(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6687636号
(P6687636)
(45)発行日　令和2年4月22日(2020.4.22)　(24)登録日　令和2年4月6日(2020.4.6)

(51)Int.Cl.　F I
H04L 12/911 (2013.01)　H04L 12/911
H04W 88/16 (2009.01)　H04W 88/16
H04L 12/66 (2006.01)　H04L 12/66　E

請求項の数 15　(全 56 頁)

(21)出願番号　特願2017-544289 (P2017-544289)
(86)(22)出願日　平成28年1月14日 (2016.1.14)
(65)公表番号　特表2018-508146 (P2018-508146A)
(43)公表日　平成30年3月22日 (2018.3.22)
(86)国際出願番号　PCT/US2016/013463
(87)国際公開番号　WO2016/137598
(87)国際公開日　平成28年9月1日 (2016.9.1)
審査請求日　平成30年12月21日 (2018.12.21)
(31)優先権主張番号　62/120,159
(32)優先日　平成27年2月24日 (2015.2.24)
(33)優先権主張国・地域又は機関
米国 (US)
(31)優先権主張番号　62/161,768
(32)優先日　平成27年5月14日 (2015.5.14)
(33)優先権主張国・地域又は機関
米国 (US)

(73)特許権者　507364838
クアルコム，インコーポレイテッド
アメリカ合衆国　カリフォルニア　９２１２１　サン　ディエゴ　モアハウス　ドライブ　５７７５
(74)代理人　100108453
弁理士　村山　靖彦
(74)代理人　100163522
弁理士　黒田　晋平
(72)発明者　ス・ボム・イ
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５

最終頁に続く

(54)【発明の名称】サービス－ユーザプレーン手法のためのネットワークトークンを使用した効率的なポリシー施行

(57)【特許請求の範囲】
【請求項１】
デバイスにおいて動作可能である方法であって、
前記デバイスによって、1つまたは複数のアプリケーションサービスに関連付けられたアプリケーションサーバとの接続を開始するステップと、
前記接続の開始に応答して、ネットワークトークンを取得するステップであって、前記ネットワークトークンが、
1つまたは複数のフローのセットのうちの第1のフローに関連付けられ、
前記1つまたは複数のアプリケーションサービスのうちの第1のアプリケーションサービスに関連付けられ、
1つまたは複数のユーザプレーンメッセージを介して前記デバイスにプロビジョニングされ、
宛先アドレスを含む入力パラメータのセットを有する関数を使用してコアネットワークのゲートウェイデバイスによって導出される、ステップと、
ユーザプレーン内で前記デバイスから前記アプリケーションサーバに1つまたは複数のアップリンク(UL)パケットとともに前記ネットワークトークンを送るステップとを含む、
方法。
【請求項２】
前記ネットワークトークンが、前記アプリケーションサーバおよび/または前記ゲートウェイデバイスのうちの1つから取得され、

前記ネットワークトークンが、前記デバイスのデバイス加入プロファイルおよび／または前記第1のアプリケーションサービスのポリシーに基づき、および／または、
前記ネットワークトークンが、前記デバイスに対してコアネットワークによって施行されたポリシーを反映する、
請求項1に記載の方法。
【請求項３】
前記接続の開始が、接続要求を送るステップを含み、前記接続要求が、前記ネットワークトークンの明示的要求を含む、または、
前記接続の開始が、前記ネットワークトークンの暗黙的要求を表すパケットを送るステップを含む、
請求項1に記載の方法。
【請求項４】
ワイヤレスネットワーク上で通信する手段と、
ユーザプレーンメッセージを使用して1つまたは複数のアプリケーションサービスに関連付けられたアプリケーションサーバとの接続を開始する手段と、
前記接続の開始に応答して、前記アプリケーションサーバからネットワークトークンを取得する手段であって、前記ネットワークトークンが、
1つまたは複数のフローのセットのうちの第1のフローに関連付けられ、
前記1つまたは複数のアプリケーションサービスのうちの第1のアプリケーションサービスに関連付けられ、
1つまたは複数のユーザプレーンメッセージを介してデバイスにプロビジョニングされ、
宛先アドレスを含む入力パラメータのセットを有する関数を使用してコアネットワークのゲートウェイデバイスによって導出される、取得する手段と、
ユーザプレーン内で前記デバイスから前記アプリケーションサーバに1つまたは複数のアップリンク(UL)パケットとともに前記ネットワークトークンを送る手段とを備える、
デバイス。
【請求項５】
ネットワーク内のゲートウェイデバイスにおいて動作可能である方法であって、
前記ゲートウェイデバイスにおいて、ユーザプレーン上で、第1のデータパケットを受信するステップと、
前記第1のデータパケットを評価することによって、第1のネットワークトークンが要求されるかどうかを決定するステップと、
前記第1のネットワークトークンが要求される場合、前記ゲートウェイデバイスにおいて前記第1のネットワークトークンを導出するステップであって、前記第1のネットワークトークンが、宛先アドレスを含む入力パラメータのセットを有する関数を使用してコアネットワークの前記ゲートウェイデバイスによって導出され、前記第1のネットワークトークンが、前記ネットワークによって維持されるデバイス加入プロファイルに基づく、ステップと、
前記第1のネットワークトークンが要求される場合、前記第1のデータパケットとともに前記第1のネットワークトークンを含めるステップと、
前記第1のデータパケットおよび前記第1のネットワークトークンを宛先に送るステップとを含む、
方法。
【請求項６】
前記第1のデータパケットがアプリケーションサーバに送られることになっており、かつ前記第1のネットワークトークンがアップリンクネットワークトークンである、
前記第1のデータパケットがアプリケーションサーバに送られることになっており、かつ前記第1のネットワークトークンがダウンリンクネットワークトークンである、
前記第1のデータパケットがデバイスに送られることになっており、かつ前記第1のネッ

トワークトークンがダウンリンクネットワークトークンである、または、
前記第1のネットワークトークンがアップリンクネットワークトークンおよびダウンリンクネットワークトークンであり、前記アップリンクネットワークトークンが前記ダウンリンクネットワークトークンとは異なる、
請求項5に記載の方法。
【請求項７】
前記第1のデータパケットが、前記第1のネットワークトークンの明示的要求を含む、または、
前記第1のデータパケットが、前記第1のネットワークトークンの暗黙的要求を表す、
請求項5に記載の方法。
【請求項８】
前記ゲートウェイデバイスにおいて、前記ゲートウェイデバイスからデータパケットを受信するステップであって、前記データパケットが、アプリケーションサーバに対応する宛先アドレスプレフィックスを少なくとも含み、前記データパケットが第2のネットワークトークンを含む、ステップと、
前記第2のネットワークトークンを検証するステップと、
前記検証が成功でない場合、前記データパケットを破棄するステップと、
前記検証が成功である場合、前記データパケットを前記アプリケーションサーバに送るステップとをさらに含む、
請求項5に記載の方法。
【請求項９】
前記第2のネットワークトークンの検証が、
前記データパケットから取得された入力パラメータおよび前記ゲートウェイデバイスに知られている鍵を使用して、第1の関数から前記第1のネットワークトークンの複製を導出するステップと、
前記第1のネットワークトークンの前記複製を前記第2のネットワークトークンと比較するステップであって、前記第1のネットワークトークンの前記複製が前記第2のネットワークトークンに等しい場合、検証が成功である、ステップとを含む、
請求項8に記載の方法。
【請求項１０】
ワイヤレスネットワーク上で通信する手段と、
ゲートウェイデバイスにおいて、ユーザプレーン上で、アプリケーションサーバに送られることになるパケットを受信する手段と、
前記パケットを評価することによって、第1のネットワークトークンが要求されているかどうかを決定する手段と、
前記第1のネットワークトークンが要求される場合、前記第1のネットワークトークンを導出する手段であって、前記第1のネットワークトークンが、宛先アドレスを含む入力パラメータのセットを有する関数を使用してコアネットワークの前記ゲートウェイデバイスによって導出され、前記第1のネットワークトークンがデバイス加入プロファイルに基づく、手段と、
前記第1のネットワークトークンが要求される場合、前記パケットとともに前記第1のネットワークトークンを含める手段と、
前記パケットおよび前記第1のネットワークトークンを前記アプリケーションサーバに送る手段とを備える、
ゲートウェイデバイス。
【請求項１１】
前記ゲートウェイデバイスからデータパケットを受信する手段であって、前記データパケットが、前記アプリケーションサーバに対応する宛先アドレスプレフィックスを少なくとも含み、前記データパケットが第2のネットワークトークンを含む、手段と、
前記第2のネットワークトークンを検証する手段と、

前記検証が成功でない場合、前記データパケットを破棄する手段と、
前記検証が成功である場合、前記データパケットを前記アプリケーションサーバに送る手段とをさらに備える、
請求項10に記載のゲートウェイデバイス。
【請求項１２】
アプリケーションサーバにおいて動作可能である方法であって、
1つまたは複数のアプリケーションサービスに関連付けられた前記アプリケーションサーバによって、デバイスを用いて第1のアプリケーションサービスを開始する要求を送るステップと、
前記第1のアプリケーションサービスを開始する前記要求の送出に応答して、ネットワークトークンを取得するステップであって、前記ネットワークトークンが、
1つまたは複数のフローのセットのうちの第1のフローに関連付けられ、
前記第1のアプリケーションサービスに関連付けられ、
1つまたは複数のユーザプレーンメッセージを介して前記アプリケーションサーバに送られ、
宛先アドレスを含む入力パラメータのセットを有する関数を使用してコアネットワークのゲートウェイデバイスによって導出される、ステップと、
ユーザプレーン内で前記アプリケーションサーバから前記デバイスに送られる1つまたは複数のダウンリンク(DL)パケットとともに前記ネットワークトークンを送るステップとを含む、
方法。
【請求項１３】
前記ネットワークトークンが、前記デバイスのデバイス加入プロファイルおよび/または
前記第1のアプリケーションサービスのポリシーに基づき、前記ネットワークトークンが、前記デバイスに対して前記コアネットワークによって施行されたポリシーを反映する、
請求項12に記載の方法。
【請求項１４】
デバイスを用いてアプリケーションサービスを開始する要求を送る手段と、
前記デバイスを用いて前記アプリケーションサービスを開始する前記要求の送出に応答して、ネットワークトークンを取得する手段であって、前記ネットワークトークンが、
1つまたは複数のフローのセットのうちの第1のフローに関連付けられ、
前記1つまたは複数のアプリケーションサービスのうちの第1のアプリケーションサービスに関連付けられ、
宛先アドレスを含む入力パラメータのセットを有する関数を使用してコアネットワークのゲートウェイデバイスによって導出され、
1つまたは複数のユーザプレーンメッセージを介してアプリケーションサーバに送られる、取得する手段とを備える、
アプリケーションサーバ。
【請求項１５】
コンピュータによって実行されたとき、請求項1から3、5から9、12から13のいずれか一項に記載の方法を前記コンピュータに動作させる命令を含む、
コンピュータプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本出願は、2015年2月24日に米国特許商標庁に出願された仮出願第62/120,159号、2015年5月14日に米国特許商標庁に出願された仮出願第62/161,768号、および2015年9月25日に米国特許商標庁に出願された非仮出願第14/866,425号の優先権および利益を主張するもの

であり、これらの出願の内容全体は、参照により本明細書に組み込まれる。

【０００２】

一態様は、一般にネットワークトークンに関し、より詳細には、ネットワークポリシー(たとえば、許可されたアプリケーションサービスのみにデバイスがアクセスしていることを検証すること)および/またはパケットステアリングの施行を容易にするためにアップリンクユーザプレーンデータフローおよびダウンリンクユーザプレーンデータフローに関連付けられたアップリンクネットワークトークンおよびダウンリンクネットワークトークンの導出、プロビジョニング、および使用に関する。

【背景技術】

【０００３】

いくつかのクライアントデバイスが、ネットワークアクセスを有することがあるが、それらのネットワークアクセスは、アプリケーションサービスのセットに限定されることがある。ネットワーク事業者が、ポリシーを使用してそのような制限を課すことがある。一例では、特定のアプリケーションサービスプロバイダが、クライアントデバイスのネットワークアクセスを保証し得る。クライアントデバイスは、そのサーバ上でアプリケーションサービスプロバイダによって実行されるアプリケーションサービスに限定されてよい。別の例では、ネットワークアクセスを有するクライアントデバイスは、所与のアプリケーションサービスに関連付けられたデータの特殊なチャージング(charging)または取り扱い(たとえば、ビットレートまたはサービス品質)を可能にする契約の一部であってよい。たとえば、クライアントデバイスは、セルラープロバイダを通してのセルラー加入を有することがあり、そのセルラープロバイダは、クライアントデバイスに1つまたは複数の制限を課すことを希望することがある。一例では、現在ソーシャルメディアのプロバイダとして知られているが、セルラープロバイダとして知られていない企業が、将来セルラープロバイダとしての役割を果たし得る。この例では、クライアントデバイスは、その企業への加入を有し得る。その加入合意の一部として、クライアントデバイスは、インターネットにアクセスし得るが、他のソーシャルメディアサイトの除外のためにその企業のソーシャルメディアサイトを使用するように制限され得る。別の例として、クライアントデバイスが、ストリーミングメディアサービスのプロバイダへの加入を有することがある。この例では、合意の一部として、クライアントデバイスは、様々なセルラープロバイダ(たとえば、モバイルネットワーク事業者)を通してインターネットにアクセスし得る。しかしながら、アクセスが、すべてのストリーミングメディアサービスにメディアサービスのプロバイダのサイトを使用するように(ストリーミングメディアサービスのプロバイダと様々なセルラープロバイダおよび/またはクライアントデバイスのユーザとの間での)合意によって制限され得る。別の例として、特定のアクセスポイント名(APN)に対して、特定のトラフィック(たとえば、制御プレーンシグナリングおよび/またはユーザプレーンメッセージ)のみが、ポリシーまたは加入制限に基づいてクライアントデバイスから送られることが許可され得る。

【０００４】

ネットワークポリシーは、クライアントデバイスが、いかなる合意も侵害していない、合意されたアプリケーションサービスへのアクセスが提供されている、および/または合意されたサービスのレベルが提供されていることを保証するために、アプリケーションサービスに関して設けられてよい。ネットワークは、クライアントデバイスからたとえばパケットデータネットワーク(たとえば、インターネット)上のアプリケーションサーバに向かって送られるアップリンク(UL)パケットに対して、そのようなポリシーを施行し得る。ネットワークは、さらに、アプリケーションサーバからクライアントデバイスに向かって送られるダウンリンク(DL)パケットに対してそのようなポリシーを施行し得る。

【０００５】

今日、アプリケーションサービスのためのポリシー施行は、ネットワークへのゲートウェイにおいて行われる。そのようなゲートウェイの一例は、コアネットワーク(たとえば、発展型パケットコア(EPC))とインターネットなどのパケットデータネットワーク(PDN)

との間のゲートウェイとして働くパケットデータネットワークゲートウェイ(P-GW)である。1つの問題が、ポリシー施行(たとえば、サービスアクセスポリシーの施行)が、P-GWに、クライアントデバイスとアプリケーションサーバとの間で送られるすべてのULパケットおよびDLパケットのバリデーションを行うことを要求し得ることに存在する。その上、各ULパケットおよびDLパケットは、その宛先アドレスに特定のベアラまたはデータフローを介してステアリングされる必要があり得る。宛先アドレスは、2つの部分、すなわち接頭部および接尾部からなり得る。

【０００６】

ネットワークポリシーは、P-GWにおけるULパケットおよびDLパケットのバリデーションによって施行され得る。施行は、クライアントデバイスが、許可されたアプリケーションサービスへ/からパケットを送って/受信しているにすぎないことを保証し得る。バリデーションとしては、P-GWを通過するパケットの宛先アドレスまたは宛先アドレスおよびポート番号を検証することがあり得る。バリデーションとしては、さらに、各パケットのソースアドレスを検証することがあり得る。各パケットのソースアドレスを検証することが、(たとえば、無許可クライアントデバイスからのパケットが、許可されたクライアントデバイスから来たように見えることによってネットワークをだますことを防ぐことによって)なりすまし防止のために有用であり得る。パケットステアリングは、合意されたサービス品質(QoS)が達成されることを保証するために必要とされ得る。

【０００７】

現在の慣行は、大幅なオーバーヘッドを招き、処理遅延により転送待ち時間を増す。現在の慣行は、一般的には、パケットインスペクション(たとえば、ディープパケットインスペクション、シャローパケットインスペクション)およびトラフィックフローテンプレート(TFT)およびサービスデータフロー(SDF)テンプレートを使用することを実現する。P-GWは、パケットが、各パケットのヘッダを検査することによって、サービスのために定義されたTFT/SDFテンプレートに適合することを確かめる。

【０００８】

図1は、サービスデータフロー104のダウンリンク部を検出し、その部分を図示のベアラ106インターネットプロトコルコネクティビティアクセスネットワーク(IP-CAN)などのベアラにマッピングする際のSDFテンプレート102の役割の従来技術の図である。図1は、3GPP技術仕様書(TS)23.203、図6.4に基づく。

【０００９】

SDFテンプレート102は、ダウンリンクパケットのバリデーションおよびマッピングのために作製される。しかしながら、パケットフィルタのセット(たとえば、SDFテンプレート102内のパケットフィルタa～fを参照されたい)の使用は、テーブルおよびテーブルルックアップ手順の使用を必要とする。そのようなテーブルおよび手順の使用は、手順を実行するためにメモリ記憶空間およびプロセッサリソースを必要とするので、効率に影響する。さらに、各パケットは、所与のパケットが、フィルタの必要条件のすべてを満たすフィルタに適用される前に、複数のフィルタを通ってフィルタリングされなければならないので、時間リソースが浪費される。

【００１０】

したがって、(アップリンクパケットおよびダウンリンクパケットのいずれかまたは両方に)P-GWにおいてパケットインスペクションおよびTFT/SDFテンプレートを使用することは、たとえば、それらの使用が大幅なオーバーヘッド(たとえば、メモリルックアップおよびパターンマッチングのための処理およびメモリリソース)を招き、処理遅延により転送待ち時間を増すので、問題がある。さらに、パケットは、TFT/SDFテンプレートによって実現される追加フィルタリングルールに対してテストされる必要があるので、追加のポリシー制御は、追加のオーバーヘッドおよび処理遅延を招くので、きめの細かい(たとえば、サービスごとの)ポリシー制御は難しい。その上、TFT/SDFテンプレートの使用は、スポンサー付き(sponsored)コネクティビティに対してスケーラブルではない。様々なサービスのスポンサーの数の増加(おそらく、今後数年間において数千のサービス)は、対応し

て増加された数のTFT/SDFテンプレートを通ってパケットをフィルタリングするために必要とされる時間の増加を意味するであろう。これは、やはり、追加のオーバーヘッドおよび処理遅延を招くであろう。

【先行技術文献】

【非特許文献】

【００１１】

【非特許文献１】3GPP技術仕様書(TS)23.203、図6.4

【発明の概要】

【発明が解決しようとする課題】

【００１２】

必要とされるものは、パケットインスペクションを捕捉および/または強化し、アップリンクネットワークポリシーおよびダウンリンクネットワークポリシーの施行における効率を改善するための代替物である。

【課題を解決するための手段】

【００１３】

第1の態様によれば、方法は、デバイスにおいて動作可能であってよい。この方法は、デバイスによって、1つまたは複数のアプリケーションサービスに関連付けられたアプリケーションサーバとの接続を開始することを含んでよい。接続の開始に応答して、デバイスは、ネットワークトークンを取得してよい。ネットワークトークンは、1つまたは複数のフローのセットのうちの第1のフローに関連付けられ、1つまたは複数のアプリケーションサービスのうちの第1のアプリケーションサービスに関連付けられ、1つまたは複数のユーザプレーンメッセージを介してデバイスにプロビジョニングされてよい。方法は、ユーザプレーン内でデバイスからアプリケーションサーバに1つまたは複数のアップリンク(UL)パケットとともにネットワークトークンを送ることも含んでよい。

【００１４】

追加の態様によれば、ネットワークトークンが、アプリケーションサーバおよび/またはゲートウェイデバイスのうちの1つから取得されてよい。ネットワークトークンは、コアネットワークのゲートウェイデバイスによって導出されてよい。ネットワークトークンは、デバイスのデバイス加入プロファイルおよび/または第1のアプリケーションサービスのポリシーに基づいてよい。ネットワークトークンは、デバイスに対してコアネットワークによって施行されたポリシーを反映してよい。接続を開始する態様は、接続要求を送ることを含んでよく、接続要求は、ネットワークトークンの明示的要求を含む。接続を開始する態様は、ネットワークトークンの暗黙的要求を表すパケットを送ることを含んでよい。

