしくは発見することなしに、ブロードキャストモジュール２１４を使用してＡＲＡネットワークに参加する要求をブロードキャストしてもよい。
【００３７】
さらに、または代替として、一実施形態において、ブロードキャストモジュール２１４

は、要求側デバイス１０２－３の存在をブロードキャストし、要求側デバイス１０２－３の存在に気付くＡＲＡネットワークにおける１または複数のデバイスは、要求側デバイス１０２－３と通信するのを待つことができる。一部の実施形態において、ブロードキャストモジュール２１４は、所定の周波数、または所定の周波数範囲において所定のコードまたは所定のメッセージを使用して、要求側デバイス１０２－３の存在をブロードキャストすることができる。

【００３８】

要求側デバイス１０２－３が１または複数の隣接デバイス１０２を発見するか、または１または複数の隣接デバイス１０２が要求側デバイス１０２－３を発見するかに関わらず、要求側デバイス１０２－３は、隣接デバイス１０２（例えば、デバイス１０２－２）を選択し、さらに隣接デバイス１０２－２に関連するＡＲＡネットワークに参加する要求を隣接デバイス１０２－２に送信することができる。一実施形態において、要求側デバイス１０２－３は、動的ホスト構成プロトコルバージョン６（ＤＨＣＰｖ６）要求またはＤＨＣＰｖ４要求を、送信モジュール２１６を介して隣接デバイス１０２－２に送信することができる。代替として、要求側デバイス１０２－３は、参加する要求をビーコンメッセージの中に含めて、そのビーコンメッセージを、送信モジュール２１６を介して隣接デバイス１０２－２に送信してもよい。

【００３９】

要求側デバイス１０２－３は、ＡＲＡネットワークに対する新たなデバイスの受け付けまたは追加を制御することを担うＡＲＡネットワークに関連する制御側デバイスのアドレス（例えば、ＩＰアドレス）を知っていることも、知らないことも可能である。この例における制御側デバイスは、エッジデバイス１０２－４、ＤＨＣＰサーバ、またはＡＲＡ外部の別のデバイスを備え得る。具体的には、参加要求またはビーコンメッセージは、要求側デバイス１０２－３の参加要求が最終的に向かう必要があるＡＲＡネットワークに関連する制御側デバイスの宛先アドレスを含むことも、含まないことも可能である。

【００４０】

一部の実施形態において、要求側デバイス１０２－３は、暗号化／解読モジュール２１８を使用して暗号化鍵によって参加要求またはビーコンメッセージの全体または一部を暗号化することができる。この暗号化鍵は、秘密鍵または対称鍵を備え得る。一実施例において、デバイス１０２のそれぞれ（ＡＲＡネットワークのメンバであるデバイス、またはＡＲＡネットワークに参加することを許可され得るデバイス）が、デバイスの製造中に、または製造後に同一の公開鍵／秘密鍵ペアまたは同一の対称鍵を共有することができる。一部の実施形態において、デバイス１０２のそれぞれ（ＡＲＡネットワークのメンバであるデバイス、またはＡＲＡネットワークに参加することを許可され得るデバイス）が、デバイス１０２のそれぞれによるアクセスが可能な暗号化／解読鍵の所定のプールから選択された暗号化／解読鍵または対称鍵を有することができる。一部の実施形態において、デバイス１０２のそれぞれ（ＡＲＡネットワークのメンバであるデバイス、またはＡＲＡネットワークに参加することを許可され得るデバイス）は、そのデバイス、並びに他の１または複数のデバイスおよび／またはサーバ（中央局１０４、認証サーバ１２０、および／またはＡＲＡネットワークの制御側デバイスなど）だけに知られている暗号化／解読鍵または対称鍵を有することが可能である。他の実施形態において、要求側デバイス１０２は、暗号化なしに、すなわち、平文フォーマットで参加要求またはビーコンメッセージを送信することができる。

【００４１】

さらに、または代替として、一実施形態において、参加要求は、要求側デバイス１０２－３の識別子、および／または要求側デバイス１０２－３に登録されており、さらにＡＲＡネットワーク、ＡＲＡネットワークの制御側デバイス、中央局１０４におけるＮＭ、および／または認証サーバ１２０に知られている所定の鍵（例えば、前述の暗号化鍵、対称鍵もしくは公開鍵）を使用して署名された、または暗号化された認証署名、ナンスもしくは任意の値などの認証情報を含み得るが、以上には限定されない。一部の実施形態におい

て、参加要求は、要求側デバイス１０２－３が孤立したデバイスであるかどうかを示すメッセージ、コードまたは他の標識をさらに含み得る。例として、限定としてではなく、要求側デバイス１０２－３は、要求側デバイス１０２－３が、ＡＲＡネットワーク以外のネットワーク（図示せず）に参加することができない場合、孤立していると決定され得る。さらに、または代替として、要求側デバイス１０２－３は、要求側デバイス１０２－３が位置するエリアを範囲に含む他のネットワークを要求側デバイス１０２－３が全く検出しない場合、孤立していると決定され得る。さらに、または代替として、要求側デバイス１０２－３は、要求側デバイス１０２－３が、別のネットワーク（図１に示される）からＡＲＡネットワークに移行しようと試みて、この別のネットワークとＡＲＡネットワークだけしか、要求側デバイス１０２－３が位置するエリアを範囲に含むネットワークが存在しない場合、孤立していると決定され得る。さらに、または代替として、要求側デバイス１０２－３は、要求側デバイス１０２－３が、ＡＲＡネットワークを除いて、要求側デバイス１０２－３のエリア内の検出される全てのネットワークについて残らず成功しなかった（すなわち、参加しようと試みて、失敗した）場合、孤立していると決定され得る。さらに、または代替として、要求側デバイス１０２－３（すなわち、参加することに失敗した）は、ＡＲＡネットワークが、要求側デバイス１０２－３と、例えば、ＮＭＳサーバおよびＤＨＣＰサーバなどの１または複数のサーバとの間で接続をもたらすことができる唯一のネットワークである場合、孤立している。

【００４２】

一部の実施形態において、隣接デバイス１０２－２に参加要求を送信後、要求側デバイス１０２－３は、隣接デバイス１０２－２を介したＡＲＡネットワークからの応答を待つ。この応答は、ＡＲＡネットワークに参加する、要求側デバイス１０２－３の参加要求が許可されたか、または拒否されたかを示すことができる。この応答が、要求側デバイス１０２－３の参加要求が拒否された、または否定されたことを示す場合、要求側デバイス１０２－３は、別のＡＲＡネットワークを探索し、要求側デバイス１０２－３が見出すことが可能なその別のＡＲＡネットワークに参加する要求を送信することができる。

【００４３】

参加要求が許可された場合、応答は、例えば、ＡＲＡネットワークに関連するグループ鍵、要求側デバイス１０２－３がＡＲＡネットワークに参加するための構成情報、および／または要求側デバイス１０２－３に割り当てられたアドレス（例えば、ＩＰアドレス）を含み得る。さらに、または代替として、一部の実施形態において、この応答は、例えば、ＡＲＡネットワーク内で要求側デバイス１０２－３からデータパケットをルーティングするために制御側デバイスによって指定された１または複数の経路上のデバイスのアドレス情報、および／またはＡＲＡネットワークに関連する制御側デバイスのアドレス情報を含め、ＡＲＡネットワーク内の１または複数のデバイス１０２のアドレス情報を含み得る。一部の実施形態において、この応答の一部または全体（例えば、グループ鍵など）が、要求側デバイス１０２－３の対称鍵を使用して暗号化され得る。さらに、または代替として、この応答の一部または全体（例えば、制御側デバイスのアドレス情報など）が、ＡＲＡネットワークに関連するグループ鍵を使用して暗号化されてもよい。

【００４４】

一部の実施形態において、要求側デバイス１０２－３は、例えばＡＲＡネットワーク（例えば、ＡＲＡネットワークの隣接デバイス１０２－２）を相手に、ＤＨＣＰｖ６プロトコルまたはＤＨＣＰｖ４プロトコルを使用して、単一回のハンドシェークまたは交換（すなわち、参加要求のための単一の上流メッセージ、および参加要求に対する応答のための単一の下流メッセージ）だけを実行して、ＡＲＡネットワークに参加することを実現することができる。一実施形態において、要求側デバイス１０２－３および／またはＡＲＡネットワークは、この単一回のハンドシェークまたは交換を使用して相互認証（すなわち、ＡＲＡネットワークまたは認証サーバ１２０による要求側デバイス１０２－３のＩＤの認証、および要求側デバイス１０２－３によるＡＲＡネットワークのＩＤの認証）を実現することができる。

【００４５】
例として、限定としてではなく、要求側デバイス１０２－３の対称鍵または非対称鍵（例えば、公開鍵／秘密鍵）が、要求側デバイス１０２－３と、ＡＲＡネットワークに関連する他の１または複数のデバイスおよび／またはサーバ（例えば、認証サーバ１２０、中央局１０４、および／または制御側デバイス）だけにしか知られていない（または知られていないことになっている）場合、要求側デバイス１０２－３とＡＲＡネットワークは、要求側デバイス１０２－３の対称鍵または非対称鍵を使用することによって互いを認証することができる。例えば、ＡＲＡネットワークは、認証サーバ１２０が、要求側デバイス１０２－３の対称鍵または非対称鍵（例えば、公開鍵）を使用して暗号化されているナンスまたは署名（参加要求に含められていることが可能な）をうまく解読することができた場合、要求側デバイス１０２－３のＩＤを認証することができる。さらに、要求側デバイス１０２－３は、例えば、要求側デバイス１０２－３が、要求側デバイス１０２－３の対称鍵または非対称鍵（例えば、公開鍵）を使用して暗号化されている暗号化されたグループ鍵（または、例えば、参加要求に応答して含められた、以前に送信されたナンスもしくは署名などの他の情報）をうまく解読することができた場合、ＡＲＡネットワークを認証することができる。一部の実施形態において、暗号化されたグループ鍵が、ＡＲＡネットワークを認証することの源として使用される場合、要求側デバイス１０２－３は、要求側デバイス１０２－３が、解読されたグループ鍵を使用してＡＲＡネットワークにおける他のデバイスとうまく通信することができた場合、ＡＲＡネットワークの認証をさらに判定することができる。代替の実施形態において、要求側デバイス１０２－３は、場合により、ＴＣＰ／ＩＰプロトコルおよび／または他のインターネットプロトコルなどの１または複数のプロトコルを使用して、ＡＲＡネットワークを相手に複数回のハンドシェークまたは交換を実行して、ＡＲＡネットワークに参加することを実現してもよい。
【００４６】
一実施形態において、隣接デバイス１０２－２は、要求側デバイス１０２－３から送信された、またはブロードキャストされた参加要求を、隣接デバイス１０２－２の受信モジュール２２０を介して受信することができる。参加要求またはビーコンメッセージが暗号化されている場合、隣接デバイス１０２－２は、隣接デバイス１０２－２の暗号化／解読モジュール２１８を使用して参加要求またはビーコンメッセージを解読することができる。隣接デバイス１０２－２は、（解読された、または暗号化されていない場合、最初から平文の）参加要求を構文解析し、解析モジュール２２２を介して、要求側デバイス１０２－３がＡＲＡネットワークに参加することを要求していると決定することができる。
【００４７】
一部の実施形態において、要求側デバイス１０２が隣接デバイス１０２－２のＡＲＡネットワークに参加することを要求していると決定したことに応答して、隣接デバイス１０２－２は、その参加要求を、そのＡＲＡネットワークに関連する制御側デバイス（例えば、デバイス１０２－４）に中継することができる。一実施形態において、隣接デバイス１０２－２は、制御側デバイスのアドレス（例えば、ＩＰアドレス）を知っていることが可能であり、さらにその参加要求を、中継モジュール２２４を介して制御側デバイスに中継することができる。例として、限定としてではなく、中継モジュール２２４は、要求側デバイス１０２－３から送信された（ＤＨＣＰｖ６の）参加要求を制御側デバイスに中継する中継エージェント、例えば、ＤＨＣＰｖ６中継エージェントを含み得る。例えば、隣接デバイス１０２－２の中継モジュール２２４は、制御側デバイスのＩＰアドレスを、要求側デバイス１０２－３の参加要求を含むデータパケットの宛先アドレスとして挿入し、さらにそのデータパケットを制御側デバイスに直接に、または隣接デバイス１０２－２の親デバイス経由で間接的に中継することができる。
【００４８】
代替として、隣接デバイス１０２－２が、制御側デバイスのアドレスを知らない場合、隣接デバイス１０２－２の中継モジュール２２４が、（要求側デバイス１０２－３の要求を含む）そのデータパケットを、ＡＲＡネットワークにおける隣接デバイス１０２－２の

親デバイスに中継することを、例えば、その親デバイスのＩＰアドレスを挿入して、隣接デバイス１０２－２の親デバイスが、要求側デバイス１０２－３の参加要求を制御側デバイスに中継するように誘導すること、または中継することを可能にすることによって、行ってもよい。

【００４９】

さらに、または代替として、参加要求が制御側デバイスに中継されるか、または隣接デバイス１０２－２の親デバイスに中継されるかに関わらず、隣接デバイス１０２－２は、隣接デバイス１０２－２の暗号化鍵を使用して、中継された要求をさらに暗号化することができる。一実施形態において、この暗号化鍵は、ＡＲＡネットワークに関連し、ＡＲＡネットワークにおける各デバイス１０２に配信されるグループ鍵を含むことができる。一部の実施形態において、この暗号化鍵は、ＡＲＡネットワークの各デバイス１０２によるアクセスが可能であり、かつ／または隣接デバイス１０２－２に割り当てられた暗号化／解読鍵のプールから選択された暗号化鍵を含み得る。他の一部の実施形態において、隣接デバイス１０２－２は、要求を平文フォーマットで、即ち、暗号化なしに中継することができる。一実施形態において、隣接デバイス１０２－２は、隣接デバイス１０２－２が要求側デバイス１０２－３に代行して中継する要求の送信元アドレスとして、隣接デバイス１０２－２のアドレスを使用する（または、要求側デバイス１０２－３の参加要求の送信元アドレスを、隣接デバイス１０２－２のアドレスで置き換える）ことができる。このことは、ＡＲＡネットワークに関連する他のデバイスまたはサーバから要求側デバイス１０２－３に戻す返信を適切に転送することを可能にする。例えば、要求側デバイス１０２－３に対する応答または返信（例えば、参加要求に関する）は、隣接デバイス１０２－２のアドレスを宛先アドレスとして使用することが可能であり、さらにそれに相応して要求側デバイス１０２－３に応答または返信を転送する、または中継するように隣接デバイス１０２－２に要求することができる。

【００５０】

一部の実施形態において、隣接デバイス１０２－２は、要求側デバイス１０２－３の参加要求を、ＡＲＡネットワークの条件、および／または要求側デバイス１０２－３の条件に関わらず、中継する。さらに、または代替として、一部の実施形態において、隣接デバイス１０２－２は、ＡＲＡネットワークは、ＡＲＡネットワークに対する新たなデバイスの受け付けを、ＡＲＡネットワークに追加されるべき、または加えられるべきその新たなデバイスが孤立したデバイスでない限り、承認することができないことを示す指示を、制御側デバイス１０２－４から受信することが可能である。そのような指示を受信する事例において、隣接デバイス１０２－２の解析モジュール２２２は、例えば、受信モジュール２２０によって受信された参加要求に基づいて、要求側デバイス１０２－３が孤立したデバイスであるかどうかをさらに判定することができる。要求側デバイス１０２－３が孤立したデバイスではないと決定したことに応答して、隣接デバイス１０２－２は、例えば、隣接デバイス１０２－２が、孤立したデバイスを除いて、新たなデバイスの受け付けを拒否する指示を制御側デバイス１０２－４からそれまでに受信しているために、ＡＲＡネットワークに参加する要求が拒否されたことを示す応答またはフィードバックを要求側デバイス１０２－３に送信することができる。

【００５１】

一部の実施形態において、隣接デバイス１０２－２から中継された要求を受信したことに応答して、ＡＲＡネットワークに関連する制御側デバイスは、ＡＲＡネットワークの条件に基づいて、要求側デバイス１０２－３の参加要求を許可するか、または拒否するかを判定することができる。制御側デバイスは、制御モジュール２２６を使用して、要求側デバイス１０２－３の参加要求を許可するか、または拒否するかを判定することができる。一実施形態において、制御側デバイスは、受け付け制御権限の役割をすることができる。一実施形態において、制御側デバイスは、ＡＲＡネットワークのルートデバイスもしくはエッジデバイス（例えば、デバイス１０２－４）、ＡＲＡネットワークのルータを備えることが可能であり、またはＡＲＡネットワークの１または複数のノードに分散されること

が可能である。一部の実施形態において、制御側デバイスは、代替として、中央局１０４、中央局１０４によって管理可能な１または複数のＡＲＡネットワークのルーティングツリーのルート、または中央局１０４の系列に属することが可能な別のサーバ１２２などのバックエンドデバイスに配置されてもよい。一部の実施形態において、制御側デバイスは、他のサーバ１２２のうちの１または複数に含められることが可能なＤＨＣＰサーバまたはＤＨＣＰｖ６サーバを含み得る。一実施形態において、制御側デバイスがＤＨＣＰサーバもＤＨＣＰｖ６サーバを、またはＤＨＣＰサーバもしくはＤＨＣＰｖ６サーバの１または複数の機能を含まない場合に、制御側デバイスは、ＤＨＣＰサーバまたはＤＨＣＰｖ６サーバに参加要求を中継することができる。一部の実施形態において、制御側デバイスは、ＤＨＣＰサーバもしくはＤＨＣＰｖ６サーバ、ルートデバイス、エッジデバイス、ルータ、中央局１０４などのバックエンドデバイス、または別のサーバ１２２を含む１または複数のデバイスの組み合わせを含み得る。本出願における参照を容易にするため、デバイス１０２－４は、制御側デバイスと呼ばれる。デバイス１０２－Ａは、ＡＲＡネットワークを、バックホールネットワーク１０６を介して中央局１０４に結合する、ＡＲＡネットワークのルートノード、エッジルータ、または他のエッジデバイスを表す。

【００５２】

一部の実施形態において、隣接デバイス１０２－２から中継される要求を受信したことに応答して、制御側デバイス１０２－４は、ＡＲＡネットワークにかかっている負荷が所定の閾値を超えているかどうかに基づいて、要求側デバイス１０２－３の要求を許可するか、または拒否するかを判定することができる。例として、限定としてではなく、制御側デバイス１０２－４は、ＡＲＡネットワークが過負荷になっているかどうか（例えば、ＡＲＡネットワークにおけるデバイスの現在の数が、収容に関する所定の閾値以上であるかどうか）に基づいて、要求側デバイス１０２－３の要求を許可するか、または拒否するかを判定することができる。さらに、または代替として、制御側デバイス１０２－４は、ＡＲＡネットワークの統計（現在の／平均の帯域幅使用率、現在の／平均の衝突率、データパケットの現在の／平均のドロップ率、現在の／平均のデータトラフィックなど）が、その統計に関する所定の閾値以上であるかどうかに基づいて、要求側デバイス１０２－３の要求を許可するか、または拒否するかを判定してもよい。

【００５３】

一実施形態において、ＡＲＡネットワークにかかっている負荷が所定の閾値を超えた（例えば、統計が、その統計に関する所定の閾値以上である）ことに応答して、制御側デバイス１０２－４は、要求側デバイス１０２－３の（ＤＨＣＰまたはＤＨＣＰｖ６の）参加要求を拒否することができる。代替として、一部の実施形態において、制御側デバイス１０２－４は、例えば、受信された要求の中の情報に基づいて、要求側デバイス１０２－３が孤立したデバイスであるかどうかをさらに判定することができる。受信された要求の中の情報は、例えば、要求側デバイス１０２－３が孤立したデバイスであることを示す標識を含み得る。要求側デバイス１０２－３が孤立したデバイスであると決定したことに応答して、制御側デバイス１０２－４は、ＡＲＡネットワークの条件に関わらず（即ち、ＡＲＡネットワークにかかっている負荷が所定の閾値を超えているかどうかに関わらず）、要求側デバイス１０２－３がＡＲＡネットワークに参加することを許可することができる。

【００５４】

一部の実施形態において、制御側デバイス１０２－４は、認証モジュール２２８を使用して要求側デバイス１０２－３の認証をさらに判定することができる。例えば、制御側デバイス１０２－４の認証モジュール２２８は、受信された要求の中に含められた要求側デバイス１０２－３の識別子または認証署名に基づいて、要求側デバイス１０２－３の認証を判定することができる。さらに、または代替として、制御側デバイス１０２－４は、要求を構文解析して、要求側デバイス１０２－３の識別子および／または認証署名を、セキュリティサーバまたは認証－許可－アカウンティング（ＡＡＡ）サーバ１２０などの認証サーバに送信してもよい。セキュリティサーバまたはＡＡＡサーバ１２０は、例えば、中央局１０４によって管理される１または複数のＡＲＡネットワーク（現在のＡＲＡネット

ワークを含む）に参加するデバイスのＩＤを認証することを担う。一実施形態において、セキュリティサーバまたはＡＡＡサーバ１２０は、ＡＲＡネットワークの外部に配置され得る。一部の実施形態において、セキュリティサーバまたはＡＡＡサーバ１２０は、制御側デバイス１０２－４の同一のＡＲＡネットワーク内の別のノードまたはデバイス（例えば、デバイス１０２－１）であり得る。制御側デバイス１０２－４は、例えば、ＲＡＤＩＵＳ（Remote Authentication Dial In User Service）などのネットワーキングプロトコルを使用して、要求側デバイス１０２－３の識別子および／または認証署名を含む情報をセキュリティサーバまたはＡＡＡサーバ１２０に送信することができる。本出願における参照を容易にするため、ＡＡＡサーバが、１または複数のＡＲＡネットワークに参加するデバイスのＩＤを認証する動作を説明する例として使用される。