【００１５】

いくつかの態様によれば、暗黙的要求は、アプリケーションサーバに第1のパケットを送ることによって表されてよい。接続の開始は、アプリケーションサーバからの肯定応答を必要とするパケットを送ることを含んでよく、この肯定応答はデバイスにネットワークトークンを搬送する。ネットワークトークンは、ユーザプレーンシムヘッダ内でデバイスからパケットデータネットワーク(PDN)ゲートウェイ(P-GW)に搬送されてよい。ユーザプレーンシムヘッダは、インターネットプロトコル(IP)層の上に配置されてよい。ネットワークトークンは、IPバージョン6(IPv6)において定義されるインターネットプロトコル(IP)拡張ヘッダ内でデバイスからパケットデータネットワーク(PDN)ゲートウェイ(P-GW)に搬送されてよい。ネットワークトークンは、パケットデータコンバージェンスプロトコル(PDCP)層においてデバイスからアクセスノードに搬送され、アクセスノード内でユーザプレーン(GTP-U)層のために汎用パケット無線サービス(GPRS)トンネリングプロトコル(GTP)層にコピーされ、GTP-U層においてアクセスノードからパケットデータネットワーク(PDN)ゲートウェイ(P-GW)に搬送されてよい。

【００１６】

一態様によれば、ワイヤレスネットワーク上で通信するように構成されたネットワーク

通信インターフェースと、このネットワーク通信インターフェースに結合された処理回路とを含むデバイスは、上記で説明された方法を実行してよい。

【００１７】

別の態様によれば、方法は、ネットワーク内のゲートウェイデバイスにおいて動作可能であってよい。方法は、ゲートウェイデバイスにおいて、ユーザプレーン上で、第1のデータパケットを受信することを含んでよい。方法は、第1のデータパケットを評価することによって、ネットワークトークンが要求されるかどうかを決定することと、ネットワークトークンが要求される場合、ネットワークトークンを取得することとをさらに含んでよい。ネットワークトークンは、ネットワークによって維持されるデバイス加入プロファイルに基づいてよい。方法は、ネットワークトークンが要求される場合、第1のデータパケットとともに前記ネットワークトークンを含めることと、第1のデータパケットおよびネットワークトークンを宛先に送ることとをさらに伴ってよい。

【００１８】

追加の態様によれば、第1のデータパケットはアプリケーションサーバに送られてよく、ネットワークトークンはアップリンクネットワークトークンである。第1のデータパケットはアプリケーションサーバに送られてよく、ネットワークトークンはダウンリンクネットワークトークンである。第1のデータパケットはデバイスに送られてよく、ネットワークトークンはダウンリンクネットワークトークンである。第1のデータパケットがデバイスに送られ、ネットワークトークンがダウンリンクネットワークトークンである場合、方法は、ゲートウェイデバイスにおいて、デバイスからダウンリンクネットワークトークンを含む第2のデータパケットを受信することと、第2のデータパケットおよびダウンリンクネットワークトークンをアプリケーションサーバに送ることとをさらに含んでよい。いくつかの態様によれば、ネットワークトークンはアップリンクネットワークトークンおよびダウンリンクネットワークトークンであり、アップリンクネットワークトークンはダウンリンクネットワークトークンとは異なる。ゲートウェイデバイスは、パケットデータネットワーク(PDN)ゲートウェイ(P-GW)であってよい。第1のパケットは、ネットワークトークンの明示的要求を含んでもよいし、ネットワークトークンの暗黙的要求を表してもよい。いくつかの態様によれば、ネットワークトークンが要求されているかどうかの決定は、第1のパケットが送られることになっているまたは第1のパケットが受信されるアプリケーションサーバがネットワークトークンを必要とするかどうかを決定することに基づいてよい。

【００１９】

ネットワークトークンの取得は、ゲートウェイデバイスにおいてネットワークトークンを導出することによって達成されてよい。ネットワークトークンは、ゲートウェイデバイスに知られている秘密鍵、クラスインデックス、発信元インターネットプロトコル(IP)アドレス、発信元ポート番号、宛先IPアドレス、宛先ポート番号、プロトコル識別子(ID)、アプリケーションID、優先順位、および/またはサービス品質クラス識別子(QCI)を含む入力パラメータのセットを有する関数を使用して導出されてよい。クラスインデックスは、ネットワークトークン導出のために使用されるフィールドを定義してよい。ネットワークトークンは、クラスインデックスおよび関数の出力の連結であってよい。

【００２０】

一態様によれば、ワイヤレスネットワーク上で通信するように構成されたネットワーク通信インターフェースと、このネットワーク通信インターフェースに結合された処理回路とを含むゲートウェイデバイスは、上記で説明された方法を実行してよい。

【００２１】

別の態様によれば、ゲートウェイデバイスにおいて動作可能である方法は、ゲートウェイデバイスにおいて、デバイスから1つまたは複数のアプリケーションサービスに関連付けられたアプリケーションサーバに送られる前記第1のネットワークトークンの要求に応答して、第1のネットワークトークンを導出することを含んでよい。この方法は、ゲートウェイデバイスにおいて、デバイスからデータパケットを受信することであって、このデ

ータパケットは、アプリケーションサーバに対応する宛先アドレスプレフィックスを少なくとも含み、このデータパケットは第2のネットワークトークンを含む、受信することを含んでよい。この方法は、第2のネットワークトークンを検証することと、検証が成功でない場合、データパケットを破棄することと、検証が成功である場合、データパケットをアプリケーションサーバに送ることとをさらに含んでよい。データパケットは、ユーザプレーンメッセージ内で受信されてよい。ゲートウェイデバイスは、パケットデータネットワーク(PDN)ゲートウェイ(P-GW)であってよい。第2のネットワークトークンを検証することは、データパケットから取得された入力パラメータおよびゲートウェイデバイスに知られている鍵を使用して、第1の関数から第1のネットワークトークンの複製を導出することを含んでよい。第2のネットワークトークンを検証することは、第1のネットワークトークンの複製を第2のネットワークトークンと比較することであって、第1のネットワークトークンの複製が第2のネットワークトークンに等しい場合、検証が成功である、比較することをさらに含んでよい。

【００２２】

いくつかの態様によれば、第2のネットワークトークンが、ヘッダIPとは別個のシムヘッダ内でデバイスからゲートウェイデバイスに搬送されてよい。第2のネットワークトークンは、インターネットプロトコル(IP)バージョン6(IPv6)において定義されたIP拡張ヘッダ内でデバイスからゲートウェイデバイスに搬送されてよい。いくつかの態様によれば、第2のネットワークトークンは、パケットデータコンバージェンスプロトコル(PDCP)層においてデバイスからアクセスノードに搬送され、アクセスノード内でユーザプレーン(GTP-U)層のために汎用パケット無線サービス(GPRS)トンネリングプロトコル(GTP)層にコピーされ、GTP-U層においてアクセスノードからゲートウェイデバイスに搬送されてよい。

【００２３】

一態様によれば、ワイヤレスネットワーク上で通信するように構成されたネットワーク通信インターフェースと、このネットワーク通信インターフェースに結合された処理回路とを含むゲートウェイデバイスは、上記で説明された方法を実行してよい。

【００２４】

別の態様によれば、アプリケーションサーバにおいて動作可能である方法は、1つまたは複数のアプリケーションサービスに関連付けられたアプリケーションサーバによって、デバイスを用いて第1のアプリケーションサービスを開始する要求を送ることを含んでよい。この方法は、第1のアプリケーションサービスを開始する要求の送出に応答して、ネットワークトークンを取得することをさらに含んでよい。ネットワークトークンは、1つまたは複数のフローのセットのうちの第1のフローに関連付けられ、第1のアプリケーションサービスに関連付けられ、1つまたは複数のユーザプレーンメッセージを介してデバイスに送られてよい。方法は、ユーザプレーン内でアプリケーションサーバからデバイスに送られる1つまたは複数のダウンリンク(DL)パケットとともにネットワークトークンを送ることをさらに含んでよい。ネットワークトークンは、コアネットワークのゲートウェイデバイスによって導出されてよい。ネットワークトークンは、デバイスのデバイス加入プロファイルおよび/または第1のアプリケーションサービスのポリシーに基づいてよい。ネットワークトークンは、デバイスに対してコアネットワークによって施行されたポリシーを反映してよい。第1のアプリケーションサービスを開始する要求は、ネットワークトークンの明示的要求を含んでもよいし、ネットワークトークンの暗黙的要求を表すパケットを送ることを含んでもよい。

【００２５】

一態様によれば、ワイヤレスネットワーク上で通信するように構成されたネットワーク通信インターフェースと、このネットワーク通信インターフェースに結合された処理回路とを含むアプリケーションサーバは、上記で説明された方法を実行してよい。

【図面の簡単な説明】

【００２６】

【図１】サービスデータフローのダウンリンク部を検出し、その部分を図示のインターネ

ットプロトコルコネクティビティアクセスネットワーク(IP-CAN)ベアラなどのベアラにマッピングする際のSDFテンプレートの役割の従来技術を示す図である。
【図２】例示的な動作環境を示す図である。
【図３】本明細書において説明される態様による例示的なアップリンク動作を示す図である。
【図４】本明細書において説明される態様による例示的なダウンリンク動作を示す図である。
【図５】本明細書において説明される態様による1つまたは複数のユーザプレーンメッセージに関連するネットワークトークン導出、プロビジョニング、および使用を示す例示的なコールフローである。
【図６】本明細書において説明される態様による1つまたは複数のユーザプレーンメッセージに関連するネットワークトークン導出、プロビジョニング、および使用を示す例示的なコールフローである。
【図７】本明細書において説明される態様による1つまたは複数のユーザプレーンメッセージに関連するネットワークトークン導出、プロビジョニング、および使用を示す例示的なコールフローである。
【図８】本明細書において説明される態様による1つまたは複数のユーザプレーンメッセージに関連する2つのネットワークトークン(たとえば、アップリンクネットワークトークンおよびダウンリンクネットワークトークン)の導出、プロビジョニング、および使用を示す例示的なコールフローである。
【図９】本明細書において説明される一態様によるシステムのユーザプレーンプロトコルスタックの例示的な図である。
【図１０】本明細書において説明される別の態様によるシステムのユーザプレーンプロトコルスタックの例示的な図である。
【図１１】本明細書において説明される別の態様によるシステムのユーザプレーンプロトコルスタックの例示的な図である。
【図１２】本明細書において説明される別の態様によるシステムのユーザプレーンプロトコルスタックの例示的な図である。
【図１３】本明細書において説明される態様によるネットワークトークンを使用するネットワークポリシー施行および/またはパケットステアリングをサポートするように構成された例示的なデバイスを示すブロック図である。
【図１４】デバイス(たとえば、チップコンポーネント、クライアントデバイス)が、アプリケーションサーバと通信し、通信に関連してネットワークトークンを利用する要求を開始し得る例示的な方法を示す図である。
【図１５】デバイス(たとえば、チップコンポーネント、クライアントデバイス)が、通信を開始し、通信に関連してネットワークトークンを利用する要求に応答し得る例示的な方法を示す図である。
【図１６】本明細書において説明される態様によるネットワークトークンを使用するネットワークポリシー施行および/またはパケットステアリングをサポートするように構成された例示的なゲートウェイデバイスを示すブロック図である。
【図１７】本明細書において説明される態様による、ネットワークトークンの使用のためにユーザプレーンメッセージングを介してデバイスからの要求を検出し、ネットワークトークンを導出して、アプリケーションサーバを介して要求側デバイスにネットワークトークンを提供するためにゲートウェイデバイス(たとえば、P-GW)において動作可能である例示的な方法を示す図である。
【図１８】本明細書において説明される態様によるユーザプレーンメッセージングを介してゲートウェイデバイス(たとえば、P-GW)におけるネットワークトークンをセットアップおよび使用する、ゲートウェイデバイス(たとえば、P-GW)において動作可能である例示的な方法を示す図である。
【図１９】本明細書において説明される態様による、ネットワークポリシーの施行および

/またはパケットのステアリングのためのネットワークトークンの使用に関連する、ネットワークトークンを検証する(たとえば、ネットワークトークンの検証)ための、ゲートウェイデバイス(たとえば、P-GW)において動作可能である例示的な方法を示す図である。
【図２０】ダウンリンクトークンバリデーションおよびパケットマッピングをサポートするように構成された例示的なアプリケーションサーバを示すブロック図である。
【図２１】本明細書において説明される態様によるアプリケーションサーバにおいてネットワークトークンをセットアップする例示的な方法のフローチャートである。
【発明を実施するための形態】
【００２７】
以下の説明では、例示として、本開示が実施され得る特定の実施形態が示される添付の図面に対する参照が、なされる。実施形態は、当業者が本発明を実施することを可能にするために本開示の態様について十分詳細に説明することが意図されている。他の実施形態が利用されてよく、変更が、本開示の範囲から逸脱することなく、開示される実施形態に対してなされてよい。以下の詳細な説明は、限定的な意味に解釈されるべきではなく、本発明の範囲は、添付の特許請求の範囲のみによって定義される。
【００２８】
「デバイス」という用語は、本明細書において、チップコンポーネントおよび/または、様々なデバイスの中でもとりわけ、モバイルデバイス、モバイル電話、モバイル通信デバイス、モバイルコンピューティングデバイス、デジタルタブレット、スマートフォン、ユーザ機器、ユーザデバイス、端末などのクライアントデバイスを指すために使用され得る。本明細書で使用されるとき、「導出する」という用語は、デバイスからローカルに導出すること、または別のデバイスから取得することを意味し得る。
【００２９】
概要
本明細書において説明される態様は、一般に、アップリンクネットワークトークンおよびダウンリンクネットワークトークンの導出、プロビジョニング、および使用に関する。ネットワークトークンは、ユーザプレーン内でパケットとともに搬送され得る。アップリンクネットワークトークンまたはダウンリンクネットワークトークは、1つまたは複数のパケットに埋め込まれ、または、これとともに含まれ、ネットワークポリシー施行および/またはトラフィックステアリング(たとえば、1つまたは複数のユーザプレーンメッセージのステアリング)に使用されてよい。
【００３０】
ネットワークトークンの要求は、明示的であってもよいし、暗黙的であってもよい。明示的要求は、たとえば、デバイスからアプリケーションサーバへと、またはアプリケーションサーバからデバイスへと作成された接続要求に含まれてよい。アプリケーションサーバは、1つまたは複数のアプリケーションサービスに関連付けられてよい。要求は、明示的な場合、接続要求を含む1つまたは複数のパケットとともに搬送されてよい。デバイスからアプリケーションサーバへの、またはアプリケーションサーバからデバイスへのパケットは、その発信元からその宛先への途中でパケットデータネットワークゲートウェイ(P-GW)を通過する。P-GWにおいて、パケットは、ネットワークトークンの要求を明示的に含む(または暗黙的に表す)かどうかを決定するためにインスペクション/検査/分析されてよい。
【００３１】
たとえば、ネットワークトークンの要求が接続要求とともに含まれる場合、P-GWは、暗号関数、P-GWに知られている非共有秘密鍵、およびパケットから取得され得るパラメータ、およびサービスに関連付けられたパラメータを使用してネットワークトークンを導出してよい。しかしながら、P-GWは、導出したばかりのネットワークトークンを、ネットワークトークンを要求したエンティティに直接送らなくてよい。代わりに、P-GWは、接続要求(およびネットワークトークンの要求)を運んだパケットとともにネットワークトークンを埋め込み、または、これを含み、パケットを(導出したばかりのネットワークトークンと

ともに)、その宛先、たとえば、パケットヘッダ内の宛先アドレス(または少なくとも宛先アドレスプレフィックス)から識別された宛先に送ってもよい。処理回路は、宛先において、接続要求への応答(たとえば、接続応答)を準備し、その接続応答を含むパケット内に、またはこれとともにネットワークトークンを含める。パケットは、ユーザプレーンを介して、ネットワークトークンの要求の発信元および接続要求の開始者に送られてよい。その後、発信元が、宛先に送るべき追加パケットを有する場合、発信元は、追加パケットのうちの1つまたは複数内に(または、これとともに)ネットワークトークンのコピーを含め得る。

【００３２】

アップリンクネットワークトークンおよび/またはダウンリンクネットワークトークンは、ネットワークポリシーを施行するためにP-GWによって使用されてよい。本明細書において説明される態様によれば、以前に導出された元のネットワークトークンのコピーを含むパケットは、P-GWにおいて受信され得る。以前に導出された元のネットワークトークンのコピーは、アップリンクネットワークトークンであってもよいし、ダウンリンクネットワークトークンであってもよい。P-GWは、以前に導出された元のネットワークトークンのコピーを検証してよい。検証プロセスは、元のネットワークトークンの複製を導出することを含んでよい。複製ネットワークトークンは、元のネットワークトークンと同じ手段で、同じ暗号関数、P-GWに知られている同じ非共有秘密鍵、およびパケットから取得され得る同じ他のパラメータを使用して、導出されてよい。元のネットワークトークンのコピーに関連付けられた新たに受信されたパケットは、元のネットワークトークンに関連付けられたパケットと異なる。しかしながら、元のパケットから取得されるパケットと同じである新たに受信されたパケットから取得され得るパラメータがある。これらの共通パラメータは、複製ネットワークトークンを導出するために暗号関数において使用されてよい。複製ネットワークトークンが元のネットワークトークンのコピーに等しい場合、受信したばかりの元のネットワークトークンのコピーは、検証が成功したと考えられてよい。成功検証時、パケットは、その宛先に送られてよい。検証が成功でない場合、パケットは破棄されてよい。

【００３３】

例示的な動作環境

図2は、例示的な動作環境200を示す。そのような例示的な動作環境200において、1つまたは複数のクライアントデバイス202、204(たとえば、クライアントデバイスA、クライアントデバイスB)は、アクセスノード206(たとえば、ノードB、eNodeB、アクセスポイント(AP))とワイヤレスで通信し得る。アクセスノード206は、無線アクセスネットワーク(RAN)208(たとえば、evolved universal terrestrial radio access network(E-UTRAN))内に含まれてよい。当業者に知られているように、RAN208は一般に、複数のアクセスノード206を含む。図面は、混乱を抑えるために1つのアクセスノード206のみを示す。

【００３４】

セルラー通信システム(たとえば、4G、LTE、LTE-A)の非限定的な一例では、RAN208は、制御プレーンシグナリングおよびユーザプレーンメッセージをコアネットワーク(CN)210(たとえば、発展型パケットコア(EPC))に通信し得る。図2の図では、破線は制御信号経路を表し、実線はユーザデータメッセージ経路を表す。制御プレーンは、制御信号(たとえば、制御プレーンシグナリング)を伝達する。ユーザプレーンは、ユーザデータ(たとえば、ユーザプレーンメッセージ)を伝達する。本明細書において説明される態様の実装形態は、ユーザプレーンを利用し、制御プレーンシグナリングは必要とされない。制御プレーンシグナリングは必要とされないので、ネットワーク機能は、大部分は影響されない。クライアントデバイスおよびP-GWのユーザプレーンプロトコルスタックの修正形態は、本明細書において説明される態様のうちのいくつかに関連して実施され得る。たとえば、ネットワークトークンセットアップ手順は、プロトコルスタック修正形態を必要とすることがある。言い換えると、クライアントデバイスが、ネットワークトークンの要求の標識を有する接続要求を開始するとき、ゲートウェイデバイスは、ネットワークトークンを導出し

、接続要求を有するネットワークトークンを(たとえば、接続要求を有するパケット内に)埋め込むか、またはこれを含む。本明細書において説明される態様は、ネットワークトークン(たとえば、TCP、IP、Shimなど)を埋め込むためのいくつかの代替形態を提供し、ネットワークトークンの埋込みを実施するための、プロトコルスタックの対応する例示的な修正形態について説明する。

【００３５】

CN210は、モビリティ管理エンティティ(MME)212と、サービングゲートウェイ(S-GW)216と、ホーム加入者サーバ(HSS)218と、パケットデータネットワークゲートウェイ(P-GW)220とを含んでよい。P-GW220は、パケットデータネットワーク(PDN)222(たとえば、インターネット)と通信してよい。より具体的には、P-GW220は、PDN222内のサーバ224、226、228、230(たとえば、アプリケーションサーバ)と通信してよい。サーバ224、226、228、230は、たとえば、販売サービス、情報サービス、ストリーミングビデオサービス、およびソーシャルメディアサービスを提供するサービスプロバイダなどのサービスプロバイダに関連付けられてよい。