【００５５】

一実施形態において、例えば、要求側デバイス１０２－３の識別子および／または認証署名に基づいて要求側デバイス１０２－３のＩＤを認証することに成功した後、ＡＡＡサーバ１２０は、要求側デバイス１０２－３のＩＤが認証されることに成功したことを示すメッセージを、制御側デバイス１０２－４、または制御側デバイス１０２－４に関連する、もしくは接続されたＤＨＣＰサーバに送信することができる。さらに、または代替として、一部の実施形態において、ＡＡＡサーバ１２０は、ＡＲＡネットワークに関連するグループ鍵（例えば、グループリンクレイヤ鍵）を、制御側デバイス１０２－４、または制御側デバイス１０２－４のＤＨＣＰサーバにさらに送信することができる。さらに、または代替として、ＡＡＡサーバ１２０は、ＡＲＡネットワークに関連するグループ鍵（例えば、グループリンクレイヤ鍵）によって署名された、または暗号化されたメッセージを、制御側デバイス１０２－４、または制御側デバイス１０２－４のＤＨＣＰサーバにさらに送信してもよい。一実施形態において、制御側デバイス１０２－４は、ＡＲＡネットワークに関連するグループ鍵をあらかじめ格納することができ、従って、暗号化されたメッセージを、そのグループ鍵を使用して解読することができる。一部の実施形態において、制御側デバイス１０２－４は、要求側デバイス１０２－３の公開鍵または対称鍵の情報を有さない可能性がある。その事例において、ＡＡＡサーバ１２０は、要求側デバイス１０２－３の公開鍵または対称鍵を使用してグループ鍵を暗号化し、さらにＡＲＡネットワークに関連するグループ鍵を使用して制御側デバイス１０２－４に対するメッセージ（暗号化されたグループ鍵を含む）を暗号化することができ、制御側デバイス１０２－４が、要求側デバイス１０２－３の公開鍵または対称鍵を使用して暗号化されているグループ鍵を要求側デバイス１０２－３に転送することができる。

【００５６】

一実施形態において、制御側デバイス１０２－４とＤＨＣＰサーバが別々のデバイスである場合、ＡＡＡサーバ１２０は、制御側デバイス１０２－４に関連するＤＨＣＰサーバにそのメッセージを送信することができる（例えば、認証要求が、ＤＨＣＰサーバから、または制御側デバイス１０２－４からＤＨＣＰサーバ経由で送信された後）。メッセージを受信したことに応答して、ＤＨＣＰサーバは、そのメッセージを解析して、要求側デバイス１０２－３のＩＤが認証されるかどうかを判定することができる。さらに、または代替として、ＤＨＣＰサーバは、そのメッセージを制御側デバイス１０２－４に中継してもよい。一部の実施形態において、ＡＡＡサーバ１２０は、認証要求が制御側デバイス１０２－４から（または制御側デバイス１０２－４とＤＨＣＰサーバが別々のデバイスである場合、ＤＨＣＰサーバ経由で制御側デバイス１０２－４から）送信された場合、メッセージを制御側デバイス１０２－４に直接に送信することができる。メッセージがＤＨＣＰサーバから中継されるか、またはＡＡＡサーバ１２０から直接に送信されるかに関わらず、一実施形態において、ＡＡＡサーバ１２０からメッセージを受信したことに応答して、制御側デバイス１０２－４は、そのメッセージを解析して、要求側デバイス１０２－３のＩＤが認証されるかどうかを判定することができる。要求側デバイス１０２－３のＩＤが認証されると決定したことに応答して、制御側デバイス１０２－４は、要求側デバイス１０２－３のＩＤが認証され、かつ／または要求側デバイス１０２－３がＡＲＡネットワーク

に参加することを許可されることを示す、前述の実施形態において説明される通り、要求側デバイス１０２－３の公開鍵または対称鍵を使用して暗号化されることも、暗号化されないことも可能な（このことは、例えば、制御側デバイス１０２－４が要求側デバイス１０２－３の公開鍵または対称鍵を有するかどうかに依存し得る）メッセージを要求側デバイス１０２－３に送信することができる。さらに、または代替として、一部の実施形態において、制御側デバイス１０２－４は、要求側デバイス１０２－３に対する、隣接デバイス１０２－２によって後に解読され、構文解析され得るメッセージを、ＡＲＡネットワークに関連するグループ鍵を使用して暗号化してもよい。一実施形態において、メッセージは、例えば、ＡＲＡネットワークに関連するグループ鍵、および、例えば、ＡＡＡサーバ１２０から受信された暗号化されたグループ鍵などの、要求側デバイス１０２－３の公開鍵または対称鍵を使用して暗号化されることも、暗号化されないことも可能な他の情報をさらに含み得る。一部の実施形態において、メッセージを受信したことに応答して、要求側デバイス１０２－３は、そのメッセージを、暗号化されている（例えば、要求側デバイス１０２－３の公開鍵または対称鍵を使用して）場合、解読して、ＡＲＡネットワークに関連するグループ鍵を取り出すことができる。さらに、または代替として、要求側デバイス１０２－３は、暗号化されたグループ鍵（要求側デバイス１０２－３の公開鍵または対称鍵を使用してＡＡＡサーバ１２０において暗号化されたグループ鍵などの）を解読して、グループ鍵を取り出すことができる。すると、要求側デバイス１０２－３は、ＡＲＡネットワークの他のデバイスを相手にデータ（例えば、グループ鍵を使用して暗号化されたデータなど）を送信すること、および／または受信することを許されることができる。

【００５７】

一部の実施形態において、制御側デバイス１０２－４（または制御側デバイス１０２－４に関連するＤＨＣＰサーバ）は、送信モジュール２１６を使用してＮＭＳに登録要求をさらに送信することができる。登録要求は、例えば、制御側デバイス１０２－４に関連する秘密鍵（公開鍵／秘密鍵のうちの）を使用して署名される、もしくは暗号化されることが可能な、要求側デバイス１０２－３の識別子、ＡＲＡネットワークに関連するグループ鍵、および／または要求側デバイス１０２－３に関連する鍵を含むことができる。一実施形態において、制御側デバイス１０２－４は、登録要求を、平文の、暗号化されていないフォーマットでＮＭＳに送信することができる。

【００５８】

制御側デバイス１０２－４から登録要求を受信した後、ＮＭＳは、そのメッセージが暗号化されている場合、そのメッセージを解読し、そのメッセージを構文解析し、さらに要求側デバイス１０２－３の識別子を獲得することができる。一部の実施形態において、ＮＭＳは、要求側デバイス１０２－３に関連する情報、および／またはＡＲＡネットワークに関連する情報をさらに取り出すことができる。一実施形態において、ＮＭＳは、取り出された情報に基づいて、要求側デバイス１０２－３がＡＲＡネットワークに参加するのに、またはＡＲＡネットワークに対してセットアップするのに使用可能な構成情報または構成パラメータを決定することができる。取り出された情報には、要求側デバイス１０２－３のモデルタイプまたはデバイスタイプ、要求側デバイス１０２－３が参加することを要求しているＡＲＡネットワークのタイプなどが含まれ得るが、以上には限定されない。さらに、または代替として、ＮＭＳは、構成情報または構成パラメータを制御側デバイス１０２－４、または制御側デバイス１０２－４のＤＨＣＰサーバに送信することができる。

【００５９】

一実施形態において、ＮＭＳから構成情報または構成パラメータを受信したことに応答して、制御側デバイス１０２－４（またはＤＨＣＰサーバ）のアドレス割り当てモジュール２３０が、要求側デバイス１０２－３のための新たなアドレス（例えば、ＩＰｖ６アドレスなどの新たなＩＰアドレス）を決定することができる。一実施形態において、制御側デバイス１０２－４（またはＤＨＣＰサーバ）は、例えば、制御側デバイス１０２－４（またはＤＨＣＰサーバ）が使用可能な中継エージェントに割り当てられたプレフィックスに基づいて、その新たなアドレスを決定することができる。さらに、または代替として、

制御側デバイス１０２－４（またはＤＨＣＰサーバ）は、制御側デバイス１０２－４のＡＲＡネットワークにおけるデバイスに指定された、またはそれらのデバイスによって共有されるプレフィックスに基づいて、その新たなアドレスを決定することができる。一実施形態において、要求側デバイス１０２－３に割り当てられた新たなアドレスは、制御側デバイス１０２－４（またはＤＨＣＰサーバ）の中継エージェントに割り当てられた、またはＡＲＡネットワークにおける各デバイスに指定された、もしくはＡＲＡネットワークにおける各デバイスによって共有されるプレフィックスを含み得る。一部の実施形態において、制御側デバイス１０２－４（またはＤＨＣＰサーバ）は、乱数をさらに生成して、その新たなアドレスの残りの部分に関してこの乱数を使用することができる。さらに、または代替として、制御側デバイス１０２－４（またはＤＨＣＰサーバ）は、ＡＲＡネットワークに追加されるデバイスのために使用されるべき複数のアドレス（例えば、ＩＰｖ６アドレス）を予め確保して、格納していてもよい。その場合、制御側デバイス１０２－４（またはＤＨＣＰサーバ）は、要求側デバイス１０２－３に割り当てるためにその複数のアドレスからアドレスをランダムに、または順次に選択することができる。

【００６０】

さらに、または代替として、一部の実施形態において、要求側デバイス１０２－３に割り当てられるべき新たなアドレスを決定した後、制御側デバイス１０２－４（またはＤＨＣＰサーバ）は、ＤＮＳ（即ち、ドメインネームシステム）サーバにその新たなアドレスをさらに確認して、その新たなアドレスが現在、割り当てられている他のデバイスが存在するかどうかを判定することができる。一実施形態において、制御側デバイス１０２－４（またはＤＨＣＰサーバ）は、要求側デバイス１０２－３の新たなアドレスおよび識別子をＤＮＳサーバに送信することができる。制御側デバイス１０２－４（またはＤＨＣＰサーバ）が、ＤＮＳサーバから、その新たなアドレスが現在、別のデバイスに割り当てられていることを示す返信を受信した場合、制御側デバイスは、要求側デバイス１０２－３のための別の新たなアドレスを再決定して、ＤＮＳサーバにその再決定された新たなアドレスを確認して、その再決定された新たなアドレスが利用できることを確実にすることができる。その新たなアドレス、またはその再決定された新たなアドレスが利用可能である場合、ＤＮＳサーバは、その新たなアドレス、またはその再決定された新たなアドレスを要求側デバイス１０２－３の識別子と一緒に登録して、要求側デバイス１０２－３のためにその新たなアドレス、またはその再決定された新たなアドレスを確保することができる。

【００６１】

一実施形態において、要求側デバイス１０２－３に割り当てられるべき新たなアドレスを確認した後、制御側デバイス１０２－４は、要求側デバイス１０２－３に返信（例えば、ＤＨＣＰ返信）を与えることができる。例として、限定としてではなく、この返信は、割り当てられたアドレス（例えば、割り当てられたＩＰｖ６グローバルアドレス）、ＡＲＡネットワークに関連するグループ鍵（例えば、グループリンクレイヤ鍵）、および／または要求側デバイス１０２－３がＡＲＡネットワークに参加するのに、またはＡＲＡネットワークに対してセットアップするのに使用可能な構成情報もしくは構成パラメータを含み得るが、これらには限定されない。一実施形態において、制御側デバイス１０２－４（またはＤＨＣＰサーバ）は、要求側デバイス１０２－３にその返信を送信することができる。一部の実施形態において、要求側デバイス１０２－３のグローバルアドレスの知識を有して、または有さずに（例えば、その新たなアドレスが要求側デバイス１０２－３にまだ割り当てられていないので）、制御側デバイス１０２－４（またはＤＨＣＰサーバ）は、その返信を、隣接デバイス１０２－２を介して（さらに、制御側デバイス１０２－４がＡＲＡネットワークの外部に位置している場合、ＡＲＡネットワークの先頭のルータを介して）要求側デバイス１０２－３に送信することができる。例えば、制御側デバイス１０２－４（またはＤＨＣＰサーバ）は、隣接デバイス１０２－２にその返信を送信して、隣接デバイス１０２－２がその返信を要求側デバイス１０２－３に中継することを要求することができる。要求側デバイス１０２－３を相手に通信を確立した隣接デバイス１０２－２は、次に、その返信を、ＤＨＣＰｖ６プロトコルを使用するメッセージ、またはビーコ