【００３６】

図3は、本明細書において説明される態様による例示的なアップリンク動作300を示す。例示的なアップリンク動作300は、便宜上、ロングタームエボリューション(LTE)システムの文脈で示されている。例は、本明細書において説明される任意の態様の範囲にいかなる制限も課すことを意図するものではない。

【００３７】

図3に表されているのは、デバイス302(たとえば、チップコンポーネント、クライアントデバイス、ユーザ機器、ユーザデバイス、端末、モバイルデバイス)、アクセスノード304(たとえば、eNodeB)、サービングゲートウェイ(S-GW)306、パケットゲートウェイ(P-GW)308、およびパケットデータネットワーク(PDN)310(たとえば、インターネット)である。

【００３８】

次に、図3の例示的なアップリンク動作300について説明する。(たとえば、デバイス302のアプリケーション/アプリケーションサービス312からの)IPフロー314は、トラフィックフローテンプレート(TFT)316とともに含まれるパケットフィルタ(図示せず)に適用される。示されるIPフロー314の数は例示的なものであり、限定することを意図したものではない。

【００３９】

TFT316のパケットフィルタは、IPフローをベアラ318(たとえば、発展型パケットシステム(EPS)ベアラ)へとフィルタリングする。3つのベアラ318(たとえば、ベアラ1、ベアラN-1、およびベアラN)は、例示のために示されている。一態様では、ベアラは、複数のアプリケーション/アプリケーションサービスによって共有されてよい。各ベアラは、パラメータの一意のセットに関連付けられてよい。

【００４０】

IPフロー314は、たとえば、デフォルトベアラにマッピングされてもよいし、1つまたは複数の専用ベアラにマッピングされてもよい。デフォルトベアラは一般に、非保証ビットレートを有してよく、専用ベアラは一般に、保証ビットレートまたは非保証ビットレートのいずれかを有してよい。ベアラ318は、アクセスノード304およびS-GW306を通過してよい。アクセスノード304およびS-GW306の態様は、本明細書において説明されず、当業者に知られている。

【００４１】

一態様では、ベアラ318からのIPフロー314は、判断および処理回路/関数/モジュール320に渡されてよい。判断および処理回路/関数/モジュール320は、ベアラ318から受信されたULパケットを、暗号バリデーションおよびトラフィックステアリング回路/関数/モジュール322に渡してもよいし、サービスデータフロー(SDF)テンプレート324およびその中に含まれるパケットフィルタ(図示せず)に渡してもよい。トラフィックステアリングは、信号関連パケットおよび/またはユーザデータメッセージ関連パケットのステアリング(たと

えば、方向付け、案内)を含む。

【００４２】

それとともに含まれるネットワークトークンを持つULパケットは、暗号バリデーションおよびトラフィックステアリング回路/関数/モジュール322に渡されてよい。ネットワークトークンに関連付けられた1つまたは複数のポリシーの施行は、ネットワークトークンのバリデーションに成功すると実行されてよい。

【００４３】

それとともに含まれるネットワークトークンを持たないULパケットは、判断および処理回路/関数/モジュール320によってSDFテンプレート324に渡されてよい。SDFテンプレート324のパケットフィルタの使用は、暗号バリデーションおよびトラフィックステアリング回路/関数/モジュール322の使用が必要とするよりも多くの処理リソースおよびメモリリソースを必要とすることがある。SDFテンプレート324のパケットフィルタを使用してフィルタリングを実行するために、たとえば、P-GW308は、SDFごとに別個のテーブルエントリテーブルを維持しなければならない。

【００４４】

したがって、ネットワークトークンの使用(および、結果として生じる暗号バリデーションおよびトラフィックステアリング回路/関数/モジュール322の使用)は、リソースを保存し、待ち時間を減少させる。一態様では、暗号ネットワークトークン(たとえば、ソフトウェアトークン)は、パケットインスペクションを補う/強化するために使用され得る。この態様の1つの利点としては、スケーラビリティがある。すなわち、テーブルエントリまたは状態が高速経路(別名、高速パス)上で保たれることは必要とされない。この態様の別の利点としては、短い待ち時間がある。すなわち、単一の暗号動作(たとえば、SHA-1、SHA-2、またはSHA-3(ここで、SHAはセキュアハッシュアルゴリズムの略である)、またはadvanced encryption standard(AES)などの暗号ハッシュ。より高速に実行され得る方、または適切に決定され得る方)が、アクセス制御に十分であってよい。その上、ネットワークトークン上で暗号動作を実行するために必要とされる時間は、P-GWによってサービス提供され得るアプリケーションサービスの数とは独立であるべきである。対照的に、SDFテンプレートのパケットフィルタが循環するために必要とされる時間は、P-GWによってサービス提供され得るアプリケーションサービスの数に依存する。アプリケーションサービスの数を増加させると、パケットフィルタの数が増加する。したがって、ポリシー施行および/またはユーザプレーンメッセージのステアリングの暗号ネットワークトークンの使用は有益である。

【００４５】

さらに別の利点としては、柔軟性があり得る。すなわち、暗号ネットワークトークンは、様々なメタデータに基づいて導出され得る。そのようなメタデータは、TFT/SDFテンプレート内でフィルタリングされているパラメータに限定されない。さらに、様々なポリシー(たとえば、信頼性ポリシーおよび/またはパケットポリシーの許可)が、ネットワークトークンに適用され得る。さらに別の利点としては、分散型サービス妨害(DDoS)攻撃への障害許容力(resilience)があり得る。すなわち、誤った/不適当な/信頼すべきでない(non-authentic)暗号ネットワークトークンを含む任意のパケットは、サーバ(たとえば、図1のサーバ124、126、128、130)に送られる前に廃棄され、それによって、パケットによるサーバのフラッディングを防止する。さらに別の利点は、再配置可能性の特徴にあり得る。この利点の実現は、第1のゲートウェイデバイスにおける対応する秘密鍵にフィルタリングルール(またはルールのセット)を定義/マッピングし、次いで、この秘密鍵を第2のゲートウェイデバイスと共有することによって理解され得る。したがって、第1のゲートウェイと第2のゲートウェイとの間ハンドオーバ中に、態様によって、秘密鍵の移送/共有を介してSDFフィルタの再配置が許可される。これによって、所与のSDFフィルタに関連付けられたフィルタリングルール(またはルールのセット)に関連するデータのすべてを移す必要性がなくなる。したがって、再配置可能性の利点によって、他の目的のためにデータのすべてを移すために使用されたかもしれない処理リソースが解放される。

【００４６】
図4は、本明細書において説明される態様による例示的なダウンリンク動作400を示す。例は、便宜上、ロングタームエボリューション(LTE)システムの文脈で示されている。例は、本明細書において説明される任意の態様の範囲にいかなる制限も課すことを意図するものではない。
【００４７】
図4に表されているのは、デバイス402(たとえば、チップコンポーネント、クライアントデバイス、ユーザ機器、ユーザデバイス、端末、モバイルデバイス)、アクセスノード404(たとえば、eNodeB)、サービングゲートウェイ(S-GW)406、P-GW408、およびPDN410(たとえば、インターネット)である。
【００４８】
次に、図4の例示的なダウンリンク動作について説明する。(たとえば、PDN410内に常駐するアプリケーションサーバ、アプリケーション、アプリケーションサービスからの)ダウンリンクIPフロー414は、P-GW408の判断および処理回路/モジュール/デバイス420に適用され得る。示されるダウンリンクIPフロー414の数は例示的なものであり、限定することを意図したものではない。判断および処理回路/モジュール/デバイス420は、ダウンリンクIPフロー414から受信されたダウンリンクパケットを、暗号検証およびトラフィックステアリング回路/モジュール/デバイス422に渡してもよいし、サービスデータフロー(SDF)テンプレート424およびその中のパケットフィルタ(図示せず)に渡してもよい。
【００４９】
その中に埋め込まれた、またはそれとともに含まれる、DLネットワークトークンを持つダウンリンクパケットは、暗号検証およびトラフィックステアリング回路/モジュール/デバイス422に渡されてよい。一態様では、DLネットワークトークンおよびアプリケーション識別子(App ID)は、単一のダウンリンクパケットに埋め込まれてもよいし、それとともに含まれてもよい。App IDは、アプリケーションアクセスポリシーを決定するために使用されてよい。アプリケーションアクセスポリシーは、アプリケーションサーバから取り出され得る。いくつかの実施形態では、アプリケーションサーバは、デバイスと通信する要求を開始するアプリケーションサーバであってもよいし、デバイスが通信を開始しようとするアプリケーションサーバであってもよい。しかしながら、第3のアプリケーションサーバも許容可能である。いくつかの態様では、アプリケーションアクセスポリシーは、アプリケーションサーバのアプリケーション関数(AF)から取り出され得る。他の態様では、アプリケーションアクセスポリシーは、ポリシーおよびチャージングルール関数サーバまたはデバイスに関連付けられた加入者プロファイルリポジトリ(SPR)から取り出され得る。
【００５０】
一態様では、アプリケーションアクセスポリシーは、たとえば、サービス優先順位、最大帯域幅、保証帯域幅、および/または最大遅延を含むサービス品質(QoS)パラメータを含んでよい。この情報は、DLネットワークトークンに関連付けられたダウンリンクパケットのためにデータフローまたはベアラを選択するために、暗号検証およびトラフィックステアリング回路/モジュール/デバイス422または何らかの他の回路/モジュール/デバイスによって使用可能であってよい。
【００５１】
その中に埋め込まれた、またはそれとともに含まれる、DLネットワークトークンを持たないダウンリンクIPフロー414内のダウンリンクパケットは、判断および処理回路/モジュール/デバイス420または他の回路/モジュール/デバイス(図示せず)によって、SDFテンプレート424に渡されてよい。
【００５２】
パケットフィルタ(図示せず)は、SDFテンプレート424とともに含まれてよい。SDFテンプレート424のパケットフィルタの使用は、暗号検証およびトラフィックステアリング回路/モジュール/デバイス422の使用が必要とするよりも多くの処理理ソースおよびメモリ

リソースを必要とし得る。SDFテンプレート424のパケットフィルタを使用してフィルタリングを実行するために、P-GW408は、SDFごとに別個のテーブルエントリを有するテーブル424aを維持することを必要とし得る。各テーブルエントリは、限定するものではないが、アプリケーションID、最大ビットレート(MBR)、およびアクセスポイント名-総合最大ビットレート(APN-AMBR)などの複数のパラメータの識別を必要とし得る。

【００５３】

SDFテンプレート424のパケットフィルタは、IPフローをベアラ418(たとえば、発展型パケットシステム(EPS)ベアラまたはIP-CANベアラ)へとフィルタリングする働きをする。3つのベアラ418は、例示のために示されている。一態様では、ベアラは、複数のアプリケーション/アプリケーションサービスによって共有されてよい。各ベアラは、パラメータの一意のセットに関連付けられてよい。

【００５４】

ダウンリンクIPフロー414は、たとえば、デフォルトベアラにマッピングされてもよいし、1つまたは複数の専用ベアラにマッピングされてもよい。デフォルトベアラは一般に、非保証ビットレートを有してよく、専用ベアラは一般に、保証ビットレートまたは非保証ビットレートのいずれかを有してよい。ベアラは、S-GW406およびアクセスノード404を通過してよい。アクセスノード404およびS-GW406の態様は、本明細書において説明されず、当業者に知られている。

【００５５】

データフロー

本明細書において説明される態様では、IPフロー、データフロー、またはフローは、図2の例示的な図に示されるベアラに限定される必要はない。クライアントデバイスは、1つまたは複数のアプリケーションを動作または実行してよい。各クライアントアプリケーションは、アプリケーションサーバ上で動作または実行するアプリケーションサービスにマッピングされてよい。アプリケーションサーバは、1つまたは複数のアプリケーションサービスに関連付けられてよい。したがって、フローは、デバイス内およびアプリケーションサーバ上で動作するアプリケーションに基づいて定義されてよい。フローは、クライアントデバイスにおいて実行されるアプリケーションとアプリケーションサーバにおいて実行されるアプリケーションサービスとの間でパケットが取る経路として定義されてよい。フローは、クライアントデバイス上で動作するアプリケーションに関連付けられてよいが、フローは、必ずしもクライアントデバイスを識別するとは限らない。ネットワークトークンは、1つまたは複数のフローを識別するために使用されてよい。したがって、ネットワークトークンは、複数のフローに関連付けられてよい。

【００５６】

1つのフローは、ネットワーク内の同じサーバ上で実行される複数のサービスにマッピングされ得る。たとえば、クライアントデバイスは、サーバ上の1つのプロバイダによって提供される1つのサービスを使用してよい。サーバは一般に、1つのIPアドレスを有する。しかしながら、サービスは、サーバ上で複数のアプリケーションをホストし得る。複数のアプリケーションとしては、たとえば、マッピングアプリケーション、情報検索アプリケーション、およびソーシャルネットワークアプリケーションがあり得る。したがって、複数のアプリケーションは同じ宛先IPアドレスを有し、そのため、コアネットワークのゲートウェイ(たとえば、P-GW)の観点から、複数のアプリケーションは、複数のフローの代わりに単一のフローと見なされてよい。したがって、単一のフローは、複数のサービスにマッピングされてよい。

【００５７】

フローは、複数のサービスに関連付け可能である。さらに、複数のアプリケーションサービスプロバイダがサービスを実行し得る場合、ネットワークトークンは複数のサービスに関連付け可能である。たとえば、クライアントデバイスは、複数のスポンサー(たとえば、複数のサービスプロバイダ)を有してよい。本明細書において説明される態様では、ゲートウェイデバイスは、複数のアプリケーションサービスプロバイダに関連付けられた

ネットワークトークンを導出し得る。したがって、単一のトークンは、1つまたは複数のフローに関連付けられた1つまたは複数のアプリケーションサービスにマッピングされ得る。

【００５８】

本明細書において提供されるいくつかの例では、ネットワークトークンは、アプリケーション識別子(App ID)に基づいて導出され得る。しかしながら、ネットワークトークンの導出は、そのような例に限定されない。他のパラメータ、および/またはパラメータの組合せは、ネットワークトークンを導出するために使用されてよい。App IDは、1つまたは複数のサーバに関連付けられてよい。たとえば、所与のサービスプロバイダは、異なる地理的場所において異なるデータセンタ(各々が、それ自体のサーバを有する)を有してよい。そのような場合、App IDは、複数のサーバに関連付けられるであろう。トークンは、サーバIPアドレスの代わりにApp IDを有利に使用してよい。ゲートウェイデバイスは、ネットワークトークンが宛先サーバのIPアドレスを指定しない場合であっても、ネットワークトークンに関連付けられたパケットが所与のサービスプロバイダのサーバに向かって進んでいることを検証することができる。

【００５９】

トークンセットアップおよび使用 - 例示的なシステムレベルコールフロー

本明細書において記載される例は、初期PDNコネクティビティ要求手順(その間に、デフォルトベアラがセットアップされ得る)および専用ベアラセットアップ手順(その間に、1つまたは複数の専用ベアラがセットアップされ得る)に適用されてよい。

【００６０】

図5は、本明細書において説明される態様による1つまたは複数のユーザプレーンメッセージに関連するネットワークトークン導出、プロビジョニング、および使用を示す例示的なコールフロー500である。示されたように、コールフローは、ユーザプレーン内で実施されてよい。図5は、デバイス502(たとえば、チップコンポーネント、クライアントデバイス)、アクセスノード504(たとえば、eNB)、MME506、S-GW508、P-GW510、ポリシーおよびチャージングルール関数(PCRF)512デバイス、ホーム加入者サーバ(HSS)514、ならびにアプリケーションサーバ516の表記を含む。

【００６１】

図5の例示的なコールフローでは、デバイス502は、接続要求をアプリケーションサーバ516に送り得る518。接続要求は、アプリケーション識別子(App ID)などの識別子を含み得る。接続要求は、コアネットワークをP-GW510にトランジット(transit)し得る。P-GW510は、ポリシー施行のためのゲートウェイであってよい。P-GW510はまた、ネットワークトークンの明確な要求または暗黙的要求を検出するために使用されてよい。

【００６２】

一態様によれば、アクセスノード504(たとえば、eNodeB)は、不可知論的(agnostic)であってよい。すなわち、アクセスノード504は、デバイスがユーザプレーン内でアプリケーションサーバ516に接続要求を送ったことを知らなくてよく、接続要求は、ネットワークトークンの要求を明確に含む、または、ネットワークトークンの暗黙的要求を表す、のいずれかである。そのような一態様によれば、ネットワークトークンの要求および交換は、不可知論的アクセスノード504にとって透過的であってよい。

【００６３】

決定は、デバイスから送られた接続要求を含むパケットが、ネットワークトークンの明確な要求を含むかまたはネットワークトークンの暗黙的要求を表すかに関して、P-GW510においてなされてよい。決定が、ネットワークトークンの必要性が存在すると結論する場合、P-GW510は、ネットワークトークンを導出し、ネットワークトークンを導出し、デバイス502からの接続要求を含んだパケットとともにネットワークトークンを埋め込む/含むために必要とされる情報を取得することを含むアクションを実行し得る。本明細書で使用されるとき、「導出する」という用語は、ローカルに導出すること、または別のデバイスから取得することを意味し得る。

【００６４】
一態様によれば、P-GW510は、パケットに関連付けられた入力パラメータのハッシュに基づいてネットワークトークンを導出し得る522。そのような一態様では、パケットに関連する追加情報を取得する必要がないことがある。追加情報が必要とされる場合、P-GW510は、PCRF512からデバイス502のプロファイルを取得し得る520。PCRF512は、PCRF512に結合された加入プロファイルリポジトリ(SPR)からデバイスの加入プロファイルを取得し得る。デバイス502のプロファイルを取得する他の手段も許容可能であってよい。
【００６５】
P-GW510は、ネットワークトークンを導出し得る522。一態様によれば、ネットワークトークンは、パケットに関連付けられた入力パラメータのハッシュに基づいて導出されてよい。一態様によれば、ネットワークトークンは、接続要求および/またはデバイスプロファイルに関連付けられた情報に基づいて導出されてよい。一例によれば、ネットワークトークンは、次のように導出され得る。

$$\text{ネットワークトークン}=CI|HMAC(K_{P-GW}, CI|IP_C|IP_S|P_C|P_S|Proto|App\ ID|\cdots)$$

上式で、CIはトークン導出に使用されるフィールドを定義するクラスインデックス、HMACは鍵付きハッシュメッセージ認証コード(keyed-hash message authentication code)、K_{P-GW}はP-GWの秘密鍵、IP_Cはクライアント(たとえば、デバイス)IPアドレス、P_Cはクライアントポート番号、IP_Sはサーバ(たとえば、宛先またはアプリケーションサーバ)IPアドレス、P_Sはサーバポート番号、Protoはプロトコル番号または識別子、App IDはアプリケーション識別子である。追加パラメータまたは代替パラメータとしては、優先順位および/またはサービス品質クラス識別子(QCI)があり得る。ネットワークトークンの導出のための他の式も許容可能であってよい。
【００６６】
P-GW510は、接続要求を含んだパケットとともにネットワークトークンを埋め込み/含み得る524。次いで、P-GWは、P-GW510によって導出されたネットワークトークンを含む接続要求をアプリケーションサーバ516に送り得る526。接続要求は、アプリケーション識別子(App ID)を含み得る。
【００６７】
次いで、アプリケーションサーバ516は、デバイス502に接続応答を送り得る528。接続応答は、ネットワークトークンを含み得る。その後、デバイス502は、アプリケーションサーバ516へのデータ送信のために構築された1つまたは複数のアップリンクデータパケットとともにネットワークトークンを含めてよい。いくつかの態様では、デバイス502は、アプリケーションサーバ516を宛先とするあらゆるアップリンクデータパケットとともに、ネットワークトークンを含めてよい。
【００６８】
施行に関して、デバイス502は、アプリケーションサーバ516にアップリンクデータパケットを送り得る530。アップリンクデータパケットは、ネットワークトークンを含み得る。ネットワークトークンを含むアップリンクデータパケットは、P-GW510にコアネットワークをトランジットし得る。述べたように、P-GW510は、ポリシー施行のためのゲートウェイであってよい。
【００６９】
P-GW510が、デバイス502から送られたアップリンクデータパケットを受信すると、P-GW510は、アップリンクデータパケットとともに含まれるネットワークトークンを検証し得る532。一態様によれば、検証は、トークンを再導出し(すなわち、検証トークンまたは元のネットワークトークンの複製を導出し)、再導出されたトークンを、アップリンクデータパケット埋め込まれたネットワークトークンと比較することによるものであってよい。検証が成功である場合、P-GW510は、埋め込まれたネットワークトークンを破棄することができ、アプリケーションサーバ516にアップリンクデータパケットを送り得る534。検証が成功でない場合、P-GWは、アップリンクデータパケットおよび埋め込まれたネットワークトークンを破棄してよい。