ンメッセージを介して要求側デバイス１０２－３に中継することができる。さらに、または代替として、隣接デバイス１０２－２は、隣接デバイス１０２－２の近隣においてその返信をブロードキャストしてもよく、隣接デバイス１０２－２に隣接する要求側デバイス１０２－３が、そのブロードキャストされた返信を受信し、その返信を構文解析して、割り当てられた新たなアドレスなどの情報を獲得して、ＡＲＡネットワークに参加することができる。

【００６２】

参加要求に対する返信を受信した後、要求側デバイス１０２－３は、例えば、その返信の中に含められた構成情報または構成パラメータに基づいて、ＡＲＡネットワーク内の通信のための構成パラメータを構成することができる。例えば、要求側デバイス１０２－３は、複数のルーティングパス、および／または複数の隣接デバイスが利用可能である場合、いずれのルーティングパスおよび／または隣接デバイスを使用すべきか決定することによって、ＡＲＡネットワークに入るルーティングトポロジにアタッチされることができる。さらに、または代替として、要求側デバイス１０２－３は、例えば、ＡＲＡネットワークに要求側デバイス１０２－３の到着を通知するメッセージを、ＡＲＡネットワークのルートノードに送信してもよい。要求側デバイス１０２－３は、ルートノードからの確認応答を要求する、もしくは必要とする可能性も、要求することも必要とすることもない可能性もある。ルートノードからの確認応答が要求される、もしくは必要とされる場合、要求側デバイス１０２－３は、ルートノードから送信される確認応答を待つことができる。一実施形態において、所定の期間にわたってルートノードからの確認応答が受信されなかった場合、要求側デバイス１０２－３は、メッセージをルートノードに再送信することができる。要求側デバイス１０２－３は、確認応答が所定の回数、受信されなかったことに対してメッセージを再送信してもよい。さらに、または代替として、要求側デバイス１０２－３は、ルートノードにメッセージを転送する、または中継するのに異なるルーティングパスおよび／または異なる隣接デバイス１０２を選択してもよい。ルートノードから確認応答を受信した後、要求側デバイス１０２－３は、例えば、要求側デバイス１０２－３を宛先としないパケットをルーティングすること、および／または転送すること、要求側デバイス１０２－３にアドレス指定されたパケットを処理すること、要求側ノード１０２－３を宛先とするパケットに関して返信すること（要求された場合）などを含め、ＡＲＡネットワークにおける通常の動作を実行することを始めることができる。ルートノードからの確認応答が、所定の回数の再試行にわたって受信されない場合、要求側デバイス１０２－３は、ルートノードから確認応答が受信されているかのように通常の動作を実行すること、所定の時間間隔の後に到着メッセージを再送信すること、または隣接する別のＡＲＡネットワークが利用可能である場合、そのようなＡＲＡネットワークに移行することを決定することなどを開始することができる。

【００６３】

（例示的なデバイス移行）

一部の実施形態において、ＡＲＡネットワーク内のデバイス１０２は、そのＡＲＡネットワークから離れること、または別のＡＲＡネットワークに移行することを決定する、または開始することができる。例として、限定としてではなく、デバイス１０２は、デバイス１０２および／またはＡＲＡネットワークに関連する１または複数のネットワーク条件に基づいて、ＡＲＡネットワーク（デバイス１０２が、現在、アタッチされている）から離れること、または別のＡＲＡネットワークに移行することを決定する、または開始することができる。例えば、デバイス１０２は、デバイス１０２に対する通信品質（例えば、リンクレイヤ通信品質）が劣悪である、または低下している、例えば、所定の品質閾値を下回っている場合、ＡＲＡネットワークから別のＡＲＡネットワークに移行することを開始することができる。さらに、または代替として、デバイス１０２は、ＡＲＡネットワークのルータに障害が生じた場合、ＡＲＡネットワークから別のＡＲＡネットワークに移行してもよい。さらに、または代替として、デバイス１０２は、現在のＡＲＡネットワークにアタッチされている間、そのＡＲＡネットワークの環境をリッスンして、隣接する他の

ＡＲＡネットワークの存在を検出する、または発見することができる。デバイス１０２は、これらの隣接ネットワークによって提供されるサービス品質（ＱｏＳ）などのパフォーマンスについて知ることができる。デバイス１０２は、ＡＲＡネットワークから別のＡＲＡネットワークに、その別のＡＲＡネットワークが、デバイス１０２が現在、アタッチされているＡＲＡネットワークと比べて、サービス品質などのより良好なパフォーマンスを提供する場合、移行することが可能である。一実施形態において、デバイス１０２は、１または複数のポリシーまたは基準に基づいて、移行するための隣接するＡＲＡネットワークを選択してもよい。これらのポリシーまたは基準の例には、デバイス１０２が現在、アタッチされているＡＲＡネットワークと比べて、ＱｏＳ、待ち時間もしくは応答待ち時間、スループット、パケットドロップ率などのパフォーマンスに関して少なくとも所定の量の向上、または所定のパーセンテージの向上を提供するネットワークを選択することが含まれ得るが、以上には限定されない。

【００６４】

さらに、または代替として、デバイス１０２は、ＡＲＡネットワークにおけるデバイスの過密または過負荷、ＡＲＡネットワークに関連するパフォーマンスの低下（例えば、パケットドロップ率の増加、利用可能な帯域幅の低下、衝突率の増加など）、ＡＲＡネットワークと別のネットワークの間の負荷分散などの、ＡＲＡネットワークに関連する管理上の理由で、ＡＲＡネットワークから別のＡＲＡネットワークに移行するよう制御側デバイス１０２－４（またはＡＲＡネットワークの先頭のルータなどのＡＲＡネットワークにおけるデバイス１０２）によって強制されてもよい。さらに、または代替として、制御側デバイス１０２－４は、デバイス１０２がＡＲＡネットワークから別のＡＲＡネットワークに移行することを、そのＡＲＡネットワークがいっぱいであり（例えば、そのＡＲＡネットワークにかかっている現在の負荷が、所定の閾値以上である）、さらにそのＡＲＡネットワークに参加することを要求している新たなデバイスが、孤立したデバイスである場合、強制してもよい。

【００６５】

一実施形態において、制御側デバイス１０２－４が、あるデバイス１０２にＡＲＡネットワークを離れること、または別のＡＲＡネットワークに移行することを強制する必要があり得る場合、制御側デバイス１０２－４は、離れるべき、または移行すべきＡＲＡネットワークにおける１または複数のデバイス１０２を、ＡＲＡネットワークからデバイス１０２をランダムに選択することによって決定することができる。一部の実施形態において、制御側デバイス１０２－４は、ＡＲＡネットワークにおける各デバイスに関連する情報に基づいて、離れるべき、または移行すべき１または複数のデバイスを選択することができる。一部の実施形態において、制御側デバイス１０２－４は、ＡＲＡネットワークにおける各デバイス１０２に関連する情報を、それぞれのデバイス１０２がＡＲＡネットワークに参加する際に、格納することができる。

【００６６】

さらに、または代替として、制御側デバイス１０２－４は、ＡＲＡネットワークにおける１または複数のデバイス１０２が離れること、または別のＡＲＡネットワークに移行することを強制するように決定したことに応答して、ＡＲＡネットワークにおける各デバイスを調査することができる。さらに、または代替として、制御側デバイス１０２－４は、ＡＲＡネットワークにおけるデバイス１０２にクエリを行って、デバイス１０２のうちのいずれがＡＲＡネットワークから離れること、または移行することができるかを判定してもよい。さらに、または代替として、制御側デバイス１０２－４は、中央局１０４から、または制御側デバイス１０２－４から階層関係において上流にある任意のデバイスもしくはノードから、ＡＲＡネットワークにおける各デバイス１０２に関連するトポロジ情報を取り出してもよい。一実施形態において、各デバイス１０２に関連する情報には、それぞれのデバイス１０２が孤立したデバイスであるかどうか、それぞれのデバイス１０２が子デバイス（すなわち、それぞれのデバイス１０２から階層関係において下流にあるデバイス）を有するかどうか、それぞれのデバイス１０２がいくつの子デバイスを有するかなど

が含まれ得るが、以上には限定されない。

【００６７】

ＡＲＡネットワークにおける各デバイス１０２に関連する情報を取り出したこと、またはＡＲＡネットワークにおけるデバイスから返信を受信したことに応答して、制御側デバイス１０２－４は、１または複数のヒューリスティクス戦略（heuristics strategies）に基づいて、離れるべき、または移行すべきＡＲＡネットワークにおける１または複数のデバイス１０２を選択することができる。例として、限定としてではなく、制御側デバイス１０２－４は、その情報に孤立していないことが示される１または複数のデバイス１０２を選択することができる。さらに、または代替として、制御側デバイス１０２－４は、有する子デバイスの数がより少ない、例えば、所定の閾値数より少ない１または複数のデバイス１０２を選択してもよい。さらに、または代替として、制御側デバイス１０２－４は、閾値数より少ない数の子デバイスを有する所定の数（例えば、１、２など）の最初のいくつかのデバイス１０２を選択してもよい。さらに、または代替として、制御側デバイス１０２－４は、例えば、ルーティング情報に基づいて、制御側デバイス１０２－４から最も遠く離れた１または複数のデバイスを選択してもよい。

【００６８】

ＡＲＡネットワークから離れるべき、または移行すべき１または複数のデバイス１０２を選択した後、制御側デバイス１０２－４は、ＡＲＡネットワークから離れる、または移行する指示または要求をその１または複数のデバイス１０２に送信することができる。一実施形態において、制御側デバイス１０２－４は、その指示または要求をデバイス１０２に送信し、このデバイス１０２が、何らかの理由で（例えば、最初のデバイスが、現在のＡＲＡネットワークを離れることを強制されたとした場合、孤立することになる）ＡＲＡネットワークから離れる、または移行することができない場合、別のデバイス１０２にその指示または要求を送信することができる。一部の実施形態において、制御側デバイス１０２－４が、複数の（または所定の数の）デバイス１０２にその指示または要求を送信して、前に送信された指示または要求が前に指示された、または要求されたデバイスによって満たされ得ない場合に、他のデバイス１０２にその指示または要求を再送信する問題を回避することができる。

【００６９】

特定の一実施例として、制御側デバイス１０２－４が、ＡＲＡネットワークから離れるよう、または移行するようデバイス１０２－５を選択することができる。移行指示または移行要求を受信したことに応答して、デバイス１０２－５は、デバイス１０２－５が移行することが可能な他の１または複数のＡＲＡネットワークが存在するかどうかを判定することができる。例えば、デバイス１０２－５は、発見モジュール２１２およびブロードキャストモジュール２１４を使用して、他のＡＲＡネットワークに属する隣接デバイスが存在するかどうかを判定することができる。デバイス１０２－５が、移行すべき他のＡＲＡネットワークを見出すことができない場合、デバイス１０２－５は、制御側デバイス１０２－４のＡＲＡネットワークを離れることを、そうすることにより、デバイス１０２－５が孤立することになるので、拒否するメッセージを制御側デバイス１０２－４に送信することができる。

【００７０】

代替として、デバイス１０２－５は、別のＡＲＡネットワークを検出するが、この別のＡＲＡネットワークとの通信の品質が劣悪である、または散発的であると決定することができる。その事例において、デバイス１０２－５は、デバイス１０２－５がＡＲＡネットワークから離れることも、移行することもできないことを示すメッセージを制御側デバイス１０２－４に送信することができる。さらに、または代替として、移行指示または移行要求を受信した時点で、デバイス１０２－５は、デバイス１０２－５が、所定の時間閾値以上の或る期間を必要とする可能性があるデータを処理すること、受信すること、および／または送信することで忙しいと決定する可能性がある。このことに応答して、デバイス１０２－５は、デバイス１０２－５がＡＲＡネットワークから離れることも、移行するこ