【００７０】
P-GW510に知られている秘密鍵は、元のネットワークトークンおよび検証トークン(たとえば、元のネットワークトークンの複製)を導出するために、暗号関数において使用されてよい。一例では、P-GW510は、アプリケーション関数(AF)から取り出されたアプリケーションアクセスポリシーに鑑みてネットワークトークンを導出し得る。一態様では、アクセスポリシーは、フローをアプリケーションに関連付け得る。たとえば、App IDがネットワークトークンの要求とともに含まれる場合、ネットワークトークンが、App IDに鑑みてさらに導出され得る。いくつかの態様では、ネットワークトークンは、暗号化された情報を含み得る。復号は、一例では、P-GW510に知られている秘密鍵をその入力として有する暗号関数を使用して達成され得る。例として、ネットワークトークンの復号成功は、ネットワークトークンを含むULパケットに関連して、サーバの宛先アドレスもしくは宛先アドレスプレフィックスならびに/またはアプリケーションサービスならびに/またはULパケットが発信されたクライアントデバイスおよび/もしくはアクセスノードのソースアドレスを示し得る値を与えることがある。一態様では、たとえば、ネットワークトークンからサーバおよび/またはアプリケーションサービスの宛先アドレスまたは宛先アドレスプレフィックスを取得できることは、トークンに関連付けられたパケットが、その宛先に送られることが許可されることを意味し得、SDFテンプレート(および、それらの関連付けられたパケットフィルタ)は必要とされないことをさらに意味し得る。したがって、パケットインスペクションが回避され得る。

【００７１】
本明細書において説明される、ユーザプレーンを使用する態様は、アップリンク方向およびダウンリンク方向に等しく十分に適用され得る。

【００７２】
図6は、本明細書において説明される態様による1つまたは複数のユーザプレーンメッセージに関連するネットワークトークン導出、プロビジョニング、および使用を示す例示的なコールフロー600である。示されたように、コールフローは、ユーザプレーン内で実施されてよい。図6は、デバイス602(たとえば、チップコンポーネント、クライアントデバイス)、アクセスノード604(たとえば、eNB)、MME606、S-GW608、P-GW610、ポリシーおよびチャージングルール関数(PCRF)612デバイス、ホーム加入者サーバ(HSS)614、ならびにアプリケーションサーバ616の表記を含む。例示的なコールフロー600によれば、ダウンリンク(DL)ネットワークトークンは、デバイス602によるDLネットワークトークンの使用のための暗黙的要求または明示的要求を介して、P-GW610によってアプリケーションサーバ616に発行され得る。

【００７３】
図6の例示的なコールフローでは、デバイス602は、P-GW610を介して、アプリケーションサーバ616を用いてアプリケーションサービスを開始する要求を送る618。要求は、アプリケーション識別子(App ID)によって達成されてもよいし、これを含んでもよい。当業者によって理解されるように、デバイス602からアプリケーションサーバ616に提供される要求は、デバイスとネットワークとの間の接続を確立または再確立する任意のタイプの接続要求とは異なっており、これと混同されるべきではない。前者の場合は、デバイスは、アプリケーションサーバからサービスを要求している(サービスは、コネクションレス型サービスですらあってよい)が、後者の場合は、デバイスは、ネットワークへの接続を要求している。

【００７４】
一態様では、アプリケーションサービスを開始する要求は、ダウンリンク(DL)ネットワークトークンの使用の暗黙的要求を表す。ダウンリンクネットワークトークンの使用の暗黙的要求は、P-GW610を介してデバイス602からアプリケーションサーバ616に初期パケットを送ることによって認識され得る。一例では、暗黙的要求は、DLネットワークトークンを運ぶためにアプリケーションサーバからのパケットを必要とする事業者のポリシーによってトリガされ得る。そのようなポリシーの認識は、たとえば、P-GWが、サービスによっ

て提供されるパケットに対してパケットインスペクションを実行し、サービスが、あらかじめ定義されたネットワークポリシーの施行のためのDLネットワークトークンを必要とすることを判断することによって取得され得る。ダウンリンクネットワークトークンの使用の暗黙的要求を示す他の手段も許容可能である。

【００７５】

一態様では、アプリケーションサービスを開始する要求としては、アプリケーションサーバからデバイスに送られる伝送におけるDLネットワークトークンの使用の明示的要求があり得る。一態様では、明示的要求は、アプリケーションサーバ616に送られる第1のパケット内に含まれ得る。しかしながら、これは必要条件ではない。

【００７６】

DLネットワークトークンの使用は、アプリケーションサービスが開始すると、またはアプリケーションサービスが修正されると、行われ得る。

【００７７】

DLネットワークトークンを使用する明示的要求または暗黙的要求の受信に応答して、一態様では、P-GW610は、PCRF612からデバイスプロファイルを取得し得る620。P-GW610は、単に例として、以下の式を使用してDLネットワークトークンを導出し得る622。

DLネットワークトークン=鍵ID | CI | ポリシーID | H(KP-GW, ポリシーID | IPS | IPC | PS| PC | Proto | App ID |…)

上式で、鍵IDはトークン導出に使用される鍵の識別子(すなわち、K_{P-GW})、CIはトークン導出に使用されるフィールドまたはトークンを導出するために使用される入力パラメータのリストを定義するクラスインデックス、ポリシーIDはフロー処理ポリシー(たとえば、QoSポリシー、ベアラへのフローのマッピング、および当業者によって理解されるフロー処理ポリシーの他の態様)を定義するポリシー識別子、Hはセキュアハッシュ関数(あるいは、ハッシュメッセージ認証コード(HMAC)が使用可能である)、K_{P-GW}はP-GWの秘密鍵、IP_Cはクライアント(たとえば、デバイス)IPアドレス、P_Cはクライアントポート番号、IP_SはサーバIPアドレス、P_Sはサーバポート番号、Protoはプロトコル番号、App IDはアプリケーション識別子である。ダウンリンクトークンに含まれるポリシーIDは、ダウンリンクパケットを所与のベアラにマッピングするために使用されてよい。あるいは、鍵IDをポリシーIDに使用することが可能であってよい。その場合、DLネットワークトークンの計算において、ポリシーID値が必要とされないことがある。

【００７８】

いったん導出されると、DLネットワークトークンは、アプリケーションサービスを開始する要求とともにパケットに埋め込まれてもよいし、これとともに含まれてもよい624。

【００７９】

任意選択で、P-GW610は、デバイスにより開始された接続を識別するために使用され得る接続識別子(接続IDまたはConn ID)を導出し得る626。一態様では、接続IDは、次のように導出され得る。

接続ID=鍵ID | CI | HMAC (K'_{P-GW}, IP_S | IP_C | P_S | P_C | Proto)

上式で、K'_{P-GW}は、DLネットワークトークンを導出するために使用される秘密鍵とは異なる、P-GWに知られている秘密鍵であってよい。接続IDは、P-GW610内のキャッシュに記憶され得る628。

【００８０】

P-GW610によって導出された埋め込まれた/含まれたDLネットワークトークンを含む、アプリケーションサービスを開始する要求は、アプリケーションサーバ616に送られ得る630。アプリケーションサービスを開始する要求は、アプリケーション識別子(App ID)と、DLネットワークトークンと、導出された場合は接続IDとを含んでよい。

【００８１】

アプリケーションサーバ616は、DLネットワークトークン(たとえば、DLネットワークトークンのコピー)と、導出された場合は接続IDとを含むアプリケーションサービス応答を、P-GW610を介してデバイス602に送り得る632。

【００８２】
P-GW610が、埋め込まれたDLネットワークトークンをその中に有するパケットを受信すると、P-GW610は、たとえば、元のネットワークトークンを導出することに関して上記で説明されたものと同じ式を使用して、パケットに含まれるデータからトークンを導出することによって、DLネットワークトークンを検証し得る634。すなわち、P-GW610は、デバイス602から受信されたデータを用いる代わりに、アプリケーションサーバ616から受信されたパケットからのデータを用いて、元のDLネットワークトークンを再導出し得る。当業者によって理解されるように、デバイス602から受信されたパケット内のデータのすべてが、アプリケーションサーバ616から受信されたパケット内のデータと同一であるとは限らない。しかしながら、同様に当業者によって理解されるように、一態様では、デバイス602から受信されたパケットとアプリケーションサーバ616から受信されたパケットの両方に含まれる共通データが、元のDLネットワークトークン(本明細書では、検証トークンとも呼ばれる)を再導出するために使用されてよい。元のDLネットワークトークンの例示的な導出に関して上記で説明されたように、そのような共通データとしては、CI、IP_S、IP_C、P_S、P_C、Proto、および/またはApp IDがあり得る。このリストは例示的なものであり、限定することを意図したものではない。

【００８３】
そのような一態様では、検証は、再導出されたDLネットワークトークンを、アプリケーションサーバ616から受信されたパケットに埋め込まれたDLネットワークトークンと比較することによって達成され得る。

【００８４】
バリデーションが成功であった場合、アプリケーションサーバ616からのアプリケーションサービス応答が、デバイス602に送られ得る636。一態様では、P-GW610は、応答とともにDLネットワークトークンを埋め込んでもよいし、これを埋め込んだまたは付着されたままであってもよい。別の態様では、P-GW610は、応答がデバイス602に送られる636前に、DLネットワークトークンを破棄してよい(図示せず)。バリデーションが成功でなかった場合、P-GW610は応答を破棄してよい(図示せず)。

【００８５】
その後、アプリケーションサーバ616は、P-GW610を介してアプリケーションサーバ616からデバイス602に送られた(DLネットワークトークンが導出された通信セッションに関連する)1つまたは複数のパケットに、DLネットワークトークンのコピーを埋め込み/含め得る。いくつかの態様では、アプリケーションサーバ616は、P-GW610を介してアプリケーションサーバ616からデバイス602に送られた(DLネットワークトークンが導出された通信セッションに関連する)あらゆるパケットに、DLネットワークトークンのコピーを埋め込み/含め得る。

【００８６】
図7は、本明細書において説明される態様による1つまたは複数のユーザプレーンメッセージに関連するネットワークトークン導出、プロビジョニング、および使用を示す例示的なコールフロー700である。示されたように、コールフローは、ユーザプレーン内で実施されてよい。図7は、デバイス702(たとえば、チップコンポーネント、クライアントデバイス)、アクセスノード704(たとえば、eNB)、MME706、S-GW708、P-GW710、ポリシーおよびチャージングルール関数(PCRF)712デバイス、ホーム加入者サーバ(HSS)714、ならびにアプリケーションサーバ716の表記を含む。例示的なコールフロー700によれば、ダウンリンク(DL)ネットワークトークンは、アプリケーションサーバ716によって作成されるDLネットワークトークンの使用のための暗黙的要求または明示的要求を介して、P-GW710によってアプリケーションサーバ716に発行され得る。

【００８７】
図7の例示的なコールフローでは、アプリケーションサーバ716は、P-GW710を介して、デバイス702を用いてアプリケーションサービスを開始する要求を送る718。要求は、アプリケーション識別子(App ID)によって達成されてもよいし、これを含んでもよい。当業者

によって理解されるように、アプリケーションサーバ716からデバイス702に提供される要求は、アプリケーションサーバとネットワークとの間の接続を確立または再確立する任意のタイプの接続要求とは異なっており、これと混同されるべきではない。前者の場合は、アプリケーションサーバは、デバイスにアプリケーションサービスを提供するように要求している(サービスは、コネクションレス型サービスですらあってよい)が、後者の場合は、アプリケーションサーバは、ネットワークへの接続を要求している。

【００８８】

一態様では、アプリケーションサービスを開始する要求は、ダウンリンク(DL)ネットワークトークンの使用の暗黙的要求を表す。ダウンリンクネットワークトークンの使用の暗黙的要求は、P-GW710を介してアプリケーションサーバ716からデバイス702に初期パケットを送ることによって認識され得る。一例では、暗黙的要求は、DLネットワークトークンを運ぶためにアプリケーションサーバからのパケットを必要とする事業者のポリシーによってトリガされ得る。そのようなポリシーの認識は、たとえば、P-GWが、サービスによって提供されるパケットに対してパケットインスペクションを実行し、サービスが、あらかじめ定義されたネットワークポリシーの施行のためのDLネットワークトークンを必要とすることを判断することによって取得され得る。ダウンリンクネットワークトークンの使用の暗黙的要求を示す他の手段も許容可能である。

【００８９】

一態様では、アプリケーションサービスを開始する要求としては、アプリケーションサーバからデバイスに送られる伝送におけるDLネットワークトークンの使用の明示的要求があり得る。一態様では、明示的要求は、デバイス702に送られる第1のパケット内に含まれ得る。しかしながら、これは必要条件ではない。

【００９０】

DLネットワークトークンの使用は、アプリケーションサービスが開始すると、またはアプリケーションサービスが修正されると、行われ得る。

【００９１】

DLネットワークトークンを使用する明示的要求または暗黙的要求の受信に応答して、一態様では、P-GW710は、PCRF712からデバイスプロファイルを取得し得る720。P-GW710は、単に例として、以下の式を使用してDLネットワークトークンを導出し得る722。

DLネットワークトークン=鍵ID | CI | ポリシーID | H(K_{P-GW}, ポリシーID | IP_S | IP_C | P_S| P_C | Proto | App ID | …)

上式で、鍵IDはトークン導出に使用される鍵の識別子(すなわち、K_{P-GW})、CIはトークン導出に使用されるフィールドまたはトークンを導出するために使用される入力パラメータのリストを定義するクラスインデックス、ポリシーIDはフロー処理ポリシー(たとえば、QoSポリシー、ベアラへのフローのマッピング、および当業者によって理解されるフロー処理ポリシーの他の態様)を定義するポリシー識別子、Hはセキュアハッシュ関数(あるいは、ハッシュメッセージ認証コード(HMAC)が使用可能である)、K_{P-GW}はP-GWの秘密鍵、IP_Cはクライアント(たとえば、デバイス)IPアドレス、P_Cはクライアントポート番号、IP_SはサーバIPアドレス、P_Sはサーバポート番号、Protoはプロトコル番号、App IDはアプリケーション識別子である。ダウンリンクトークンに含まれるポリシーIDは、ダウンリンクパケットを所与のベアラにマッピングするために使用されてよい。あるいは、鍵IDをポリシーIDに使用することが可能であってよい。その場合、DLネットワークトークンの計算において、ポリシーID値が必要とされないことがある。

【００９２】

いったん導出されると、DLネットワークトークンは、アプリケーションサービスを開始する要求とともにパケットに埋め込まれてもよいし、これとともに含まれてもよい724。

【００９３】

任意選択で、P-GW710は、サーバにより開始された接続を識別するために使用され得る接続識別子(接続IDまたはConn ID)を導出し得る726。一態様では、接続IDは、次のように導出され得る。

接続ID=鍵ID | CI | HMAC (K'_{P-GW}, IP_S | IP_C | P_S | P_C | Proto)
上式でK'_{P-GW}は、DLネットワークトークンを導出するために使用される秘密鍵とは異なる、P-GWに知られている秘密鍵であってよい。接続IDは、P-GW710内のキャッシュに記憶され得る728。

【００９４】

P-GW710によって導出された埋め込まれた/含まれたDLネットワークトークンを含む、アプリケーションサービスを開始する要求は、デバイス702に送られ得る730。アプリケーションサービスを開始する要求は、アプリケーション識別子(App ID)と、DLネットワークトークンと、導出された場合は接続IDとを含んでよい。

【００９５】

デバイス702が、埋め込まれたDLネットワークトークンを含むアプリケーションサービスを開始する要求を受信すると、デバイス702は、要求を検証し得る732。任意選択で、デバイス702は、認証のために別のトークンを発行してよい733。

【００９６】

デバイス702は、DLネットワークトークンを含むアプリケーションサービス応答をP-GW710を介してアプリケーションサーバ716に送る734ことによって、アプリケーションサーバ716にDLネットワークトークンを付与し得る。デバイス702は、アプリケーションサービス応答にDLネットワークトークンを埋め込んでもよいし、これを含んでもよい。接続IDがデバイス702に送られた場合、デバイス702はまた、アプリケーションサービス応答に接続IDを埋め込んでもよいし、これを含んでもよい。

【００９７】

接続IDが導出され726、記憶された728場合、P-GW710が、その中に埋め込まれたまたはそれに付着された接続IDおよびDLネットワークトークンを有するデバイス702からパケットを受信したとき、P-GW710は、接続IDを検証し得る736。DLネットワークトークンが、ダウンリンク方向における検証およびパケットマッピングに使用されるので、一態様では、P-GW710は、このとき、DLネットワークトークンを検証しなくてよい。しかしながら、述べたように、P-GW710は、接続IDを検証し得る736。

【００９８】

接続IDの検証は、たとえば、元の接続IDを導出することに関して上記で説明されたものと同じ式を使用して、パケットに含まれるデータから元の接続IDを再導出することによって達成され得る。すなわち、P-GW710は、アプリケーションサーバ716から受信されたデータを用いる代わりに、デバイス702から受信されたパケットからのデータを用いて、元の接続IDを再導出し得る。当業者によって理解されるように、デバイス702から受信されたパケット内のデータのすべてが、アプリケーションサーバ716から受信されたパケット内のデータと同一であるとは限らない。しかしながら、同様に当業者によって理解されるように、一態様では、デバイス702から受信されたパケットとアプリケーションサーバ716から受信されたパケットの両方に含まれる共通データのみが、元の接続ID(本明細書では、第2の接続IDまたは検証接続IDとも呼ばれる)を再導出するために使用されるであろう。元の接続IDの例示的な導出に関して上記で説明されたように、そのような共通データとしては、CI、IP_C、IP_S、P_C、P_S、および/またはProtoがあり得る。このリストは例示的なものであり、限定的ではない。そのような一態様では、検証は、再導出された接続IDを、デバイス702から受信されたパケットに埋め込まれた接続IDと比較することによって達成され得る。

【００９９】

検証が成功であった場合、または接続IDを検証する任意選択のステップが実行されなかった場合、デバイス702からのアプリケーションサービス応答は、アプリケーションサーバ716に送られ得る738。一態様では、P-GW710は、アプリケーションサービス応答とともにDLネットワークトークンを埋め込んでもよいし、これを付着または含めてもよい。このようにして、アプリケーションサーバ716は、DLネットワークトークンを備える。任意選択の接続IDのバリデーションが成功でなかった場合、P-GW710は、アプリケーションサー

ビス応答を破棄してよい(図示せず)。

【０１００】

その後、アプリケーションサーバ716は、P-GW710を介してアプリケーションサーバ716からデバイス702に送られた740(DLネットワークトークンが導出された通信セッションに関連する)各パケットに、DLネットワークトークンのコピーを埋め込み得る。P-GW710は、DLネットワークトークンを使用してデータパケットを検証し得る742。検証が成功である場合、P-GW710は、デバイス702にデータパケットを送り得る744。検証が成功でない場合、P-GW710は、データパケットを破棄し得る(図示せず)。

【０１０１】

図8は、本明細書において説明される態様による1つまたは複数のユーザプレーンメッセージに関連する2つのネットワークトークン(たとえば、アップリンクネットワークトークンおよびダウンリンクネットワークトークン)の導出、プロビジョニング、および使用を示す例示的なコールフロー800である。図8のコールフロー800は、ユーザプレーン内で実施されてよい。以下の説明は、アップリンクトークンとダウンリンクトークンの両方の導出、プロビジョニング、および施行に関する。

【０１０２】

図8は、デバイス802(たとえば、チップコンポーネント、クライアントデバイス)、アクセスノード804(たとえば、eNB)、MME806、S-GW808、P-GW810、ポリシーおよびチャージングルール関数(PCRF)812デバイス、ホーム加入者サーバ(HSS)814、ならびにアプリケーションサーバ816の表記を含む。

【０１０３】

図8の例示的なコールフローでは、デバイス802は、接続要求をアプリケーションサーバ816に送り得る818。接続要求は、アプリケーション識別子(App ID)などの識別子を含み得る。接続要求は、コアネットワークをP-GW810にトランジットし得る。P-GW810は、ポリシー施行のためのゲートウェイであってよい。P-GW810はまた、ネットワークトークンの明確な要求または暗黙的要求を検出するために使用されてよい。

【０１０４】

一態様によれば、アクセスノード804(たとえば、eNodeB)は、不可知論的であってよい。すなわち、アクセスノード804は、デバイスがユーザプレーン内でアプリケーションサーバ816に接続要求を送ったことを知らなくてよく、接続要求は、ネットワークトークンの要求を明確に含む、または、ネットワークトークンの暗黙的要求を表す、のいずれかである。そのような一態様によれば、ネットワークトークンの要求および交換は、不可知論的アクセスノード804にとって透過的であってよい。

【０１０５】

決定は、デバイスから送られた接続要求を含むパケットが、ネットワークトークンの明確な要求を含むかまたはネットワークトークンの暗黙的要求を表すかに関して、P-GW810においてなされてよい。決定が、ネットワークトークンの必要性が存在すると結論する場合、P-GW810は、ULネットワークトークンおよびDLネットワークトークンを導出し、デバイス802からの接続要求を含んだパケットとともにULネットワークトークンおよびDLネットワークトークンを埋め込む/含むために必要とされる情報を取得することを含むアクションを実行し得る。本明細書で使用されるとき、「導出する」という用語は、ローカルに導出すること、または別のデバイスから取得することを意味し得る。

【０１０６】

一態様によれば、P-GW810は、パケットに関連付けられた入力パラメータのハッシュに基づいて、ULネットワークトークンを導出し得る822。そのような一態様では、パケットに関連する追加情報を取得する必要がないことがある。追加情報が必要とされる場合、一態様によれば、P-GW810は、PCRF812からデバイス802のプロファイルを取得し得る820。PCRF812は、PCRF812に結合された加入プロファイルリポジトリ(SPR)からデバイスの加入プロファイルを取得し得る。デバイス802のプロファイルを取得する他の手段も許容可能であってよい。同様の様式で、P-GW810は、DLネットワークトークンを導出し得る823。

【０１０７】
P-GW810は、接続要求を含んだパケットとともにULネットワークトークンおよびDLネットワークトークンを埋め込み/含み得る824。次いで、P-GW810は、P-GW810によって導出されたULネットワークトークンおよびDLネットワークトークンを含む接続要求を、アプリケーションサーバ816に送り得る826。接続要求は、アプリケーション識別子(App ID)を含み得る。
【０１０８】
次いで、アプリケーションサーバ816は、P-GW810を介してデバイス802に接続応答を送り得る828。接続応答は、ULネットワークトークンを含んでよく、DLネットワークトークンも含んでよい。DLネットワークトークンが接続応答とともに含まれる場合、P-GW810は、接続応答とともに含まれるDLネットワークトークンを検証し得る830。一態様によれば、検証は、元のDLネットワークトークンの複製を導出し(すなわち、DL検証トークンを導出し)、再導出された元のDLトークンを、接続応答内に/これとともに埋め込まれた/含まれるDLネットワークトークンと比較することによるものであってよい。検証が成功である場合、P-GW810は、DLネットワークトークンを破棄し、ULネットワークトークンとともに接続応答をデバイス802に送る832ことができる。検証が成功でない場合、P-GW810は、接続要求ならびに埋め込まれた/含まれるDLネットワークトークンおよびULネットワークトークンを破棄し得る。その後、デバイス802は、アプリケーションサーバ816へのデータ送信のために構築された1つまたは複数のアップリンクデータパケットとともにULネットワークトークンを含めてよい834。いくつかの態様では、デバイス802は、アプリケーションサーバ816を宛先とするあらゆるアップリンクデータパケットとともに、ULネットワークトークンを含めてよい834。
【０１０９】
アプリケーションサーバ816は、DLネットワークトークン(たとえば、DLネットワークトークンのコピー)を保持し得る。その後、アプリケーションサーバ816は、デバイス802へのデータ送信のために構築された1つまたは複数のダウンリンクデータパケットとともにDLネットワークトークンを含めてよい840。いくつかの態様では、アプリケーションサーバ816は、デバイス802を宛先とするあらゆるダウンリンクデータパケットとともに、DLネットワークトークンを含めてよい。
【０１１０】
アップリンク方向における施行に関して、デバイス802は、P-GW810を介してアプリケーションサーバ816にアップリンクデータパケットを送り得る834。アップリンクデータパケットは、ULネットワークトークンを含み得る。ULネットワークトークンを含むアップリンクデータパケットは、P-GW810にコアネットワークをトランジットし得る。述べたように、P-GW810は、ポリシー施行のためのゲートウェイであってよい。
【０１１１】
P-GW810が、デバイス802から送られたULデータパケットアップリンクを受信すると、P-GW810は、アップリンクデータパケットとともに含まれるULネットワークトークンを検証し得る836。一態様によれば、検証は、トークンを再導出し(すなわち、UL検証ネットワークトークンを導出し)、再導出されたトークンを、アップリンクデータパケット埋め込まれたネットワークトークンと比較することによるものであってよい。検証が成功である場合、P-GW810は、埋め込まれたネットワークトークンを破棄することができ、アプリケーションサーバ816にアップリンクデータパケットを送り得る838。検証が成功でない場合、P-GWは、アップリンクデータパケットおよび埋め込まれたULネットワークトークンを破棄してよい。
【０１１２】
ダウンリンク方向における施行に関して、アプリケーションサーバ816は、P-GW810を介してデバイス802にダウンリンクデータパケットを送り得る840。ダウンリンクデータパケットは、パケットが向けられるデバイスを示すデバイスIDを含んでよい。ダウンリンクデータパケットは、DLネットワークトークンを含み得る。DLネットワークトークンは、デバ

イス802から明示的または暗黙的に受信されたダウンリンクトークンの使用の要求に応答して、P-GW810によって導出されている可能性がある。P-GW810は、ユーザプレーン内でアプリケーションサーバ816にDLネットワークトークンをプロビジョニングした可能性がある。P-GW810は、ダウンリンクデータパケットとともに含まれるDLネットワークトークンを検証し得る842。一態様によれば、検証は、元のDLネットワークトークンの複製を導出し(すなわち、DL検証トークンを導出し)、再導出された元のDLトークンを、ダウンリンクデータパケットとともに埋め込まれたDLネットワークトークンと比較することによるものであってよい。検証が成功である場合、P-GW810は、埋め込まれたDLネットワークトークンを破棄し、デバイス802にダウンリンクデータパケットを送る844ことができる。検証が成功でない場合、P-GWは、ダウンリンクデータパケットおよび埋め込まれたDLネットワークトークンを破棄してよい。

【０１１３】

この態様では、P-GW810は、ダウンリンク方向において、ならびにアップリンク方向において、IPフローを効率的に向けることが可能であり得る。P-GW810が元のDLネットワークトークンを導出したので、P-GW810は、アプリケーションサーバ816からパケットとともに受信されたDLネットワークトークンのバリデーションを行うことが可能であり得る。これは、TFT/SDFを使用するダウンリンクパケットインスペクションの有用で効率的な代替形態であることがある。

【０１１４】

たとえば、P-GW810に知られている秘密鍵は、元のDLネットワークトークンおよび検証DLトークンを導出するために、暗号関数において使用されてよい。一例では、P-GW810は、アプリケーション関数(AF)から取り出されたアプリケーションアクセスポリシーに鑑みてネットワークトークンを導出し得る。一態様では、アクセスポリシーは、フローをアプリケーションに関連付け得る。ネットワークトークンは、App IDまたはデバイスIDに鑑みてさらに導出され得る。いくつかの態様では、DLネットワークトークンは、暗号化された情報を含み得る。復号は、一例では、P-GW810に知られている秘密鍵をその入力として有する暗号関数を使用して達成され得る。例として、DLネットワークトークンの復号成功は、DLネットワークトークンを含むDLパケットに関連して、DLパケットが宛先とするデバイスおよび/またはアクセスノードの宛先アドレスまたは宛先アドレスプレフィックスを示し得る値を与えることがある。一態様では、たとえば、DLネットワークトークンからデバイスアドレスを取得できることは、DLネットワークトークンに関連付けられたパケットが、その宛先に送られることが許可されることを意味し得、パケットインスペクションは必要とされないことをさらに意味し得る。したがって、パケットインスペクションが回避され得る。

【０１１５】

ネットワークトークン、すなわちDLネットワークトークンとULネットワークトークンの両方は、特定の条件下でのみ妥当であることがある。たとえば、いくつかの態様では、ネットワークトークンは、定期的に変化し得る。別の態様では、ネットワークトークンは、ネットワークトークンの導出以降の所定の時間に基づいて満了を起こしやすいことがある。ネットワークトークンは、所定の時間が満了すると、妥当であることを中止する場合がある。いくつかの態様では、ネットワークトークンは、ネットワークトークンを導出するために使用される鍵(K_{P-GW})に課せられた制限に基づいて満了を起こしやすいことがある。たとえば、ネットワークトークンを導出するために使用される鍵は、新しい鍵(K''_{P-GW})によって交換されてよい。既存の鍵(たとえば、K'_{P-GW})の、新しい異なる鍵(たとえば、K''_{P-GW})との交換は、たとえば、既存の鍵の所定の定期満了、鍵識別子、または何らかの他のイベントに起因し得る。既存のネットワークトークンが、もはや有効でない、またはもはやネットワークトークンとしての使用に望ましくないと決定されるとき、P-GWは、新しいネットワークトークンを導出して、現在使用されているネットワークトークンを交換してよい。

【０１１６】

新しいネットワークトークンを導出する判断は、たとえば、P-GWにかかっていることがある。しかしながら、判断は、他のエンティティによってなされてよい。たとえば、一態様では、デバイスが、新しいネットワークトークンが必要とされることを決定し得る。別の態様では、アプリケーションサーバが、新しいネットワークトークンが必要とされることを決定し得る。いくつかの態様では、現在使用されているネットワークトークンが妥当な場合でも、ネットワークトークンの使用を開始したエンティティと異なるエンティティが、新しいネットワークトークンの使用を開始し得る。任意の態様では、本明細書において説明されたように、新しいネットワークトークンセットアップが、先行し得る。新しいネットワークトークンが既存のネットワークトークンと同一でないように、(ネットワークトークンを導出するために使用される複数のパラメータの中の)少なくとも1つのパラメータが変更されることが必要とされ得ることは、当業者には理解されよう。

【０１１７】

一態様では、ネットワークトークンを導出することは、デバイスに関連付けられたアプリケーション識別子(App ID)およびアプリケーションアクセスポリシーを検証することを含み得る。App IDは、以前に受信されたパケットに含まれてよく、この以前に受信されたパケットは、ネットワークトークンを導出するために使用された。App IDは、アプリケーションアクセスポリシーを決定するために使用され得る。アプリケーションアクセスポリシーは、アプリケーションサーバから取り出され得る。一態様では、アプリケーションアクセスポリシーは、アプリケーションサーバのアプリケーション関数(AF)から取り出され得る。別の態様では、アプリケーションアクセスポリシーは、アプリケーションサーバ内の加入者プロファイルリポジトリ(SPR)から取り出され得る。一態様では、アプリケーションアクセスポリシーは、サービス優先順位、最大帯域幅、保証帯域幅、および/または最大遅延を含むサービス品質(QoS)パラメータを含んでよい。

【０１１８】

トークン使用/施行 - 例示的なシステムレベルプロトコルスタック

次に、上記で説明されたネットワークトークンに対する使用および施行の態様が示される。

【０１１９】

ネットワークトークンの使用は、クライアントデバイス、アクセスノード、ゲートウェイデバイス、およびアプリケーションサーバのユーザプレーンプロトコルスタックとの間でのネットワークトークンの移動に関して説明され得る。本明細書において示されるのは、ユーザプレーンプロトコルスタックの例示的なセットを示す2つの図である。各図は、プロトコルスタック間でのネットワークトークン移動のその描写に関して、次の図と異なる。プロトコルスタックに表される層の多く、および層間の相互接続はよく知られている。これらの層について、図5の図に関して簡単に説明する。それらの説明は、繰返しを回避し、適用の簡潔さを改善するために、各例示的な図に関して繰り返されない。図のうちの1つは、その中に示されるそれぞれの態様に関連してネットワークトークンの移動に利用される層と見なされ得るシム層を含む。

【０１２０】

図9は、本明細書において説明される一態様によるシステムのユーザプレーンプロトコルスタック900の例示的な図である。図9は、クライアントデバイス902、アクセスノード904、ゲートウェイデバイス906、およびアプリケーションサーバ908を示す。例示的な図である図9では、クライアントデバイス902のプロトコルスタックは、最下層から上方に、物理(PHY)層910と、メディアアクセス制御(MAC)層912と、無線リンク制御(RLC)層914と、パケットデータコンバージェンスプロトコル(PDCP)層916と、インターネットプロトコル(IP)層918とを含み得る。一態様では、ネットワークトークンは、インターネットプロトコル(IP)バージョン6(IPv6)において定義されたIP拡張ヘッダ内で運ばれてよい。

【０１２１】

一態様では、シム層920が、クライアントデバイス902のユーザプレーンプロトコルスタックに追加されてよく、対応するシム層922が、ゲートウェイデバイス906のプロトコルス

タックに追加されてよい。シム層920および対応するシム層922は、本明細書において説明される態様によれば、クライアントデバイス902からゲートウェイデバイス906へのネットワークトークンの移動を容易にする。一態様では、シム層920は、クライアントデバイス902のIP層918の下かつMAC層912の上にある。この態様では、対応するシム層922は、ゲートウェイデバイス906のIP層924の下かつユーザプレーンのための汎用パケット無線サービス(GPRS)トンネリングプロトコル(GTP)(GTP-U)層の上にある。当業者に知られているように、GTP-Uは、GPRSバックボーンネットワーク内でユーザデータパケットを運ぶためのサービスを提供する。

【０１２２】

図9によって示される態様は、アクセスノード904による処理を必要としない、クライアントデバイス902からゲートウェイデバイス906へのネットワークトークン960の移動に有用であり得る。代替方法も許容可能である。例として、クライアントデバイス902は、上記で説明されたように、ユーザプレーンメッセージングを介してアプリケーションサーバ908からネットワークトークン960を受信し得る。ネットワークトークンの使用の一態様によれば、クライアントデバイス902は、アプリケーションサーバ908を宛先とするパケット内にネットワークトークンを含んでよい。ネットワークトークン960は、図9に示されるように、ゲートウェイデバイス906にシム層920のシムヘッダ内で運ばれてよい。ネットワークトークン960は、IPヘッダとは別個のシムヘッダ内で運ばれてよい。

【０１２３】

ゲートウェイデバイス906におけるネットワークトークンの検証が成功である場合、ゲートウェイデバイス906は、ネットワークトークンを破棄した後、パケットをアプリケーションサーバ908に転送してよい。ゲートウェイデバイス906におけるネットワークトークンの検証が成功でない場合、ゲートウェイデバイス906は、パケットおよびネットワークトークンを破棄してよい。図示の態様によれば、ネットワークトークンベースアプリケーションアクセスをサポートするために、アプリケーションサーバ908における変更は必要とされないであろう。

【０１２４】

次に、説明を完全なものにするために、アクセスノード904、ゲートウェイデバイス906、およびアプリケーションサーバ908のユーザプレーンプロトコルスタックの層について簡単に説明する。例示的な図である図9では、アクセスノード904のプロトコルスタックは、最下層から上方に、物理(PHY)層930と、メディアアクセス制御(MAC)層932と、無線リンク制御(RLC)層934と、パケットデータコンバージェンスプロトコル(PDCP)層936とを含み得、これらはそれぞれ、クライアントデバイス902の同じように名付けられた層(910、912、914、および916)と結び付く。例示的な図である図9では、さらに、アクセスノード904のプロトコルスタックは、最下層から上方に、イーサネット（登録商標）層940と、MAC層942と、IP層944と、ユーザデータグラムプロトコル(UDP)層946と、GTP-U948とを含む。これらのそれぞれの層は、ゲートウェイデバイス906の同じように名付けられた層(950、952、954、956、および926)と結び付く。図9の例示的な図では、クライアントデバイスIP層918はゲートウェイデバイス906のIP層924につながり、ゲートウェイデバイス906のIP層924はアプリケーションサーバ908のIP層958につながる。

【０１２５】

図10は、本明細書において説明される別の態様によるシステムのユーザプレーンプロトコルスタック1000の例示的な図である。図10は、クライアントデバイス1002と、アクセスノード1004と、ゲートウェイデバイス1006と、アプリケーションサーバ1008とを示す。

【０１２６】

図10によって示される態様は、アクセスノード1004を介した、クライアントデバイス1002からゲートウェイデバイス1006へのネットワークトークン1060の移動に有用であり得る。この態様では、シム層は必要とされない。例として、クライアントデバイス1002は、上記で説明されたように、ユーザプレーンメッセージングを介してアプリケーションサーバ1008からネットワークトークン1060を受信し得る。ネットワークトークンの使用の一態様

によれば、クライアントデバイス1002は、アプリケーションサーバ1008を宛先とするパケット内にネットワークトークン1060を含んでよい。ネットワークトークン1060を含むパケットは、PDCP層1016ヘッダ内でクライアントデバイス1002からアクセスノード1004のPDCP層1036に運ばれてよい。アクセスノード1004は、PDCPヘッダ内で見つかったネットワークトークンをGTP-Uヘッダへとコピーし得る。次いで、ネットワークトークン1060を含むパケットは、GTP-U層1048ヘッダ内でアクセスノード1004からゲートウェイデバイス1006のGTP-U層1026に運ばれてよい。すなわち、一態様では、ネットワークトークンは、汎用パケット無線サービス(GPRS)トンネリングプロトコル(GTP)ヘッダ内で運ばれてよい。例示的な一態様では、元来アプリケーションサーバ1008からクライアントデバイス1002に送られるネットワークトークンが、ゲートウェイデバイスに知られている秘密鍵を使用して、ゲートウェイデバイス1006において作成された可能性がある。そのような一態様では、(アクセスノード1004は、検証に必要とされる秘密鍵を所有していないであろうという理由から)アクセスノード1004は、ネットワークトークンを検証することができないであろう。したがって、図10の図におけるアクセスノード1004の例示的な目的は、1つのヘッダから別のヘッダにネットワークトークンをコピーし、それによって、すでに存在しているPDCP層1036ヘッダおよびGTP-U層1048ヘッダを介してクライアントデバイス1002からゲートウェイデバイス1006にネットワークトークンを転送することである。ネットワークトークンがいったんゲートウェイデバイスに到達すると、ゲートウェイデバイス1006におけるネットワークトークンの検証が成功である場合、ゲートウェイデバイス1006は、ネットワークトークンを破棄した後、パケットをアプリケーションサーバ1008に転送してよい。ゲートウェイデバイス1006におけるネットワークトークン1060の検証が成功でない場合、ゲートウェイデバイス1006は、パケットおよびネットワークトークンを破棄してよい。図示の態様によれば、トークンベースアプリケーションアクセスをサポートするために、アプリケーションサーバ1008における変更は必要とされないであろう。

【０１２７】

次に、図10に関連して説明されなかったクライアントデバイス1002、アクセスノード1004、ゲートウェイデバイス1006、およびアプリケーションサーバ1008のユーザプレーンプロトコルスタックの層については、その説明が、図9の同じように名付けられた層の説明と同じまたはこれに類似しているので、説明しない。

【０１２８】

図11は、本明細書において説明される別の態様によるシステムのユーザプレーンプロトコルスタック1100の例示的な図である。図11のユーザプレーンプロトコルスタック1100は、トークン埋込みおよび搬送にIPヘッダを利用する。図11は、クライアントデバイス1102と、アクセスノード1104と、ゲートウェイデバイス1106と、アプリケーションサーバ1108とを示す。例示的な図である図11では、クライアントデバイス1102のプロトコルスタックは、最下層から上方に、物理(PHY)層1110と、メディアアクセス制御(MAC)層1112と、無線リンク制御(RLC)層1114と、パケットデータコンバージェンスプロトコル(PDCP)層1116と、インターネットプロトコル(IP)層1118とを含み得る。

【０１２９】

一態様では、IP層1118のヘッダは、本明細書において説明される態様により、クライアントデバイス1102とゲートウェイデバイス1106とアプリケーションサーバ1108との間のネットワークトークンの移動を容易にし得る。IPv4とIPv6は両方とも、本明細書において説明される態様を用いてよい。

【０１３０】

図11によって示される態様は、アクセスノード1104による処理を必要としない、ゲートウェイデバイス1106とクライアントデバイス1102との間のダウンリンクネットワークトークン1160の移動に有用であり得る。例として、施行動作中に、クライアントデバイス1102は、1つまたは複数のユーザプレーンメッセージにおいて、ゲートウェイデバイス1106を介してアプリケーションサーバ1108からダウンリンクネットワークトークン1160を受信し得る。ダウンリンクネットワークトークンの使用の一態様によれば、アプリケーションサ