ともできないというメッセージを制御側デバイス１０２－４に送信することができる。一実施形態において、デバイス１０２－５は、デバイス１０２－５がＡＲＡネットワークから離れる、または移行することにより、デバイス１０２－５が孤立することになる場合、デバイス１０２－５がＡＲＡネットワークから離れることも、移行することも強制されないことを例外として、そのような移行の結果に関わらず、ＡＲＡネットワークから離れる、または移行することを強制されることができる。

【００７１】

一実施形態において、デバイス１０２－５が、別のＡＲＡネットワークを検出し、さらにデバイス１０２－５が、ＡＲＡネットワークから離れること、または移行することができる場合、デバイス１０２－５は、前段の例示的なデバイス登録セクションにおいて説明されるとおり、その別のＡＲＡネットワークに参加することを開始することができる。例えば、デバイス１０２－５は、隣接するＡＲＡネットワークに属する隣接デバイス１０２に、その隣接ネットワークに参加することを要求する要求（前述の実施形態において説明されるとおり、暗号化鍵および／または暗号化アルゴリズムを使用して暗号化されても、暗号化されなくてもよい）を送信することができる。さらに、デバイス１０２－５は、デバイス１０２－５がネットワークを離れることを示すメッセージを、デバイス１０２－５が離れつつある、もしくは移行しつつある元のネットワークにおけるデバイス１０２にさらにブロードキャストすることができる。一部の実施形態において、デバイス１０２－５は、制御側デバイス１０２－４のＡＲＡネットワークに参加する際に、それまでにＮＭＳに登録することに成功しているので、デバイス１０２－５は、新たなＡＲＡネットワークに参加する際に、前述した認証プロセスの一部または全てを免除され得る（例えば、そのＡＲＡネットワークに関連するグループ鍵、および／またはデバイス１０２－５のデバイス識別子を、その別のＡＲＡネットワークの制御側デバイスに供給することによって）。

【００７２】

一実施形態において、デバイス１０２－５は、その別のＡＲＡネットワークに指定された特定のプレフィックス（例えば、ＩＰｖ６プレフィックス）を含む新たなアドレスを受信することができる。その新たなアドレスを受信した後、デバイス１０２－５は、デバイス１０２－５の古いアドレス（すなわち、制御側デバイス１０２－４によってデバイス１０２－５に以前に割り当てられたアドレス）を、米国国家規格協会（ＡＮＳＩ）Ｃ１２．２２、ＤＮＳにおいてなど、アプリケーションレベルにおいて、その新たなアドレスで更新することができる。

【００７３】

一実施形態において、移行の期間中、および移行の完了前に、デバイス１０２－５は、デバイス１０２－５が現在、アタッチされている、または最初にアタッチされたＡＲＡネットワークに対する接続またはアタッチメントを維持することができる。例えば、デバイス１０２－５は、デバイス１０２－５を宛先としないパケットをルーティングすること、および転送すること、デバイス１０２－５にアドレス指定されたパケットを処理すること、要求された場合、現在のＡＲＡネットワークを介してデバイス１０２－５を宛先とするパケットに返信することなどを含め、現在のＡＲＡネットワークにおける通常の動作を依然として実行することができる。さらに、または代替として、デバイス１０２－５は、新たなＡＲＡネットワークから隣接デバイス１０２を選択し、この隣接デバイス１０２を、データパケットに関する中継器および／または転送するデバイスとして使用してもよい。さらに、または代替として、デバイス１０２－５は、ＡＲＡネットワークにおける他のデバイス１０２からの、デバイス１０２－５の古いアドレスを宛先とするデータパケットを依然として受信することができる。一部の実施形態において、移行の期間中、デバイス１０２－５は、デバイス１０２－５の古いアドレスを格納して、もしくはキャッシュして、デバイス１０２－５の古いアドレスにアドレス指定されたデータまたはデータパケットを引き続き通常どおり処理し、このため、移行のこの期間中、デバイス１０２－５が移行する元のＡＲＡネットワークとの接続を維持することができる。一実施形態において、デバイス１０２－５が、移行する元のＡＲＡネットワークのデバイス１０２－５の親デバイス

との接続を失った場合、デバイス１０２－５は、例えば、デバイス１０２－５のバッファから全ての上流パケット（そのＡＲＡネットワークのより上位の階層レベルにおけるデバイスに送信されるデータパケット）をドロップすることができる。一部の実施形態において、デバイス１０２－５は、移行の期間中、受信されたデータパケットを、デバイス１０２－５が移行している元のＡＲＡネットワークに転送することができる（依然としてアタッチされている場合）。一実施形態において、デバイス１０２－５が、デバイス１０２－５の新たなアドレスを受け取り、現時点でその別のＡＲＡネットワーク（すなわち、新たなＡＲＡネットワーク）にアタッチされている場合、デバイス１０２－５は、バッファリングされたデータパケット、すなわち、デバイス１０２－５の「古い」ＡＲＡネットワークから来るデータパケットを、例えば、新たなＡＲＡネットワークを介してデバイス１０２－５の新たなアドレスを使用して、「トンネリング」し、それらの受信されたデータパケット（例えば、新たなパケットの中に含められる、またはカプセル化される）を送信することができる。

【００７４】

一実施形態において、新たなＡＲＡネットワークにアタッチされること、または移行することに成功した後、デバイス１０２－５は、古いＡＲＡネットワークから自らをデタッチする、または離れる。一実施形態において、デバイス１０２－５は、古いＡＲＡネットワークのルートノードに、古いＡＲＡネットワークからのデバイス１０２－５の離脱を通知する、または告知するメッセージを送信することができる。さらに、または代替として、デバイス１０２－５は、デバイス１０２－５経由でデータパケットを転送し、さらに／またはルーティングする古いＡＲＡネットワークにおける１または複数のデバイス１０２にメッセージ（古いＡＲＡネットワークからのデバイス１０２－５の離脱を示す）を送信することができる。これらのメッセージ（すなわち、古いＡＲＡネットワークにおけるルートノードおよび／またはその他のデバイス１０２に対するメッセージ）は、古いＡＲＡネットワークにおけるルートノードおよび／またはその他のデバイス１０２から確認応答を要求することも、要求しないこともできる。さらに、一部の実施形態において、デバイス１０２－５は、これらのメッセージを古いＡＲＡネットワークにおけるルートノードおよび／またはその他のデバイス１０２に繰り返し送信して、ルートノードおよび／またはその他のデバイス１０２がこれらのメッセージを受信する見込みを高める、または確実にすることができる。

【００７５】

さらに、または代替として、デバイス１０２－５は、デバイス１０２－５の古いアドレスを宛先とするいずれのデータパケットも処理することを停止することができる。一実施形態において、デバイス１０２－５は、データパケットが、例えば、デバイス１０２－５の古いアドレスを宛先とするデータパケット、および／または高い度合の緊急性もしくは重要性（応答が必要とされる時刻によって示される）を示すデータパケット（デバイス１０２－５の古いアドレスを宛先とすることも、宛先としないことも可能である）である場合、データパケットを処理することを選択することが可能である。さらに、または代替として、デバイス１０２－５は、データパケットがデバイス１０２－５の古いアドレスを宛先とする場合、特定の意図または目的を有するいくつかのタイプのデータパケットに応答することを選択してもよい。例として、限定としてではなく、デバイス１０２－５は、事前定義されたセットのアプリケーションを宛先とするデータを伝送するとともに、デバイス１０２－５からの応答を要求するデータパケットを処理することができる。デバイス１０２－５は、新たなＡＲＡネットワークを介して応答を送信するとともに、その新たなＡＲＡネットワークにおけるデバイス１０２－５の新たなアドレスを応答の送信元アドレスとして使用することができる。さらに、または代替として、デバイス１０２－５は、特定の意図のデータパケットでも、事前定義されたセットのアプリケーションを宛先とするデータパケットでもないデータパケットを無視する、またはドロップすることができる。一部の実施形態において、デバイス１０２－５が、古いＡＲＡネットワークからデタッチされ、新たなＡＲＡネットワークにおける通常の動作を実行しているとき、デバイス１０２

－５は、古いＡＲＡネットワークもしくは新たなＡＲＡネットワークによってデフォルトであり得る、または古いＡＲＡネットワークもしくは新たなＡＲＡネットワークの管理者によって事前定義され得る所定の期間にわたって、古いアドレスを宛先とするパケットを依然として受け付けることができる。デバイス１０２－５は、前段で説明される前述の実施形態により、デバイス１０２－５の古いアドレス（および／またはデバイス１０２－５の古いアドレスを宛先としないデータパケット）を処理することができる。

【００７６】

一部の実施形態において、デバイス１０２－５の古いアドレスは、移行期間と呼ばれる、或る期間中、別のデバイスに再割り振りされることはない。この移行期間は、システム全体（例えば、古いＡＲＡネットワークおよび新たなＡＲＡネットワークのルートノード、ＤＮＳサーバなどを含む）が、デバイス１０２－５の移行を反映するように更新されるまで、ＡＲＡ切り換えプロセス全体に及ぶだけ十分に長く設定される。

【００７７】

（代替の実施形態）

前述の実施形態は、ＡＭＩ（Advanced Metering Infrastructure）の自律的ルーティングエリアネットワークにおける応用例を説明するものの、本開示は、そのような応用例に限定されない。一実施形態において、本開示は、セルラネットワーク、ホームネットワーク、オフィスネットワークなどのネットワークに適用され得る。例えば、セルラ局が、セルラ局によって制御されるセルラネットワークにかかる負荷が所定の閾値を超えたと決定した場合に、セルラ局は、セルラ局のネットワークに接続されたモバイルデバイスのうちのいくつかを選択して、離脱するよう、または別のセルラネットワークに移行するよう強制して、その結果、セルラ局によって制御されるネットワークに関する負荷分散を実行することができる。

【００７８】

（例示的な方法）

図３は、ネットワークにおけるデバイス登録の例示的な方法３００を示す流れ図である。図４は、デバイスがネットワークに参加することを許可するか、または拒否するかの判定の例示的な方法４００を示す流れ図である。図５は、ネットワークからのデバイス移行の例示的な方法５００を示す流れ図である。図３、図４および図５の方法は、図１の環境において、図２のデバイスを使用して実施され得るが、そうでなくてもよい。説明を容易にするため、方法３００、４００および５００は、図１および図２を参照して説明される。しかし、方法３００、４００および５００は、代替として、他の環境において、さらに／または他のシステムを使用して実施されてもよい。

【００７９】

方法３００、４００および５００は、コンピュータ実行可能命令の一般的な脈絡で説明される。一般に、コンピュータ実行可能命令には、特定の機能を実行する、または特定の抽象データ型を実装するルーチン、プログラム、オブジェクト、構成要素、データ構造、プロシージャ、モジュール、関数などが含まれ得る。また、これらの方法は、通信ネットワークを介して結び付けられた遠隔処理デバイスによって機能が実行される分散コンピューティング環境において実施されることも可能である。分散コンピューティング環境において、コンピュータ実行可能命令は、メモリストレージデバイスを含む、ローカルコンピュータ記憶媒体および／または遠隔コンピュータ記憶媒体の中に配置され得る。

【００８０】

例示的な方法は、ハードウェアとして、ソフトウェアとして、ファームウェアとして、または以上の組み合わせとして実装され得る一連の動作を表すロジカルフローグラフ（logical flow graph）におけるブロックを集めたものとして示される。これらの方法が説明される順序は、限定として解釈されることは意図しておらず、任意の数の説明される方法ブロックが、これらの方法、または代替の方法を実施するように任意の順序で組み合わされることが可能である。さらに、個々のブロックは、本明細書で説明される主題の趣旨および範囲を逸脱することなく、方法から省かれてもよい。ソフトウェアの脈絡で、ブロッ

クは、１または複数のプロセッサによって実行されたとき記載される動作を実行するコンピュータ命令を表す。

【００８１】

図３を再び参照すると、ブロック３０２で、要求側デバイス１０２－３は、要求側デバイス１０２－３が位置するエリアを範囲に含むネットワークに参加することを所望することができる。要求側デバイス１０２－３は、隣接デバイス１０２－２を発見することが可能であり、隣接デバイス１０２－２に参加要求（例えば、参加する要求を含むＤＨＣＰｖ６要求またはビーコンメッセージ）を送信する。

【００８２】

ブロック３０４で、参加要求を受信したことに応答して、隣接デバイス１０２－２は、その要求を解析し、要求側デバイス１０２－３が、隣接デバイス１０２－２がメンバであるネットワークに参加することを要求すると決定することができる。

【００８３】

ブロック３０６で、要求側デバイス１０２－３がそのネットワークに参加することを要求すると決定したことに応答して、隣接デバイス１０２－２は、オプションとして、その参加要求を選別することができる。一実施形態において、隣接デバイス１０２－２は、その参加要求をネットワークの他のデバイスに中継すべきかどうかを判定することができる。例えば、隣接デバイス１０２－２は、孤立したデバイス以外、いずれのデバイスも、ネットワークの過密または過負荷などの管理上の理由またはネットワーキング上の理由でネットワークに受け付けられ得ないという指示または要求を、制御側デバイス１０２－４から受信していることができる。この事例において、隣接デバイス１０２－２は、例えば、参加要求の中に含められた情報に基づいて、要求側デバイス１０２－３が孤立したデバイスであるかどうかを判定することができる。一実施形態において、隣接デバイス１０２－２が、孤立したデバイス以外、いずれのデバイスもネットワークに受け付けられ得ないという指示もしくは要求を受信しており、さらに要求側デバイス１０２－３が、孤立したデバイスではない場合、隣接デバイス１０２－２は、参加要求が拒否されたことを示す応答を要求側デバイス１０２－３に送信することができる。そうでない場合には、隣接デバイス１０２－２は、要求側デバイス１０２－３の参加要求をネットワークの他のデバイスに中継する準備をすることができる。

【００８４】

ブロック３０８で、要求側デバイス１０２－３は、要求側デバイス１０２－３の参加要求が拒否されたことを示す応答を隣接デバイス１０２－２から受信する。

【００８５】

ブロック３１０で、隣接デバイス１０２－２は、参加要求を、隣接デバイス１０２－２が制御側デバイス１０２－４のアドレスを知っているかどうかに基づいて、制御側デバイス１０２－４、または隣接デバイス１０２－２の親デバイスに中継することができる。

【００８６】

ブロック３１２で、隣接デバイス１０２－２から中継された参加要求を受信したことに応答して、制御側デバイス１０２－４は、要求側デバイス１０２－３の参加要求を許可するか、または拒否するかを判定することができる。一実施形態において、制御側デバイス１０２－４は、ネットワークの条件、および／または要求側デバイス１０２－３の条件に基づいて、参加要求を許可するかどうかを判定することができる。制御側デバイス１０２－４が、要求側デバイス１０２－３の参加要求を拒否すると決定した場合、制御側デバイス１０２－４は、制御側デバイス１０２－４またはネットワークが、要求側デバイス１０２－３が参加することを許可することができないことを示す返信を、隣接デバイス１０２－２を介して要求側デバイス１０２－３に送信することができる。

【００８７】

ブロック３１４で、要求側デバイス１０２－３の要求を許可すると決定したことに応答して、制御側デバイス１０２－４は、要求側デバイス１０２－３の参加要求の中に含められた要求側デバイス１０２－３の識別子および／または認証署名を含むメッセージを認証

サーバ（例えば、ＡＡＡサーバ１２０）に送信することができる。一実施形態において、制御側デバイス１０２－４は、ネットワークに関連するグループ鍵、または制御側デバイス１０２－４に関連する暗号化鍵を使用して、そのメッセージにさらに署名する、またはそのメッセージをさらに暗号化することができる。

【００８８】

ブロック３１６で、メッセージを受信した後、認証サーバ１２０は、暗号化されている場合、メッセージを解読し、さらにメッセージを構文解析して、要求側デバイス１０２－３の識別子および／または認証署名を獲得することができる。次に、認証サーバ１２０は、要求側デバイス１０２－３の獲得された識別子、および／または獲得された認証署名に基づいて、認証を実行することができる。要求側デバイス１０２－３のＩＤを認証することに成功したことに応答して、認証サーバ１２０は、場合により、ネットワークに関連するグループ鍵（要求側デバイス１０２－４の公開鍵または対称鍵を使用して暗号化されても、暗号化されなくてもよい）を含む認証成功メッセージを制御側デバイス１０２－４に送信することができる。一実施形態において、要求側デバイス１０２－４の公開鍵または対称鍵は、要求側デバイス１０２－４と認証サーバ１２０だけにしか知られていないことが可能である。一部の実施形態において、要求側デバイス１０２－４の公開鍵または対称鍵は、ネットワーク管理またはネットワーク監視を担うＡＲＡネットワークの他のデバイスまたは他のサーバ（例えば、中央局１０４および／または制御側デバイス１０２－４など）にさらに知られていることが可能である。例えば、認証サーバ１２０は、ＡＲＡネットワークに関連するグループ鍵で暗号化されている、要求側デバイス１０２－４の公開鍵または対称鍵をさらに含む認証成功メッセージを送信することができる。代替として、認証サーバ１２０が要求側デバイス１０２－３のＩＤを認証できなかった場合、認証サーバ１２０は、認証が失敗したことを示す認証失敗メッセージを制御側デバイス１０２－４に送信してもよい。

【００８９】

ブロック３１８で、認証サーバ１２０からメッセージを受信したことに応答して、制御側デバイス１０２－４は、要求側デバイス１０２－３のＩＤの認証が成功したかどうかを判定することができる。失敗した場合、制御側デバイス１０２－４は、要求側デバイス１０２－３の参加要求が拒否されたことを示す返信を、隣接デバイス１０２－２を介して要求側デバイス１０２－３に送信することができる。要求側デバイス１０２－３のＩＤの認証が成功したと決定したことに応答して、制御側デバイス１０２－４は、要求側デバイス１０２－３の参加要求が許可されることを示すメッセージを含む受け付け応答を、隣接デバイス１０２－２を介して要求側デバイス１０２－３に送信することができる。一実施形態において、応答は、要求側デバイス１０２－３の公開鍵または対称鍵を使用して認証サーバにおいて暗号化されても、されなくてもよいネットワークに関連するグループ鍵をさらに含み得るが、そのようなグループ鍵には限定されない。さらに、または代替として、一部の実施形態において、制御側デバイス１０２－４は、制御側デバイス１０２－４が、例えば、認証サーバ１２０から要求側デバイス１０２－３の公開鍵または対称鍵を知っている場合、要求側デバイス１０２－３の公開鍵または対称鍵を使用して応答を暗号化してもよい。さらに、または代替として、一部の実施形態において、制御側デバイス１０２－４は、要求側デバイス１０２－３の公開鍵または対称鍵を使用して（この公開鍵または対称鍵が制御側デバイス１０２－４に知られている場合）グループ鍵（および／またはネットワークに参加することと関係する他の情報）を暗号化し、さらにネットワークに関連するグループ鍵を使用して、暗号化されたグループ鍵および／またはメッセージを暗号化してもよい。一部の実施形態において、制御側デバイス１０２－４は、要求側デバイス１０２－３の公開鍵または対称鍵を使用してグループ鍵およびメッセージを暗号化し、さらにグループ鍵を使用して、暗号化されたグループ鍵、暗号化されたメッセージ、および／または他の情報（要求側デバイス１０２－３に応答をルーティングすることを可能にする情報、例えば、隣接デバイス１０２－２のアドレス、および／または要求側デバイス１０２－３のＩＤなど）をさらに暗号化することができる。

【００９０】
一部の実施形態において、制御側デバイス１０２－４は、認証サーバ１２０から要求側デバイス１０２－３のＩＤ認証成功を受信した後（すなわち、要求側デバイス１０２－３のＩＤの認証が成功したと決定した後）、要求側デバイス１０２－３に受け付け応答を送信しなくてもよい。これらの代替の実施形態において、制御側デバイス１０２－４は、オプションとして、後段のブロック３２４で説明されるとおり、要求側デバイス１０２－３をＮＭＳまたは中央局１０４に登録する登録要求をＮＭＳに送信することができる。
【００９１】
ブロック３２０で、隣接デバイス１０２－２は、制御側デバイス１０２－４から送信された受け付け応答を受信し、解析することができる。一実施形態において、この応答が、ネットワークに関連するグループ鍵を使用して暗号化されている場合、隣接デバイス１０２－２は、暗号化された応答を解読することができる。一実施形態において、受け付け応答が、要求側デバイス１０２－３の参加要求と関係する応答であると決定したことに応答して、隣接デバイス１０２－２は、この応答の一部または全体を要求側デバイス１０２－３に中継することができる。例えば、隣接デバイス１０２－２は、要求側デバイス１０２－３の公開鍵または対称鍵を使用して暗号化されたこの応答の一部を要求側デバイス１０２－３に中継することができる。
【００９２】
ブロック３２２で、要求側デバイス１０２－３は、隣接デバイス１０２－２から中継された応答を受信し、さらにこの応答を解析して、参加要求の結果、および／またはネットワークのグループ鍵（含まれる場合）を取り出す。要求側デバイス１０２－３は、そのグループ鍵を使用してネットワークの他のデバイスからデータを受信すること、および／またはそのようなデバイスにデータを送信することを開始することができる。
【００９３】
ブロック３２４で、制御側デバイス１０２－４は、オプションとして、要求側デバイス１０２－３をＮＭＳまたは中央局１０４に登録する登録要求をＮＭＳに送信することができる。この登録要求は、要求側デバイス１０２－３の識別子を含み得るが、そのような識別子には限定されない。
【００９４】
ブロック３２６で、制御側デバイス１０２－４から登録要求を受信したことに応答して、ＮＭＳは、ネットワークに関連する情報、およびネットワークにおける要求側デバイス１０２－３に関連する情報、または他のデバイスからの情報を獲得することができる。ＮＭＳは、獲得された情報に基づいて、要求側デバイス１０２－３のために使用可能な構成情報または構成パラメータを決定することができる。例えば、ＮＭＳは、要求側デバイス１０２－３のタイプ、ネットワークのタイプなどに基づいて、要求側デバイス１０２－３のために使用可能な構成情報または構成パラメータを決定することができる。構成情報または構成パラメータを決定した後、ＮＭＳは、その構成情報または構成パラメータを制御側デバイス１０２－４に送信することができる。
【００９５】
ブロック３２８で、ＮＭＳから構成情報または構成パラメータを獲得したことに応答して、制御側デバイス１０２－４は、要求側デバイス１０２－３に新たなアドレスを割り当てることができる。一実施形態において、制御側デバイス１０２－４は、ネットワークに規定された、または指定されたプレフィックスを含む新たなアドレスを割り当てることができる。制御側デバイス１０２－４は、要求側デバイス１０２－３に対する返信（例えば、ＤＨＣＰ返信）をさらに準備することができる。一実施形態において、この返信は、割り当てられた新たなアドレス、構成情報もしくは構成パラメータ、および／またはネットワークに関連するグループ鍵を含み得るが、以上には限定されない。一実施形態において、制御側デバイス１０２－４が、要求側デバイス１０２－３のＩＤの認証が成功したと決定した直後に、要求側デバイス１０２－３に受け付け応答を送信していない場合、制御側デバイス１０２－４からこの返信を送信することによって、要求側デバイス１０２－３の