ーバ1108は、クライアントデバイス1102を宛先とするパケット内に、所与のダウンリンクネットワークトークンのコピーを含んでよい。IP層1118、1124、1158内のIPヘッダは、図11に示されるように、(たとえば、ダウンリンクパケット内に埋め込まれた)ダウンリンクネットワークトークン1160をゲートウェイデバイス1106に運んでよい。ゲートウェイデバイス1106におけるダウンリンクネットワークトークンの検証が成功である場合、ゲートウェイデバイス1106は、パケットをクライアントデバイス1102に転送してよい。ゲートウェイデバイス1106は、検証されたダウンリンクネットワークトークンを含んだパケットを転送する前にネットワークトークンを破棄してもよいし、破棄しなくてもよい。ゲートウェイデバイス1106におけるダウンリンクネットワークトークン1160の検証が成功でない場合、ゲートウェイデバイス1106は、パケットおよびネットワークトークンを破棄してよい。図示の態様によれば、DLトークンベースポリシー施行プロトコルをサポートするために、アプリケーションサーバ1108における変更は必要とされないであろう。

【０１３１】

DLトークンを含むパケットの配信に関して、一態様では、DLトークンは、IPバージョン4(IPv4)ヘッダまたはIPバージョン6(IPv6)ヘッダなどのIPヘッダ内に埋め込まれてよい。IPv4におけるIPヘッダは、IPv4 Optionsフィールドであってよい。IP Optionsフィールドに関して、例示的なIPv4 Optionsフィールドの使用のために、インターネット技術標準化委員会(IETF)において、新しいオプション番号が定義されることが必要な場合がある。IPv6におけるIPヘッダは、IP拡張ヘッダであってよい。IP拡張ヘッダに関して、例示的なIPv6拡張ヘッダの使用のために、インターネット技術標準化委員会(IETF)において、Next Header Codeなどのコードが定義されることが必要な場合がある。一態様では、DLトークンは、伝送制御プロトコル(TCP)ヘッダ内に埋め込まれてよい。DLトークンは、TCPヘッダのOptionsフィールド内に埋め込まれてよい。一態様では、DLトークンは、トランスポート層セキュリティ(TLS)レコードヘッダ内に埋め込まれてよい。TLSレコードに関して、新しいレコードタイプが、例示的なTLSレコードプロトコルのために、インターネット技術標準化委員会(IETF)において定義されることが必要な場合がある。一態様では、DLトークンは、IPヘッダと伝送制御プロトコル/ユーザデータグラムプロトコル(TCP/UDP)ヘッダとの間でシムヘッダ内に埋め込まれてよい。さらに別の態様では、DLトークンは、ハイパーテキスト転送プロトコル(HTTP)ヘッダ内に埋め込まれてよい。HTTPヘッダは、HTTP eXperimentalまたはeXtensionヘッダであってよい。HTTP eXperimentalまたはeXtensionヘッダは、セキュアでないHTTP接続にX-タグを利用してよい。

【０１３２】

次に、図11に関連して説明されたクライアントデバイス1102、アクセスノード1104、ゲートウェイデバイス1106、およびアプリケーションサーバ1108のプロトコルスタックの層については、その説明が、図9の同じように名付けられた層の説明と同じまたはこれに類似しているので、説明しない。

【０１３３】

図12は、本明細書において説明される別の態様によるシステムのユーザプレーンプロトコルスタック1200の例示的な図である。図12のユーザプレーンプロトコルスタック1200において、ネットワークトークン搬送のために、シム層1220、1222、1223が追加された。図12は、クライアントデバイス1202、アクセスノード1204、ゲートウェイデバイス1206、およびアプリケーションサーバ1208を示す。

【０１３４】

図12によって示される態様は、ゲートウェイデバイス1206を介した、アプリケーションサーバ1208からクライアントデバイス1202に向けてダウンリンクネットワークトークン1260の移動に有用であり得る。いくつかの態様では、ダウンリンクネットワークトークンは、アプリケーションサーバ1208からゲートウェイデバイス1206に搬送され得るが、クライアントデバイス1202には搬送されない。例として、アプリケーションサーバ1208は、ユーザプレーンメッセージングを介してゲートウェイデバイス1206からダウンリンクネットワークトークン1260を受信し得る。

【０１３５】
例示的な図である図12では、クライアントデバイス1202のプロトコルスタックは、最下層から上方に、物理(PHY)層1210と、メディアアクセス制御(MAC)層1212と、無線リンク制御(RLC)層1214と、パケットデータコンバージェンスプロトコル(PDCP)層1216と、インターネットプロトコル(IP)層1218と、シム層1220とを含み得る。
【０１３６】
一態様では、シム層1220が、クライアントデバイス1202のユーザプレーンプロトコルスタックに追加されてよく、対応するシム層1222が、ゲートウェイデバイス1206のプロトコルスタックに追加されてよく、さらに別の対応する対応するシム層1223が、アプリケーションサーバ1208のプロトコルスタックに追加されてよい。シム層1220、対応するシム層1222、および対応するシム層1223は、クライアントデバイス1202とゲートウェイデバイス1206とアプリケーションサーバ1208との間のネットワークトークンの移動を容易にし得る。一態様では、シム層1220は、クライアントデバイス1202のIP層1218の上にある。この態様では、対応するシム層1222はゲートウェイデバイス1206のIP層1224の上にあり、対応するシム層1223は、アプリケーションサーバ1208のIP層1258の上にある。
【０１３７】
図12によって示される態様は、アプリケーションサーバ1208とゲートウェイデバイス1206との間のダウンリンクネットワークトークン1260の移動に有用であり得る。クライアントデバイス1202にダウンリンクネットワークトークンを搬送することが必要な場合、図12によって示される態様は、アクセスノード1204による処理を必要としない、そのような搬送を提供する。
【０１３８】
例として、施行動作中に、ゲートウェイデバイス1206は、1つまたは複数のユーザプレーンメッセージにおいて、アプリケーションサーバ1208からダウンリンクネットワークトークンを受信し得る。シムヘッダは、ダウンリンクネットワークトークン1260をゲートウェイデバイス1206に運び得る。
【０１３９】
ゲートウェイデバイス1206におけるダウンリンクネットワークトークン1260の検証が成功である場合、ゲートウェイデバイス1206は、ダウンリンクネットワークトークン1260に関連付けられたパケットパケットをクライアントデバイス1202に転送してよい。ゲートウェイデバイスは、パケットをクライアントデバイス1202に転送する前に、ダウンリンクネットワークトークン1260を破棄してよい。ゲートウェイデバイス1206におけるダウンリンクネットワークトークン1260の検証が成功でない場合、ゲートウェイデバイス1206は、パケットおよびダウンリンクネットワークトークン1260を破棄してよい。
【０１４０】
次に、図12に関連して説明されなかったクライアントデバイス1202、アクセスノード1204、ゲートウェイデバイス1206、およびアプリケーションサーバ1208のユーザプレーンプロトコルスタックの層については、その説明が、図9の同じように名付けられた層の説明と同じまたはこれに類似しているので、説明しない。
【０１４１】
例示的なデバイス
図13は、本明細書において説明される態様によるネットワークトークンを使用するネットワークポリシー施行および/またはパケットステアリングをサポートするように構成された例示的なデバイス1300を示すブロック図である。本明細書で使用されるとき、「デバイス」という用語は、チップコンポーネントおよび/またはクライアントデバイスなどのエンドユーザデバイス(たとえば、モバイルデバイス、ユーザ機器、ユーザデバイス)を示し得る。一例では、デバイス1300は、ワイヤレスネットワーク上で通信するためのネットワーク通信インターフェース回路1302と、ネットワーク通信インターフェース回路1302に結合された処理回路1304と、処理回路1304に結合されたメモリデバイス1306とを含んでよい。このリストは非限定的である。

【０１４２】
ワイヤレスネットワーク上で通信するためのネットワーク通信インターフェース回路1302は、ユーザとの入力/出力動作のための第1の入力/出力モジュール/回路/関数1308を含んでよい。ネットワーク通信インターフェース回路1302は、アクセスノードとのワイヤレス通信のための受信機/送信機モジュール/回路/関数1310を含んでよい。このリストは非限定的である。
【０１４３】
処理回路1304は、トークンベースアプリケーションアクセスをサポートするように構成された、1つまたは複数のプロセッサ、特定用途向けプロセッサ、ハードウェアおよび/またはソフトウェアモジュールなどを含んでもよいし、これらを実施してもよい。たとえば、ネットワークトークンハンドリングモジュール/回路/関数1312は、メモリデバイス1306内に記憶され得る非共有秘密鍵または共有秘密鍵に基づいて、トークンを導出するように構成されてよい。別の例として、ネットワークトークン抽出/埋込みモジュール/回路/関数1314は、デバイスからのアップリンクパケットからネットワークトークンを抽出する、および/またはゲートウェイデバイスに送られたダウンリンクパケット内にネットワークトークンを埋め込む(これを含める)ように構成されてよい。さらに別の例として、暗号バリデーション/検証モジュール/回路/関数1316は、たとえば、パケットとともに受信されたネットワークトークンのバリデーションを行う/検証するように構成されてよい。このリストは非限定的である。
【０１４４】
メモリデバイス1306は、ネットワークトークンハンドリング命令1320と、ネットワークトークン抽出/埋込み命令1322と、暗号バリデーション/検証命令1324と、共有および非共有の秘密鍵記憶および命令1326とを含むように構成されてよい。このリストは非限定的である。
【０１４５】
ネットワーク通信インターフェース回路1302と処理回路1304とメモリデバイス1306とデバイス1300の他の構成要素との間の通信は、通信バス1334を経由してよい。
【０１４６】
デバイスにおいて動作可能である方法
図14は、デバイス(たとえば、チップコンポーネント、クライアントデバイス)が、1つまたは複数のアプリケーションサービスに関連付けられたアプリケーションサーバと通信し、通信に関連してネットワークトークンを利用する要求を開始し得る例示的な方法1400である。ネットワークトークンは、ネットワークポリシー施行およびデータパケットステアリング(たとえば、ユーザデータメッセージ関連パケットのステアリング)に使用されてよい。ネットワークトークンは、アプリケーションサーバとデバイスとの間のアプリケーションサービス伝送のバリデーションおよびマッピングのために使用されてよい。方法1400は、デバイスにおいて動作可能であってよい。方法1400は、デバイスが、ネットワークトークンを使用する要求を開始する場合に適用され得る。ネットワークトークンは、アップリンク(UL)ネットワークトークンであってもよいし、ダウンリンク(DL)ネットワークトークンであってもよいし、ULネットワークトークンとDLネットワークトークンの両方であってもよい。
【０１４７】
一態様では、デバイスは、ユーザプレーンメッセージングを使用して、1つまたは複数のアプリケーションサービスに関連付けられたアプリケーションサーバとの接続を開始し得る1402。
【０１４８】
接続の開始に応答して、デバイスは、アプリケーションサーバからネットワークトークンを取得し得る1404。ネットワークトークンは、1つまたは複数のフローのセットにおける第1のフローに関連付けられ得る。ネットワークトークンは、1つまたは複数のアプリケーションサービスのうちの第1のアプリケーションサービスに関連付けられ得る。ネット

ワークトークンは、1つまたは複数のユーザプレーンメッセージを介してデバイスにプロビジョニングされ得る。

【０１４９】

ネットワークトークンを受信した後、デバイスは、ユーザプレーン内でその後デバイスからアプリケーションサーバに送られる1つまたは複数のアップリンク(UL)パケットとともにネットワークトークンを送り得る1406。いくつかの態様によれば、デバイスは、ユーザプレーン内でその後デバイスからアプリケーションサーバに送られるあらゆるアップリンク(UL)パケットとともにネットワークトークンを含み得る。

【０１５０】

ネットワークトークンは、コアネットワークのゲートウェイデバイス(たとえば、P-GW)によって導出され得る。すなわち、いくつかの態様によれば、アプリケーションサーバは、ネットワークトークンをデバイスに提供する。しかしながら、アプリケーションサーバはネットワークトークンを導出しなかった。本明細書において説明される態様によれば、ネットワークトークンは、ゲートウェイデバイスによって導出され、アプリケーションサーバに送られ得る。これによって、ユーザプレーン内でアプリケーションサーバからデバイスへのネットワークトークンの配信が可能になり得る。ネットワークトークンは、パケット内に埋め込まれてもよいし、これとともに含められてもよい。いくつかの態様では、ネットワークトークンは、1つまたは複数のパケット間で分散され得る。

【０１５１】

いくつかの態様によれば、ネットワークトークンは、デバイスに対してコアネットワークによって施行されたポリシーを反映する。いくつかの態様によれば、コアネットワーク内のゲートウェイデバイスは、コアネットワークによって維持されるデバイスのデバイス加入プロファイルおよび/または第1のアプリケーションサービスのポリシーに基づいて、ネットワークトークンを導出し得る。

【０１５２】

デバイス加入プロファイルは、加入プロファイルリポジトリ(SPR)内に記憶され得る。PCRFはSPRと通信し得る。言い換えると、PCRFは、ユーザおよび/またはデバイスの加入プロファイルをSPRに要求し得る。ネットワークトークンは、加入プロファイルに関してコアネットワークによって施行されるポリシーを反映し得る。たとえば、ポリシーは、音声トラフィックまたはリアルタイムメディアトラフィックに関する具体的なQoS要件を含み得る。

【０１５３】

本明細書において説明される様々な態様によれば、接続を開始することは、接続要求を送ることを含んでよく、接続要求は、ネットワークトークンの明示的要求を含み得る。他の態様によれば、接続を開始することは、ネットワークトークンの暗黙的要求を表すパケットを送ることを含んでよい。

【０１５４】

明示的または暗黙的のいずれかであるネットワークトークンの要求に応答したネットワークトークンの受信を保証するために、接続を開始するプロセスは、アプリケーションサーバに肯定応答を求めるパケットを送ることを含んでよく、肯定応答は、ネットワークトークンをデバイスに搬送する。したがって、一態様によれば、ネットワークトークンは、デバイスによって受信される肯定応答パケット内に含まれてよい。たとえば、パケットは、伝送制御プロトコル同期(TCP SYN)パケットであってよい。この態様によれば、デバイスによって受信されるネットワークトークンは、デバイスによって受信されるTCP SYN肯定応答(ACK)パケット内に含まれてよい。

【０１５５】

ネットワークトークンの暗黙的要求は、いくつかの手段において認識され得る。一態様によれば、暗黙的要求は、たとえば、ネットワークトークン(たとえば、DLネットワークトークン)を運ぶために所与のアプリケーションサーバからのパケットを必要とする事業者のポリシーの認識によって認識され得る。一態様によれば、デバイスが最初にアプリケ

ーションサーバと接続しようとしたとき、暗黙的要求が認識され得る。そのような一態様では、P-GWは、デバイス(たとえば、チップコンポーネント、クライアントデバイス)からアプリケーションサーバに向けられた第1のパケットを検出すると、暗黙的要求が作成されることを決定し得る。別の態様によれば、暗黙的要求は、ネットワークトークンを必要とするアプリケーションサーバの宛先アドレスまたは宛先アドレスプレフィックスを含むパケットの伝送において含まれ得る(P-GWが、宛先アプリケーションサーバがネットワークトークンの使用を必要とすることを認識する場合)。さらなる例として、第1のネットワークトークンの暗黙的要求が、デバイスから送られるパケットとともに含まれるアプリケーション識別子(App ID)に基づいて確立され得る(P-GWが、アプリケーション識別子に関連付けられたアプリケーションサービス、アプリケーションサーバ、またはアプリケーションがネットワークトークンの使用を必要とすることを認識する場合)。いくつかの態様では、(たとえば、制御プレーン内の)新しい信号は、ネットワークトークンの明示的および/または暗黙的使用を実施することが必要とされないことがある。

【０１５６】

いったんデバイスがネットワークトークンを受信すると、施行目的のために、アップリンクデータパケットに関連するネットワークトークンをP-GWに搬送するいくつかの手段があり得る。一態様によれば、ネットワークトークンは、ユーザプレーンシムヘッダ内でデバイスからパケットデータネットワーク(PDN)ゲートウェイ(P-GW)に搬送され得る。ユーザプレーンシムヘッダは、インターネットプロトコル(IP)層の上に配置されてよい。あるいは、ユーザプレーンシムヘッダは、インターネットプロトコル(IP)層の下に配置されてよい。別の態様によれば、ネットワークトークンは、IPバージョン6(IPv6)において定義されるインターネットプロトコル(IP)拡張ヘッダ内でデバイスからパケットデータネットワーク(PDN)ゲートウェイ(P-GW)に搬送され得る。別の態様によれば、ネットワークトークンは、パケットデータコンバージェンスプロトコル(PDCP)層内でデバイスからアクセスノードに搬送され得る。ネットワークトークンは、次いで、アクセスノード内のユーザプレーン(GTP-U)ヘッダのために、汎用パケット無線サービス(GPRS)トンネリングプロトコル(GTP)層にコピーされ得る。ネットワークトークンは、次いで、GTP-U層内でアクセスノードからパケットデータネットワーク(PDN)ゲートウェイ(P-GW)に搬送され得る。

【０１５７】

一態様では、ネットワークトークンは、ベアラおよび/またはデータフローに関連付けられ得る。ネットワークトークンは、アプリケーションサーバ、アプリケーションサービス、および/またはデバイスにバインドされ得る。一態様では、アプリケーションサービスを開始する要求は、要求の宛先であるアプリケーションサーバまたはアプリケーションサービスを識別するために、アプリケーション識別子(App ID)を含んでよい。そのような一態様では、または任意の他の態様では、ネットワークトークンは、アプリケーションサーバ、App ID、およびデバイスにバインドされ得る。本明細書で使用されるとき、(「トークンがパラメータに『バインドされる』」のような)「バインドされる」という用語は、トークン(すなわち、DLトークン)が、限定されるものではないが、名前付きバインドパラメータを含む関数を使用して導出され得ることを示す。関数は名前付きパラメータに限定されないことが理解されよう。例として、DLトークンは、アプリケーションサーバおよびデバイスにバインドされ得る(すなわち、トークンは、識別されたアプリケーションサーバおよび識別されたデバイスに固有である)。しかしながら、DLトークンを導出するために使用される式は、アプリケーションサーバおよび/またはデバイスを具体的に識別するパラメータに加えて、パラメータを含んでよい。本明細書において記載されるパラメータは、ネットワークトークンを導出するために使用される式の例に関連して、網羅的または限定的であることを意図するものではないことが理解されよう。

【０１５８】

DLトークンは、たとえば、秘密鍵、ポリシー識別子、発信元インターネットプロトコル(IP)アドレス、発信元ポート番号、宛先IPアドレス、宛先ポート番号、プロトコル識別子(ID)、App ID、優先順位、および/またはサービス品質クラス識別子(QCI)を含む入力パラ

メータのセットとともに関数を使用して導出され得る。一例では、DLトークンは、関数の結果、ならびにDLトークン導出に使用される鍵を識別する鍵識別子(鍵ID)などの、リストされたばかりのパラメータおよび/または他のパラメータのうちのいくつかの連結を含んでよい。DLトークンは、トークン導出に使用されるフィールドを定義するクラスインデックス(CI)を含んでもよいし、トークンを導出するために使用される入力パラメータのリストを含んでもよい。いくつかの態様では、秘密鍵(たとえば、K_{P-GW}、図4および図5)は、ゲートウェイデバイスのみに知られてよい。

【０１５９】

一態様では、鍵識別子は、トークン導出に使用される秘密鍵を定義し得る。鍵識別子は、定期的に、またはP-GWからの命令により、変化してよい。ゲートウェイデバイスのみが秘密鍵を知り得る。いくつかの態様では、P-GWは、トークン導出のために複数の鍵を有してよい。P-GWがトークン導出鍵を変更する場合、2つの鍵は同時に有効であってよい。したがって、鍵識別子は、そのようなシナリオにおいて即時トークン廃止を回避するために使用されてよい。

【０１６０】

クラスインデックス(CI)は、トークン導出に使用されるフィールドを定義してもよいし、トークンを導出するために使用される入力パラメータのリストを定義してもよい。

【０１６１】

一態様では、DLトークンは、鍵識別子、クラスインデックス(CI)、ポリシー識別子、およびDLトークンの導出に関連して使用される関数の出力の連結であってよい。いくつかの態様では、この関数は、SHA-1、SHA-2、またはSHA-3などのセキュアハッシュアルゴリズム(SHA)などのセキュアハッシュ関数であってよい。他の実施形態では、関数は、ハッシュメッセージ認証コード(HMAC)関数であってよい。さらに他の実施形態では、関数は、メッセージ認証コード(MAC)導出関数であってよい。MAC導出関数としては、暗号ブロック連鎖メッセージ認証コード(CBC-MAC)関数、暗号ベースMAC(CMAC)関数、またはガロアメッセージ認証コード(GMAC)関数があり得る。