ＩＤの認証が成功したことを示すことが可能である。一部の実施形態において、制御側デバイス１０２－４は、要求側デバイス１０２－３のＩＤの認証と関係する認証サーバ１２０から受信された情報をこの返信にさらにマージすることができる。一部の実施形態において、制御側デバイス１０２－４は、隣接デバイス１０２－２（および、制御側デバイスがネットワークの外部に位置する場合、ネットワークの先頭のルータ）を介してこの返信を要求側デバイス１０２－３に送信することができる。

【００９６】

ブロック３３０で、隣接デバイス１０２－２は、制御側デバイス１０２－４からの返信を要求側デバイス１０２－３に中継する。

【００９７】

ブロック３３２で、要求側デバイス１０２－３が、返信の中で受信された情報（例えば、グループ鍵、割り当てられたアドレス、および／または構成情報もしくは構成パラメータ）を使用してネットワークに参加することに成功し、ネットワークに登録される。一実施形態において、要求側デバイス１０２－３は、要求側デバイス１０２－３の対称鍵もしくは非対称鍵が要求側デバイス１０２－３自らと許可された１または複数のデバイスおよび／またはサーバ（例えば、認証サーバ１２０、中央局１０４、および／または制御側デバイス１０２－４）だけにしか知られていない場合、ネットワークをさらに認証することができる。例えば、返信の中に含められたグループ鍵が、要求側デバイス１０２－３の対称鍵または非対称鍵（例えば、公開鍵）を使用して暗号化されることが可能である。従って、要求側デバイス１０２－３が、要求側デバイス１０２－３の対称鍵または非対称鍵（例えば、秘密鍵）を使用して、暗号化されたグループ鍵を解読することができ、さらにその解読されたグループ鍵を使用してＡＲＡネットワークの他のデバイスとうまく通信することができる場合、要求側デバイス１０２－３はネットワークを認証することができる。しかし、要求側デバイス１０２－３が、その解読されたグループ鍵を使用して他のデバイスとデータを通信することができない場合、要求側デバイス１０２－３は、ネットワークの認証が失敗したと決定し、それに相応してネットワークを離れる（またはネットワークから切断する）ことができる。

【００９８】

図４を再び参照すると、ブロック４０２で、制御側デバイス１０２－４は、隣接デバイス１０２－２を介して要求側デバイス１０２－３から要求を受信することができる。要求側デバイス１０２－３は、ネットワーク内に新たに展開されたデバイス、または別のネットワークからそのネットワークに移行しようと試みているデバイスを含み得る。一実施形態において、制御側デバイス１０２－４は、要求側デバイス１０２－３の要求が制御側デバイス１０２－４に関連付けられたネットワークに参加することを要求する参加要求であると決定することができる。この参加要求は、要求側デバイス１０２－３が孤立したデバイスであるかどうかについての情報を少なくとも含み得る。一部の実施形態において、この参加要求は、要求側デバイス１０２－３のＩＤなどをさらに含み得るが、そのようなＩＤなどには限定されない。一部の実施形態において、この参加要求は、要求側デバイス１０２－３の秘密鍵または対称鍵によって暗号化される、または署名されることが可能である。制御側デバイス１０２－４は、要求が暗号化されている場合、要求側デバイス１０２－３の公開鍵または対称鍵を使用して要求を解読することができる。

【００９９】

ブロック４０４で、要求が参加要求であると決定したことに応答して、制御側デバイス１０２－４は、ネットワークがさらなるデバイスを収容する容量を有するかどうかを判定することができる。例えば、制御側デバイス１０２－４は、ネットワークに関連する負荷が所定の閾値以上であるかどうかを判定することができる。ネットワークに関連する負荷には、デバイスの現在の数、現在のトラフィック、現在もしくは平均のパケットドロップ率、現在もしくは平均の帯域幅使用率などが含まれ得るが、以上には限定されない。

【０１００】

ブロック４０６で、制御側デバイス１０２－４が、ネットワークがさらなるデバイスを

収容できる、例えば、負荷が所定の閾値未満であると決定した場合、制御側デバイス１０２－４は、他のデバイスおよび／または他のサーバに対して、前述の実施形態、例えば、図３で説明されるとおり、要求側デバイス１０２－３の参加要求を処理することに進むことができる。

【０１０１】

ブロック４０８で、制御側デバイス１０２－４が、ネットワークがさらなるデバイスを収容できない、例えば、負荷が所定の閾値を超えていると決定した場合、制御側デバイス１０２－４は、要求側デバイス１０２－３が、例えば、参加要求の中に含められた情報に基づいて、孤立したデバイス１０２－３であるかどうかを判定することができる。

【０１０２】

ブロック４１０で、制御側デバイス１０２－４が、要求側デバイス１０２－３が孤立したデバイスではないと決定した場合、制御側デバイス１０２－４は、要求側デバイス１０２－３の参加要求を拒否し、隣接デバイス１０２－２を介して要求側デバイス１０２－３に拒否の応答を送信することができる。

【０１０３】

ブロック４１２で、制御側デバイス１０２－４が、要求側デバイス１０２－３が孤立したデバイスであると決定した場合、制御側デバイス１０２－４は、他のデバイスおよび／または他のサーバに対して、前述の実施形態、例えば、図３で説明されるとおり、要求側デバイス１０２－３の参加要求を処理することに進むことができる。さらに、制御側デバイス１０２－４は、ネットワークの１または複数のデバイスが、前述の実施形態において説明され、さらに図５および後段の付随する説明において説明されるとおり、ネットワークの１または複数のデバイスがネットワークから離れること、または移行することを強制することができる。

【０１０４】

図５を再び参照すると、ブロック５０２で、制御側デバイス１０２－４は、１または複数のデバイス１０２がネットワークから離れる、または移行することを強制することを決定する。制御側デバイス１０２－４は、ネットワークの負荷分散、孤立したデバイスの、既に過負荷になったネットワークに参加する要求などの、１または複数の理由に基づいて、この決定を行うことができる。

【０１０５】

ブロック５０４で、制御側デバイス１０２－４は、１または複数のヒューリスティクス戦略に基づいて、離れるべき、または移行すべきネットワークにおける１または複数のデバイス１０２を選択することができる。この１または複数のヒューリスティクス戦略には、孤立していないデバイスを選択すること、子デバイスを有さない、もしくは有する子デバイスの数がより少ないデバイスを選択すること、制御側デバイスから通信上、最も遠く離れたデバイスを選択することが含まれ得るが、以上には限定されない。

【０１０６】

ブロック５０６で、離れるべき、または移行すべき１または複数のデバイスを選択した後、制御側デバイス１０２－４は、その１または複数のデバイスがネットワークから離れること、または移行することを強制する、または要求する指示または要求をその１または複数のデバイスに送信することができる。

【０１０７】

ブロック５０８で、移行指示または移行要求を受信したことに応答して、その１または複数のデバイス、例えば、デバイス１０２－５は、デバイス１０２－５がネットワークから離れること、または移行することができると決定することができる。一実施形態において、デバイス１０２－５は、デバイス１０２－５が位置しているエリア内に１または複数のネットワーク（デバイス１０２－５が、現在、メンバであるネットワーク以外の）が存在するかどうかを検出すること、または発見することによって、デバイス１０２－５が、現在、孤立したデバイスであるかどうかを判定することができる。デバイス１０２－５は、デバイス１０２－５が離れること、または別のネットワークに移行することができない

と決定したことに応答して、制御側デバイス１０２－４にメッセージを送信することができる。

【０１０８】

ブロック５１０で、１または複数のネットワーク（デバイス１０２－５が、現在、メンバであるネットワーク以外の）が存在すると決定したことに応答して、デバイス１０２－５は、例えば、図３に関連して前述したとおり、その１または複数のネットワークのうちの１のネットワークに参加することを開始することができる。さらに、デバイス１０２－５は、デバイス１０２－５がネットワークから離れつつある、または移行しつつあるというメッセージを、そのネットワークにおけるデバイス１０２にさらにブロードキャストすることができる。

【０１０９】

ブロック５１２で、移行の期間中、および移行の完了前に、デバイス１０２－５の「古い」アドレス（すなわち、デバイス１０２－５が離れつつある、または移行しつつある元のネットワークによってデバイス１０２－５に割り当てられたアドレス）を宛先とするデータパケットを受信したことに応答して、デバイス１０２－５は、それらのデータパケットをドロップすること、またはそれらのデータパケットを、デバイス１０２－５が依然として接続されているネットワークにおける他のデバイスに転送することができる。

【０１１０】

ブロック５１４で、新たなアドレスを獲得することに成功し、新たなネットワークにアタッチされた後、デバイス１０２－５は、新たなネットワークにおいて通常の、または割り当てられた動作または機能を実行することを始めることができる。

【０１１１】

図５は、デバイス１０２－５が、制御側デバイス１０２－４によってＡＲＡネットワークから離れること、または移行することを強制され得る、または指示され得ることを説明するものの、一部の実施形態において、デバイス１０２－５は、実際には、ＡＲＡネットワークから離れること、またはＡＲＡネットワークから別のＡＲＡネットワークに移行することを自ら開始する。例として、限定としてではなく、デバイス１０２－５は、デバイス１０２－５および／またはＡＲＡネットワークに関連する１または複数のネットワーク条件に基づいて、ＡＲＡネットワークから離れること、またはＡＲＡネットワークから別のＡＲＡネットワークに移行することを決定する、または開始することができる。例えば、デバイス１０２－５は、デバイス１０２－５に対する通信品質（例えば、リンクレイヤ通信品質）が劣悪である、または低下している、例えば、所定の品質閾値を下回っている場合、そのＡＲＡネットワークから別のＡＲＡネットワークに移行することを開始することができる。さらに、または代替として、デバイス１０２－５は、ＡＲＡネットワークのルータに障害が生じた場合、そのＡＲＡネットワークから別のＡＲＡネットワークに移行してもよい。さらに、または代替として、デバイス１０２－５は、現在のＡＲＡネットワークにアタッチされている間、そのＡＲＡネットワークの環境をリッスンして、隣接する他のＡＲＡネットワークの存在を検出する、または発見することができる。デバイス１０２－５は、これらの隣接ネットワークによって提供されるパフォーマンス／サービス品質について知ることができる。デバイス１０２－５は、別のＡＲＡネットワークが、デバイス１０２－５が現在アタッチされているＡＲＡネットワークと比べて、より良好なパフォーマンス／サービス品質を提供する場合、ＡＲＡネットワークからその別のＡＲＡネットワークに移行することができる。