【０１６２】

P-GWは、DLトークンの明示的要求または暗黙的要求を発したデバイスまたはアプリケーションサーバを識別するためにP-GWによって使用され得る接続識別子も導出し得る。接続IDは、DLトークンの導出の前、その間、またはその後に導出されてよい。接続IDは、P-GWのものであってよく、P-GWのみにとって有用であってよい。接続IDは、P-GWの一時記憶域(たとえば、キャッシュ428、図4)内に記憶され得る。接続IDは、アプリケーションサーバとデバイスが所与の交換に関連してパケットを交換している時間の間にのみ有用であり得るので、キャッシュは、適切な記憶場所であり得る。いったんアプリケーションサーバとデバイスとの間のサービスが終了されると、または所定の時間の量もしくは何らかの他のトリガイベントの後、接続IDは、P-GW内の記憶域から除去されてよい(たとえば、上書きされてよい、またはP-GWのキャッシュから消去されてよい)。

【０１６３】

P-GWは、DLトークンを使用して、ユーザプレーンメッセージに関連するダウンリンクポリシーを含むダウンリンクトラフィックポリシーを施行し得る。施行は、たとえば、アプリケーションサーバからの所与のパケット内で受信されるDLトークンを検証し、DLトークンから取得された情報を使用してパケットを適切なデバイスに転送することによって実行され得る。適切なデバイスに転送されるパケットは、DLトークンを含んでもよいし、含まなくてもよい。P-GWは、接続IDを検証してもよい(以前に導出された場合)。

【０１６４】

ネットワークトークンは、ネットワークにおいてアプリケーションサーバとデバイスとの間のアプリケーションサービス伝送のバリデーションを行うおよびマッピングするセキュアな手段であり得る。そのような目的のためのネットワークトークンの使用は、アプリケーションサーバIDをパケットに追加することのみよりも優れたセキュリティを提供する。さらに、前述のように、ネットワークトークンは、バリデーションに使用されるセキュ

アなハッシュ、セキュアなハッシュがどのようにバリデーションに使用されるかを決定するために使用されるインデックス、および/またはパケットのバリデーションが行われた後にどのようにしてパケットを処理するかを決定するために使用されるポリシーのうちの1つまたは複数を備え得る。

【０１６５】

任意選択のステップとして、デバイスは、第2のアプリケーションサーバとの接続を確立または開始してよい。その後、デバイスは、任意選択で、第1のネットワークトークンと異なる第2のネットワークトークンを第2のアプリケーションサーバから取得してよい。第1のアプリケーションサーバおよび第2のアプリケーションサーバは、アプリケーションサービスまたは宛先IPアドレスに関連付けられてよい。追加または代替として、第1のアプリケーションサーバおよび第2のアプリケーションサーバは、第1のアプリケーションサービスおよび第2のアプリケーションサービスに関連付けられてよい。

【０１６６】

図15は、デバイス(たとえば、チップコンポーネント、クライアントデバイス)が、通信を開始し、通信に関連してネットワークトークンを利用する要求に応答し得る例示的な方法1500である。通信を開始する要求は、ネットワークトークンを利用する要求を含み得る。方法1500は、デバイスにおいて動作可能であってよい。方法1500は、アプリケーションサーバが、通信を開始する要求および/またはネットワークトークンを利用する要求を開始した場合に適用され得る。

【０１６７】

通信を開始する要求(たとえば、アプリケーションサービスを開始する要求)は、アプリケーションサーバから来ることがある。要求、たとえばアプリケーションサービス要求は、ネットワークトークンを利用する明示的要求を含み得る。あるいは、ネットワークトークンを利用する要求は暗黙的であり得る。要求は、要求を開始したアプリケーションサーバまたはアプリケーションサービスを識別するアプリケーション識別子(App ID)を含み得る。

【０１６８】

一態様では、デバイスは、アプリケーションサービスを開始する要求をアプリケーションサーバから受信し得る1502。デバイスは、ネットワークトークンを取得し得る1504。一態様では、ネットワークトークンは、ゲートウェイ(たとえば、P-GW)から取得され得る。デバイスは、(たとえば、IPアドレス、デバイスID、またはアプリケーション資格情報に基づいて)アプリケーションサービスを開始する要求を検証し得る1506。

【０１６９】

デバイスは、アプリケーションサービスを開始する要求に応答してネットワークトークンを埋め込む、または含めることによって、アプリケーションサーバにネットワークトークンを付与し得る1508。ネットワークトークンは、アプリケーションサービスを開始する要求への応答を含むパケットに埋め込まれてよい。一態様では、ネットワークトークンは、複数のパケット間で分散されてよく、これらのパケットは、たとえば、アプリケーションサービスを開始する要求への応答のうちのいくつかまたはすべてを含んでよい。

【０１７０】

次いで、デバイスは、埋め込まれたネットワークトークンを含む応答をアプリケーションサーバに送り得る1510。このようにして、アプリケーションサーバは、ネットワークトークンを備えてよく、ネットワークトークンは、ネットワークトークンのコピーを、アプリケーションサーバからデバイスにダウンリンク方向に送られている1つまたは複数のパケットへと埋め込むまたは含めることができる。いくつかの態様では、アプリケーションサーバは、ネットワークトークンのコピーを、アプリケーションサーバからデバイスにダウンリンク方向に送られているあらゆるパケットへと埋め込むまたは含め得る。

【０１７１】

いくつかの態様では、ネットワークトークンは、ダウンリンクネットワークトークンであってよい。ネットワークトークンは、デバイスにおいてゲートウェイデバイス(たとえ

ば、P-GW)から受信され得る。いくつかの態様では、DLトークンは、ゲートウェイデバイスから受信されたパケット内に埋め込まれてもよいし、これとともに含められてもよい。パケットは、ユーザプレーン内で送られてよい。

【０１７２】

ネットワークトークンは、アプリケーションサーバおよびデバイスにバインドされてもよいし、アプリケーションサーバ、アプリケーションサービス、およびデバイスにバインドされてもよい。一態様では、DLトークンは、ベアラまたはデータフローに関連付けられ得る。DLトークンは、ダウンリンクパケットの検証に、およびダウンリンクフロー内で受信されたダウンリンクパケットをベアラにマッピングするために使用され得る。

【０１７３】

通信を確立する要求をデバイスが開始するのかアプリケーションサーバが開始するに関係なく、要求は、トランスポート層要求であってもよいし、アプリケーション層要求であってもよい。初期要求内のパケットは、伝送制御プロトコル同期(TCP SYN)パケットであってよい。初期要求内のパケットがTCP SYNパケットである場合、第1のネットワークトークンは、TCP SYN肯定応答(ACK)パケット内でデバイスまたはアプリケーションサーバに運ばれてよい。

【０１７４】

ネットワークトークンを利用する要求は、明示的要求であってもよいし、暗黙的要求であってもよい。明示的要求は、ユーザプレーン内のアプリケーションサーバから(または、これに)送られる要求内に埋め込まれてよい。暗黙的要求は、たとえば、アプリケーションサーバからデバイスに(または、その逆に)初期メッセージを送ることによって認識されてよい。すなわち、システムは、新しい通信サービスが確立されるときはいつでもネットワークトークンを使用する必要性を認識するように準備され得る。さらなる例として、サービスを開始することは、第1のネットワークトークンの暗黙的要求を表すパケットを送ることを含んでよく、この暗黙的要求は、アプリケーションサーバに(またはデバイスに)向けられた第1のパケットの送信であると認識され得る。さらなる例として、サービスを開始することは、ネットワークトークンの暗黙的要求を表すパケットを送ることを含んでよく、この暗黙的要求は、ネットワークトークンを必要とするアプリケーションサーバの宛先アドレスまたは少なくとも宛先アドレスプレフィックスを含むパケットの送信であると認識され得る(たとえば、P-GWが、宛先アプリケーションサーバがネットワークトークンの使用を必要とすることを認識する場合)。さらなる例として、サービスを確立または開始することは、第1のネットワークトークンの暗黙的要求を表すパケットを送ることを含んでよく、暗黙的要求は、パケットとともに含まれるアプリケーション識別子(App ID)に基づいて認識され得る。いくつかの態様では、(たとえば、制御プレーン内の)新しい信号は、ユーザプレーンメッセージングを通して実施されるトークン要求の明示的使用および/または暗黙的使用を実施するために必要とされない場合がある。

【０１７５】

一態様では、ネットワークトークンは、ユーザプレーンシム層ヘッダ内で受信され得る。ユーザプレーンシム層は、ユーザプレーンプロトコルスタック内のインターネットプロトコル(IP)層の上に配置され得る。あるいは、ユーザプレーンシム層は、ユーザプレーンプロトコルスタック内のインターネットプロトコル(IP)層の下に配置されてよい。

【０１７６】

一態様では、ネットワークトークンは、IPバージョン4(IPv4)ヘッダまたはIPバージョン6(IPv6)ヘッダなどのIPヘッダ内に埋め込まれてよい。IPv4におけるIPヘッダは、IP Optionsフィールドであってよい。IPv6におけるIPヘッダは、IP拡張ヘッダであってよい。

【０１７７】

一態様では、ネットワークトークンは、伝送制御プロトコル(TCP)ヘッダ内に埋め込まれてよい。ネットワークトークンは、TCPヘッダのOptionsフィールド内に埋め込まれてよい。

【０１７８】

一態様では、ネットワークトークンは、トランスポート層セキュリティ(TLS)レコードヘッダ内に埋め込まれてよい。

【０１７９】

一態様では、ネットワークトークンは、IPヘッダと伝送制御プロトコル/ユーザデータグラムプロトコル(TCP/UDP)ヘッダとの間でシムヘッダ内に埋め込まれてよい。

【０１８０】

さらに別の態様では、ネットワークトークンは、ハイパーテキスト転送プロトコル(HTTP)ヘッダ内に埋め込まれてよい。HTTPヘッダは、HTTP eXperimentalまたはeXtensionヘッダであってよい。

【０１８１】

例示的なゲートウェイデバイス

図16は、本明細書において説明される態様によるネットワークトークンを使用するネットワークポリシー施行および/またはパケットステアリングをサポートするように構成された例示的なゲートウェイデバイス1600を示すブロック図である。一例では、例示的なゲートウェイデバイス1600は、ワイヤレスネットワーク上で通信するためのネットワーク通信インターフェース回路1602と、ネットワーク通信インターフェース回路1602に結合された処理回路1604と、処理回路1604に結合されたメモリデバイス1606(たとえば、データを記憶するための磁気および/または光学デバイス)とを含んでよい。このリストは非限定的である。

【０１８２】

ワイヤレスネットワーク上で通信するためのネットワーク通信インターフェース回路1602は、サービングゲートウェイとの通信のための第1の入力/出力回路/関数/モジュール1608と、パケットデータネットワークとの通信のための第2の入力/出力回路/関数/モジュール1610とを含んでよい。第1の入力/出力回路/関数/モジュール1608は、複数のベアラ上で確立された複数のIPフローを取り扱ってよい。第2の入力/出力回路/関数/モジュール1610は、パケットデータネットワーク上の複数のサーバとの複数のIPフローを取り扱ってよい。このリストは非限定的である。

【０１８３】

処理回路1604は、トークンベースアプリケーションアクセスをサポートするように構成された、1つまたは複数のプロセッサ、特定用途向けプロセッサ、ハードウェアおよび/またはソフトウェアモジュールなどを含んでもよいし、これらを実施してもよい。たとえば、ネットワークトークン生成/検証回路/関数/モジュール1612は、メモリデバイス1606内に記憶され得る秘密鍵に基づいてトークンを導出するように構成されてよい。ゲートウェイデバイスのみが秘密鍵を知り得る。別の例として、鍵導出回路/関数/モジュール1614は、たとえば、メモリデバイス1606内に記憶され得る秘密鍵および所与のアクセスノードの識別子に基づいて、アクセスノードに固有の秘密鍵を導出するように構成されてよい。さらに別の例として、判断および処理回路/関数/モジュール1616は、EPSベアラから受信された(または、より一般的に、デバイスから受信された)アップリンクパケットおよび/またはアプリケーションサーバから受信されたダウンリンクパケットがネットワークトークンを含むかどうかを判断するように構成されてよく、そうである場合、受信されたパケットを暗号バリデーションおよびトラフィックステアリング回路/関数/モジュール1618に渡すようにさらに構成されてよい。さらに別の例として、暗号バリデーション/検証モジュール/回路/関数1630は、たとえばデバイスまたはアプリケーションサーバから受信されたネットワークトークンのバリデーションを行う/これを検証するように構成されてよい。判断および処理回路/関数/モジュール1616は、ネットワークトークンを含まない、受信されたパケットをサービスデータフローフィルタバンク(図示せず)に渡すようにさらに構成されてよい。このリストは非限定的である。

【０１８４】

メモリデバイス1606は、ネットワークトークン導出/検証命令1620と、鍵導出命令1622と、判断および処理命令1624と、暗号バリデーションおよびトラフィックステアリング命

令1626と、共有および非共有の秘密鍵記憶および命令1632とを含むように構成されてよい。このリストは非限定的である。

【０１８５】

ネットワーク通信インターフェース回路1602と処理回路1604とメモリデバイス1606と例示的なゲートウェイデバイス1600の他の構成要素（図示せず）との間の通信は、通信バス1634を経由してよい。

【０１８６】

ゲートウェイデバイスにおいて動作可能な方法

図17は、本明細書において説明される態様による、ネットワークトークンの使用のためにユーザプレーンメッセージングを介してデバイスからの要求を検出し、ネットワークトークンを導出して、アプリケーションサーバを介して要求側デバイスにネットワークトークンを提供するためにゲートウェイデバイス(たとえば、P-GW)において動作可能である例示的な方法1700を示す。

【０１８７】

一態様によれば、ネットワーク内のゲートウェイデバイス(たとえば、P-GW)において動作可能である方法は、ゲートウェイデバイスにおいて、ユーザプレーン上でデータパケットを受信する1702ことを含んでよい。次いで、ゲートウェイデバイスは、ネットワークトークンが(たとえば、明示的または暗黙的に)要求されるかどうかを決定する1704ためのステップを実行してよい。ネットワークトークンが要求される場合、ゲートウェイデバイスは、ネットワークトークンを取得してよい1706。ネットワークトークンは、ネットワークによって維持されるデバイス加入プロファイルに基づいてよい。

【０１８８】

一態様によれば、ネットワークトークンは、ゲートウェイデバイスにおいてネットワークトークンをローカルに導出することによって取得されてよい。本明細書において説明される態様によれば、ネットワークトークンは、ゲートウェイデバイスに関連付けられたコアネットワークによって維持されるデバイス加入プロファイルに基づいて、ゲートウェイデバイスによって導出されてよい。デバイス加入プロファイルは、加入プロファイルリポジトリ(SPR)内に記憶され得る。ネットワークトークンは、デバイスに関してコアネットワークによって施行されるポリシーを反映し得る。言い換えると、ネットワークトークンは、アプリケーションサーバのポリシーを反映する必要はない。ネットワークトークンは、ネットワークに代わって、ネットワークのために、ゲートウェイデバイスによって導出および使用されてよい。

【０１８９】

いったんゲートウェイデバイスがネットワークトークンを取得すると、ゲートウェイデバイスは、データパケットとともにネットワークトークンを含める1708ために必要なステップを実行してよい。次いで、ゲートウェイデバイスは、データパケットおよびネットワークトークンを宛先に送り得る1710。

【０１９０】

いくつかの態様では、データパケットは、アプリケーションサーバに送られることになっており、ネットワークトークンはアップリンクネットワークトークンである。いくつかの態様では、データパケットは、アプリケーションサーバに送られることになっており、ネットワークトークンはダウンリンクネットワークトークンである。いくつかの態様では、データパケットは、デバイスに送られることになっており、ネットワークトークンはダウンリンクネットワークトークンである。いくつかの態様では、データパケットがデバイスに送られることになっており、ネットワークトークンがダウンリンクネットワークトークンであるとき、方法は、ダウンリンクネットワークトークンを含む第2のパケットをデバイスから受信し、第2のパケットおよびダウンリンクネットワークトークンをアプリケーションサーバに送ることをさらに含んでよい。この後者の態様では、アプリケーションサーバは、ダウンリンクネットワークトークンを要求した可能性がある。要求されたダウンリンクネットワークトークンは、ゲートウェイからデバイスに送られるであろう。ゲー

トウェイは、その後、ダウンリンクネットワークトークンを含むデータパケットをデバイスから受信するであろう。ゲートウェイは、ダウンリンクネットワークトークンのそのコピーを、当初ダウンリンクネットワークトークンを要求したアプリケーションサーバに送るであろう。さらに他の態様では、ネットワークトークンはアップリンクネットワークトークンおよびダウンリンクネットワークトークンであってよく、アップリンクネットワークトークンは、ダウンリンクネットワークトークンとは異なる。そのような一態様では、ゲートウェイデバイスは、アップリンクネットワークトークンとダウンリンクネットワークトークンの両方を導出し、両方を宛先に送り得る。

【０１９１】

上述のように、ゲートウェイデバイスは、パケットデータネットワーク(PDN)ゲートウェイ(P-GW)であってよい。

【０１９２】

ネットワークトークンが要求されるかどうかを決定するステップは、パケットがネットワークトークンの明示的要求を含むか、またはパケットがネットワークトークンの暗黙的要求を表す(たとえば、これを代表する)のかに依存してよい。いくつかの態様によれば、ネットワークトークンが要求されるかどうかを決定することは、パケットが送られることになるアプリケーションサーバがネットワークトークンを必要とするかどうかを決定することに基づく。パケットが送られることになるアプリケーションサーバがネットワークトークンを必要とする場合、ゲートウェイデバイスは、ネットワークトークンを取得し得る。ネットワークトークンの必要性を決定するための暗黙的標識の他の試験も許容可能である。

【０１９３】

ネットワークトークンが要求される場合、ゲートウェイデバイスは、ネットワークトークンを取得してよい。一態様によれば、ネットワークトークンを取得することは、ゲートウェイデバイスにおいてネットワークトークンを導出することによって達成される。ネットワークトークンは、ゲートウェイデバイスに知られている秘密鍵、クラスインデックス、発信元インターネットプロトコル(IP)アドレス、発信元ポート番号、宛先IPアドレス、宛先ポート番号、プロトコル識別子(ID)、アプリケーションID、優先順位、および/またはサービス品質クラス識別子(QCI)を含む入力パラメータのセットを有する関数を使用して導出され得る。クラスインデックスは、ネットワークトークン導出のために使用されるフィールドを定義し得る。

【０１９４】

上記で提供され、便宜上以下で再生される一例によれば、ネットワークトークンは、次のように導出され得る。

ネットワークトークン=CI | HMAC(K_{P-GW}, CI | IP_C | IP_S | P_C | P_S | Proto | App ID | …)

上式で、CIはトークン導出に使用されるフィールドを定義するクラスインデックス、HMACは鍵付きハッシュメッセージ認証コード、K_{P-GW}はP-GWの秘密鍵、IP_Cはクライアント(たとえば、デバイス)IPアドレス、P_Cはクライアントポート番号、IP_Sはサーバ(たとえば、宛先またはアプリケーションサーバ)IPアドレス、P_Sはサーバポート番号、Protoはプロトコル番号または識別子、アプリIDはアプリケーション識別子である。追加パラメータまたは代替パラメータとしては、優先順位および/またはサービス品質クラス識別子(QCI)があり得る。

【０１９５】

上記の例に示されるように、ネットワークトークンは、クラスインデックスおよび例示の関数の出力の連結であってよい。いくつかの態様によれば、関数は、ハッシュメッセージ認証コード(HMAC)関数であってよい。いくつかの態様によれば、関数は、メッセージ認証コード(MAC)導出関数であってよい。MAC導出関数としては、暗号ブロック連鎖メッセージ認証コード(CBC-MAC)関数、暗号ベースMAC(CMAC)関数、またはガロアメッセージ認証コード(GMAC)関数がある。ネットワークトークンの導出のための他の式も許容可能であって

よい。

【０１９６】

図18は、本明細書において説明される態様によるユーザプレーンメッセージングを介してゲートウェイデバイス(たとえば、P-GW)におけるネットワークトークンをセットアップおよび使用する、ゲートウェイデバイス(たとえば、P-GW)において動作可能である例示的な方法1800である。