【０１１２】

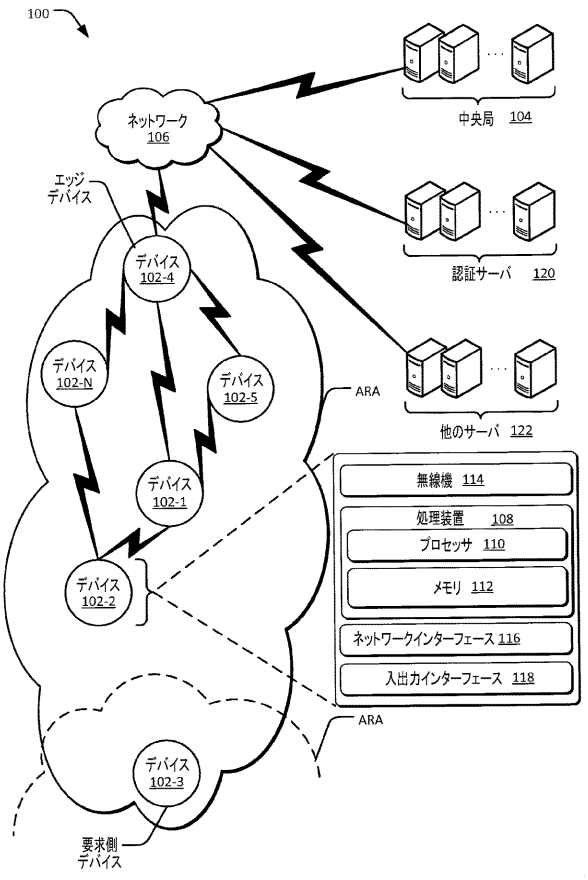
本明細書で説明されるいずれの方法のうちのいずれの動作も、少なくとも部分的には、１または複数のコンピュータ可読媒体上に格納された命令に基づいてプロセッサまたは他の電子デバイスによって実施され得る。例として、限定としてではなく、本明細書で説明されるいずれの方法のうちのいずれの動作も、１または複数のコンピュータ記憶媒体などの１または複数のコンピュータ可読媒体上に格納され得る実行可能命令で構成された１または複数のプロセッサの制御下で実施され得る。

【０１１３】

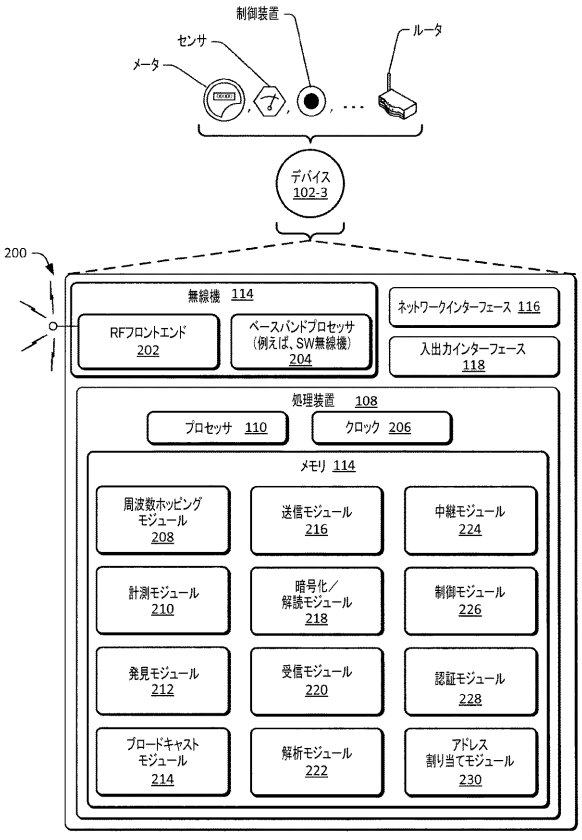
（結論）

本発明は、構造上の特徴、および／または方法上の動作に特有の言い回しで説明されてきたものの、本発明は、説明される特定の特徴または動作に必ずしも限定されないことを理解されたい。むしろ、特定の特徴および動作は、本発明を実施する例示的な形態として開示される。

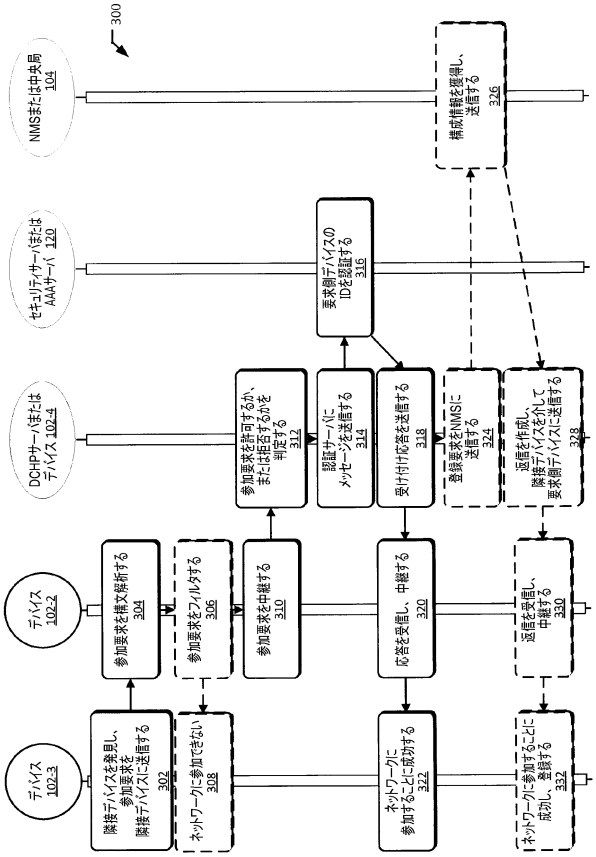
【図１】



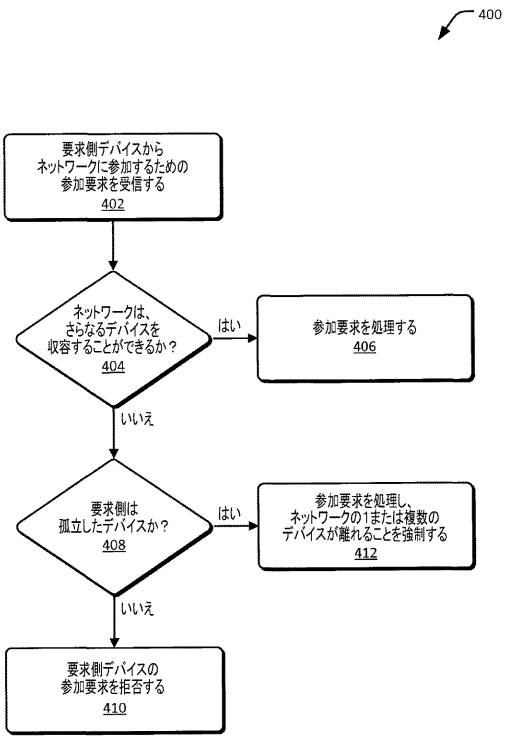
【図２】



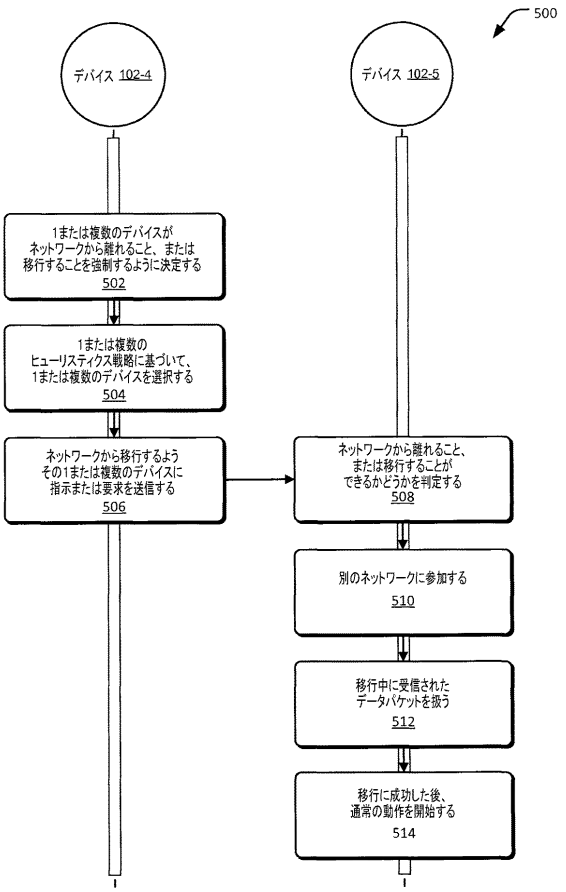
【図３】


300
NMSまたは中央局 104
セキュリティサーバまたは AAAサーバ 120
DCHPサーバまたは デバイス 102-4
デバイス 102-2
デバイス 102-3
構成情報を獲得し、送信する 326
要求側デバイスのIDを登録する 316
参加要求を許可するか、または拒否するかを判定する 312
認証サーバにメッセージを送信する 314
受け付け応答を送信する 318
登録要求をNMSに送信する 324
返信を作成し、隣接デバイスを介して要求側デバイスに送信する 328
参加要求を構文解析する 304
参加要求をフィルタする 306
参加要求を中継する 310
応答を受信し、中継する 320
返信を受信し、中継する 330
隣接デバイスを発見し、参加要求を隣接デバイスに送信する 302
ネットワークに参加できない 308
ネットワークに参加することに成功する 322
ネットワークに参加することに成功し、登録する 332

【図４】


400
要求側デバイスからネットワークに参加するための参加要求を受信する 402
ネットワークは、さらなるデバイスを収容することができるか？ 404
はい
参加要求を処理する 406
いいえ
要求側は孤立したデバイスか？ 408
はい
参加要求を処理し、ネットワークの1または複数のデバイスが離れることを強制する 412
いいえ
要求側デバイスの参加要求を拒否する 410

【図５】


500
デバイス 102-4
デバイス 102-5
1または複数のデバイスがネットワークから離れること、または移行することを強制するように決定する 502
1または複数のヒューリスティクス戦略に基づいて、1または複数のデバイスを選択する 504
ネットワークから移行するようその1または複数のデバイスに指示または要求を送信する 506
ネットワークから離れること、または移行することができるかどうかを判定する 508
別のネットワークに参加する 510
移行中に受信されたデータパケットを扱う 512
移行に成功した後、通常の動作を開始する 514

フロントページの続き

(72)発明者　マハディ　マニ
アメリカ合衆国　９９０１９　ワシントン州　リバティー　レイク　ノース　モルター　ロード　２１１１　アイトロン　インコーポレイテッド内
(72)発明者　マイケル　ティー. ガリソン　ステューバー
アメリカ合衆国　９９０１９　ワシントン州　リバティー　レイク　ノース　モルター　ロード　２１１１　アイトロン　インコーポレイテッド内

審査官　松野　吉宏

(56)参考文献　特開２００６－２０３４８０（ＪＰ，Ａ）
特開２００５－３１１５２７（ＪＰ，Ａ）
米国特許出願公開第２００５／０１８８０６９（ＵＳ，Ａ１）
米国特許出願公開第２００３／０１７９７４２（ＵＳ，Ａ１）
特開２０１０－１１８７５２（ＪＰ，Ａ）
特表２００７－５２０１３１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｂ　７／２４　－　７／２６
Ｈ０４Ｗ　４／００　－　９９／００
Ｈ０４Ｌ　９／３２
３ＧＰＰ　ＴＳＧ　ＲＡＮ　ＷＧ１－４
ＳＡ　ＷＧ１－４
ＣＴ　ＷＧ１、４