【０１９７】

一態様では、ネットワークトークンをセットアップする方法は、ゲートウェイデバイスにおいて、ネットワークサービスの要求(たとえば、第1のパケット)を受信する1802ことを含んでよい。ネットワークサービスの要求は、ネットワークトークンの要求を明示的に含んでもよいし、これを暗黙的に表してもよい。ネットワークサービスの要求は、(たとえば、アップリンクデータフロー内の)クライアントデバイスから受信されてもよいし、(たとえば、ダウンリンクデータフロー内の)アプリケーションサーバから受信されてもよい。ゲートウェイデバイスは、ネットワークトークンの要求に応答して、要求に対して適切に、アップリンクネットワークトークン、ダウンリンクネットワークトークン、またはアップリンクネットワークトークンとダウンリンクネットワークトークンの両方を導出し得る1804。

【０１９８】

任意選択で、ゲートウェイデバイスは、ネットワークトークンに関連付けられた接続を開始したクライアントデバイスまたはアプリケーションサーバを識別し得る接続識別子も導出し得る1806。導出される場合、接続識別子は、任意選択で、ゲートウェイデバイスにおいて記憶され得る1808。たとえば、記憶域は、ゲートウェイデバイスのキャッシュ内にあってよい。

【０１９９】

ゲートウェイデバイスは、デバイスまたはアプリケーションサーバのいずれかに送られることになるパケット内にネットワークトークンを埋め込み得る、またはこれを含み得る1810。一態様では、パケットは、アプリケーションサービスの要求に関連付けられ得る。ゲートウェイデバイスは、埋め込まれた/含まれるネットワークトークンを含むアプリケーションサービスの要求を、デバイスまたはアプリケーションサーバのいずれかに送り得る1812。

【０２００】

その後、ゲートウェイデバイスは、以前に導出されたネットワークトークン(または以前に導出されたネットワークトークンのコピー)を含むパケットを受信し得る1814。アプリケーションサービスの要求(たとえば、サービス開始要求)の非限定的な例を続けると、受信されたパケットは、サービス開始応答に関連付けられ得る。ゲートウェイデバイスは、ネットワークトークンのバリデーションを行う1816ことによって、受信されたパケットのバリデーションを行い得る。任意選択で、以前に導出された場合、ゲートウェイデバイスは、接続IDのバリデーションを行い得る1818。ゲートウェイデバイスは、ネットワークトークンのバリデーションを行わない場合、開始応答をその宛先に送り得る1820。いくつかの態様では、ゲートウェイデバイスは、開始応答とともにネットワークトークンを含んでよい。他の態様では、ゲートウェイデバイスは、ネットワークトークンを破棄してよく、したがって、ネットワークトークンは、その宛先に開始応答が送られるときに初期応答とともに含まれない。

【０２０１】

いくつかの態様では、ネットワークトークンは、デバイス(たとえば、チップコンポーネント、クライアントデバイス)およびアプリケーションサーバにバインドされてもよいし、デバイス、App ID、およびアプリケーションサーバにバインドされなくてもよい。

【０２０２】

図19は、本明細書において説明される態様による、ネットワークポリシーの施行および/またはパケットのステアリングのためのネットワークトークンの使用に関連する、ネッ

トワークトークンを検証するための、ゲートウェイデバイス(たとえば、P-GW)において動作可能である例示的な方法1900である。いくつかの態様によれば、特定の特徴は、ゲートウェイデバイスが、ポリシー施行および/またはパケットステアリングのためにデータパケットとともに含まれるネットワークトークンを使用することが可能であり得ることを示し得る。一例では、フラグが、パケットがポリシー施行および/またはパケットステアリングのためのネットワークトークンを含むことを示すように設定され得る。

【０２０３】

一態様によれば、方法は、ゲートウェイデバイスにおいて、第1のネットワークトークンの要求に応答して、第1のネットワークトークンを導出すること1902を含み得る。第1のネットワークトークンの要求は、デバイスから、1つまたは複数のアプリケーションサービスに関連付けられたアプリケーションサーバに送られ得る。ゲートウェイデバイスにおいて、デバイスからデータパケットを受信する1904こと。データパケットは、少なくとも、アプリケーションサーバに対応する宛先アドレスプレフィックスを含み得る。データパケットは、第2のネットワークトークンを含み得る。

【０２０４】

方法は、第2のネットワークトークンを検証する1906ことによって続行し得る。一態様によれば、第2のネットワークトークンを検証すること1906は、パケットから取得された入力パラメータおよびゲートウェイデバイスに知られている鍵を使用して、第1の関数から第1のネットワークトークンの複製を導出することを含み得る。第1のネットワークトークンは、以前に導出され、デバイスへのその後の配信のためにアプリケーションサーバに送られる。いったんデバイスが第1のネットワークトークンを受信すると、第1のネットワークトークンは、同じアプリケーションサーバに送られるアップリンクパケットとともに第1のネットワークトークンのコピーを含む。現在検討中の受信されたアップリンクパケットを含む第2のネットワークトークンは、第1のネットワークトークンのコピーであるべきである。両方のネットワークトークンが、同じ関数、ゲートウェイデバイスに知られている同じ秘密鍵、および同じデバイスからゲートウェイデバイスに送られた異なるパケットから出された同じ共通パラメータを使用して導出された場合、第2のネットワークトークンは、第1のネットワークトークンの複製と同一である。

【０２０５】

任意選択で、接続識別子が導出され、元のネットワークトークンの導出に関連してゲートウェイデバイスにおいて記憶された場合、ゲートウェイデバイスにおける回路/モジュール/関数は、接続識別子を検証し得る1908。

【０２０６】

決定1910は、(たとえば、第2のネットワークトークンおよび任意選択で接続識別子の)検証が成功かどうかに関してなされてよい。検証が成功でない場合、方法は、パケットおよびその関連付けられた第2のネットワークトークンを破棄する1912ことによって続行し得る。検証が成功である場合、方法は、任意選択で第2のネットワークトークンを破棄し1914、アプリケーションサーバにパケットを送る1916ことによって続行し得る。

【０２０７】

例示的なアプリケーションサーバ

図20は、ダウンリンクトークンバリデーションおよびパケットマッピングをサポートするように構成された例示的なアプリケーションサーバ2000を示すブロック図である。一例では、アプリケーションサーバ2000は、ワイヤレスネットワーク上で通信するためのネットワーク通信インターフェース回路2002と、ネットワーク通信インターフェース回路2002に結合された処理回路2004と、処理回路2004に結合されたメモリデバイス2006とを含んでよい。このリストは非限定的である。

【０２０８】

ワイヤレスネットワーク上で通信するためのネットワーク通信インターフェース回路2002は、S-GWを介したP-GWとの通信のための第1の入力/出力モジュール/回路/関数2008を含んでよい。ネットワーク通信インターフェース回路2002は、デバイスとのワイヤレス通信

のための受信機/送信機モジュール/回路/関数2010を含んでよい。このリストは非限定的である。

【０２０９】

処理回路2004は、トークンベースアプリケーションアクセスをサポートするように構成された、1つまたは複数のプロセッサ、特定用途向けプロセッサ、ハードウェアおよび/またはソフトウェアモジュールなどを含んでもよいし、これらを実施してもよい。たとえば、ネットワークトークンハンドリングモジュール/回路/関数2012は、メモリデバイス2006内に記憶され得る非共有秘密鍵または共有秘密鍵に基づいて、トークンを導出するように構成されてよい。別の例として、ネットワークトークン抽出/埋込みモジュール/回路/関数2014は、デバイスからのアップリンクパケットからネットワークトークンを抽出する、および/またはゲートウェイデバイスに転送されたパケット内にネットワークトークンを埋め込む(これを含める)ように構成されてよい。さらに別の例として、暗号バリデーション/検証モジュール/回路/関数2016は、たとえば、デバイスから受信されたネットワークトークンのバリデーションを行う/検証するように構成されてよい。このリストは非限定的である。

【０２１０】

メモリデバイス2006は、ネットワークトークンハンドリング命令2020と、ネットワークトークン抽出/埋込み命令2022と、暗号バリデーション/検証命令2024と、共有および非共有の秘密鍵記憶および命令2026とを含むように構成されてよい。このリストは非限定的である。

【０２１１】

ネットワーク通信インターフェース回路2002と処理回路2004とメモリデバイス2006とアプリケーションサーバ2000の他の構成要素(図示せず)との間の通信は、通信バス2034を経由してよい。

【０２１２】

アプリケーションサーバにおいて動作可能である方法

図21は、本明細書において説明される態様によるアプリケーションサーバにおいてネットワークトークンをセットアップする例示的な方法2100のフローチャートである。

【０２１３】

一態様によれば、決定2102は、アプリケーションサーバが、デバイス(たとえば、チップコンポーネント、クライアントデバイス)にアプリケーションサービスを提供する要求を開始するかどうかに関してなされてよい。アプリケーションサーバが要求を開始する場合、アプリケーションサーバは、ネットワークトークン(たとえば、DLネットワークトークン)の利用の要求を明示的に含むまたはこれを暗黙的に表す、ユーザプレーン内で送信されるパケットを含む要求を送り得る2104。次いで、アプリケーションサーバは、ネットワークトークンを取得することを待機し得る2106。2102に戻ると、アプリケーションサーバが要求を開始しないことが決定される場合、アプリケーションサーバは、たとえば、デバイス(たとえば、チップコンポーネント、クライアントデバイス)から送られるネットワークトークンの使用の明示的要求または暗黙的要求に基づいて、送られたネットワークトークンを取得することを待機し得る2106。

【０２１４】

アプリケーションサーバは、次に、ネットワークトークンを取得し得る2108。本明細書において説明される態様によれば、コアネットワークに関連付けられたゲートウェイデバイスは、コアネットワークによって維持されるデバイス加入プロファイルに基づいてネットワークトークンを導出した可能性がある。デバイス加入プロファイルは、加入プロファイルリポジトリ(SPR)内に記憶され得る。SPRは、PCRFに構成され得る。ネットワークトークンは、デバイスに関してコアネットワークによって施行されるポリシーを反映し得る。言い換えると、ネットワークトークンは、アプリケーションサーバのポリシーを反映する必要はない。ネットワークトークンは、ネットワークに代わって、ネットワークのために、ゲートウェイデバイスによって導出および使用されてよい。

【０２１５】
ネットワークトークンを取得する(たとえば、これを受信する)と、たとえば、ネットワークトークンが、デバイスとの接続に関連するDLネットワークトークンである場合、アプリケーションサーバは、デバイスに送られる少なくともいくつかのパケット内にDLネットワークトークンのコピーを埋め込む、またはこれを含んでよい。いくつかの態様では、アプリケーションサーバは、DLネットワークトークンのコピーを、デバイスに送られるあらゆるパケット内に埋め込むまたは含め得る。
【０２１６】
いくつかの態様では、アプリケーションサーバからデバイスに送られるパケットとともにDLトークンを送ることは、インターネットプロトコルIPバージョン4(IPv4)ヘッダまたはIPバージョン6(IPv6)ヘッダであって、IPv4ヘッダ内のトークンはIP Optionsフィールド内にあってよく、IPv6ヘッダ内のトークンはIP拡張ヘッダ、伝送制御プロトコル(TCP)ヘッダ、セキュアソケット層(SSL)ヘッダ、トランスポート層セキュリティ(TLS)レコードヘッダ、インターネットプロトコル(IP)ヘッダと伝送制御プロトコル/ユーザデータグラムプロトコル(TCP/UDP)ヘッダとの間のシムヘッダ、および/またはハイパーテキスト転送プロトコル(HTTP)ヘッダ内にあってよい、DLトークンを含めることを含んでよい。
【０２１７】
DLトークンがアプリケーションサーバによって要求された一態様では、DLトークンは、デバイスから送られる応答を含むパケットから取得され得る。別の態様では、DLトークンは、デバイスから送られるアプリケーションサービスを開始する要求から取得され得る。
【０２１８】
図示および説明される特定の実装形態は例にすぎず、本明細書において別段に規定されていない限り、本開示を実施する唯一の手段と解釈されるべきではない。本開示における様々な例は、数多くの他の区分解決策(partitioning solution)によって実施され得ることは、当業者には容易に明らかである。
【０２１９】
本明細書において説明され図面に示される構成要素、行為、特徴、および/または機能のうちの1つまたは複数は、単一の構成要素、行為、特徴、または機能に再編成および/または組み合わされてもよいし、いくつかの構成要素、行為、特徴、または機能において実施されてもよい。追加の要素、構成要素、行為、および/または機能も、本発明から逸脱することなく追加されてよい。本明細書において説明されるアルゴリズムも、効率的にソフトウェア内で実施されてよく、および/またはハードウェア内に埋め込まれてもよい。
【０２２０】
説明では、要素、回路、関数、およびモジュールが、不必要に詳細に本開示を曖昧にしないようにブロック図形式において図示され得る。逆に、図示および説明される特定の実装形態は例示的にすぎず、本明細書において別段に規定されていない限り、本開示を実施する唯一の手段と解釈されるべきではない。さらに、ブロック定義および様々なブロック間の論理の区分は、特定の実装形態の例である。本開示が数多くの他の区分解決策によって実施され得ることは、当業者には容易に明らかである。ほとんどの場合、タイミングの検討などに関する詳細は、そのような詳細が本開示の完全な理解を得るために必要ではなく、関連技術の当業者の能力の範囲内である場合、省略されている。
【０２２１】
さらに、実施形態は、フローチャート、流れ図、構造図、またはブロック図と示されるプロセスとして説明され得ることに留意されたい。フローチャートは、動作について連続的プロセスとして説明することがあるが、動作の多くは、並列にまたは同時に実行されてよい。さらに、動作の順序は、再編成されてよい。プロセスは、その動作が完了されると終了される。プロセスは、方法、関数、プロシージャ、サブルーチン、サブプログラムなどに対応し得る。プロセスが関数に対応するとき、その終了は、呼び出し側関数またはメイン関数への関数の復帰に対応する。
【０２２２】

情報および信号は、様々な異なる技術および技法のうちのいずれかを使用して表されてよいことが、当業者には理解されよう。たとえば、本明細書全体を通して言及され得るデータ、命令、コマンド、情報、信号、ビット、シンボル、およびチップは、電圧、電流、電磁波、磁場もしくは磁性粒子、光学場もしくは光学粒子、またはそれらの任意の組合せによって表されてよい。いくつかの図面は、提示および説明を明快にするために、信号を単一の信号として示し得る。信号は信号のバスを表してよく、バスは、様々なビット幅を有してよく、本開示は、単一のデータ信号を含む任意の数のデータ信号上で実施されてよいことが、当業者によって理解されよう。

【０２２３】

「第1の」、「第2の」などの指定を使用する、本明細書における要素への任意の言及は、そのような制限が明示的に述べられない限り、それらの要素の量または順序を制限しないことを理解されたい。むしろ、これらの指定は、本明細書において、2つ以上の要素または要素のインスタンスを区別する簡便な方法として使用されてよい。したがって、第1の要素および第2の要素の言及は、2つの要素のみがそこで用いられ得ること、または第1の要素が何らかの様式で第2の要素に先行しなければならないことを意味しない。さらに、別段に述べられない限り、要素のセットは、1つまたは複数の要素を含んでよい。

【０２２４】

その上、記憶媒体は、読出し専用メモリ(ROM)、ランダムアクセスメモリ(RAM)、磁気ディスク記憶媒体、光学記憶媒体、フラッシュメモリデバイス、ならびに/または情報を記憶するための他の機械可読媒体、およびプロセッサ可読媒体、および/もしくはコンピュータ可読媒体を含むデータを記憶するための1つまたは複数のデバイスを表し得る。「機械可読媒体」、「コンピュータ可読媒体」、および/または「プロセッサ可読媒体」という用語は、限定するものではないが、命令および/またはデータを記憶する、含む、または運ぶことが可能なポータブル記憶デバイスもしくは固定記憶デバイス、光学式記憶デバイス、および様々な他の媒体などの非一時的な媒体を含んでよい。したがって、本明細書において説明される様々な方法は、「機械可読媒体」、「コンピュータ可読媒体」、および/または「プロセッサ可読媒体」内に記憶され得る命令および/またはデータによって完全にまたは部分的に実施され、1つまたは複数のプロセッサ、機械、および/またはデバイスによって実行されてよい。

【０２２５】

その上、実施形態は、ハードウェア、ソフトウェア、ファームウェア、ミドルウェア、マイクロコード、またはそれらの任意の組合せによって実施されてよい。ソフトウェア、ファームウェア、ミドルウェア、またはマイクロコード内で実施されるとき、必要なタスクを実行するためのプログラムコードまたはコードセグメントは、記憶媒体または他の記憶域などの機械可読媒体内に記憶されてよい。プロセッサは、必要なタスクを実行してよい。コードセグメントは、プロシージャ、関数、サブプログラム、プログラム、ルーチン、サブルーチン、モジュール、ソフトウェアパッケージ、クラス、または命令、データ構造、もしくはプログラム命令文の任意の組合せを表してよい。コードセグメントは、情報、データ、引数、パラメータ、またはメモリ内容を渡すことによって、別のコードセグメントまたはハードウェア回路に結合されてよい。情報、引数、パラメータ、データなどは、メモリ共有、メッセージ受渡し、トークン受渡し、ネットワーク伝送、トラフィックなどを含む任意の適切な手段を介して渡され、転送され、または送信されてよい。

【０２２６】

本明細書で開示される例に関連して説明される様々な例示的な論理ブロック、要素、回路、モジュール、関数、および/または構成要素は、本明細書において説明される機能を実行するように設計された、汎用プロセッサ、デジタル信号プロセッサ(DSP)、特定用途向け集積回路(ASIC)、フィールドプログラマブルゲートアレイ(FPGA)もしくは他のプログラマブルロジックコンポーネント、ディスクリートゲートもしくはトランジスタ論理、ディスクリートハードウェア構成要素、またはそれらの任意の組合せを用いて実施または実行されてよい。汎用プロセッサはマイクロプロセッサであってよいが、代替形態では、プ

ロセッサは、任意の従来のプロセッサ、コントローラ、マイクロコントローラ、または状態機械であってよい。プロセッサは、コンピューティング構成要素の組合せ、たとえば、DSPとマイクロプロセッサの組合せ、いくつかのマイクロプロセッサ、DSPコアと関連する1つもしくは複数のマイクロプロセッサ、または任意の他のそのような構成として実施されてもよい。本明細書において説明される実施形態を実行するために構成された汎用プロセッサは、そのような実施形態を実行するための特殊目的プロセッサと見なされる。同様に、汎用コンピュータは、本明細書において説明される実施形態を実行するように構成されるとき、特殊目的コンピュータと見なされる。

【０２２７】

本明細書で開示される例に関連して説明される方法またはアルゴリズムは、ハードウェア内で、プロセッサによって実行可能なソフトウェアモジュール内で、または処理ユニット、プログラミング命令、または他の指示の形で両方の組合せにおいて直接実施されてよく、単一のデバイス内に含まれてもよいし、複数のデバイスにわたって分散されてもよい。ソフトウェアモジュールは、RAMメモリ、フラッシュメモリ、ROMメモリ、EPROMメモリ、EEPROMメモリ、レジスタ、ハードディスク、リムーバブルディスク、CD-ROM、または当技術分野で知られている任意の他の形式の記憶媒体内に常駐してよい。記憶媒体は、プロセッサが記憶媒体から情報を読み取り、記憶媒体に情報を書き込むことができるように、プロセッサに結合されてよい。代替形態では、記憶媒体は、プロセッサと一体化されてよい。

【０２２８】

当業者は、本明細書で開示される実施形態に関連して説明される様々な例示的な論理ブロック、回路、関数、モジュール、およびアルゴリズムステップは、電子ハードウェア、コンピュータソフトウェア、または両方の組合せとして実施されてよいことをさらに認識するであろう。ハードウェアおよびソフトウェアのこの互換性を明確に示すために、様々な例示的な要素、構成要素、ブロック、回路、関数、モジュール、およびステップについて、それらの機能に関して一般的に上記で説明してきた。そのような機能がハードウェアとして実施されるか、ソフトウェアとして実施されるか、それらの組合せとして実施されるかは、特定の適用例およびシステム全体に課される設計選択に依存する。

【０２２９】

本明細書において説明される本発明の様々な特徴は、本発明から逸脱することなく異なるシステムにおいて実施されてよい。前述の実施形態は例にすぎず、本発明を限定すると解釈されるべきではないことに留意されたい。実施形態の説明は例示的であり、特許請求の範囲を制限しないことを意図したものである。したがって、本教示は、他のタイプの装置に容易に適用可能であり、多くの代替形態、修正形態、および変形形態が当業者に明らかであろう。

【符号の説明】

【０２３０】

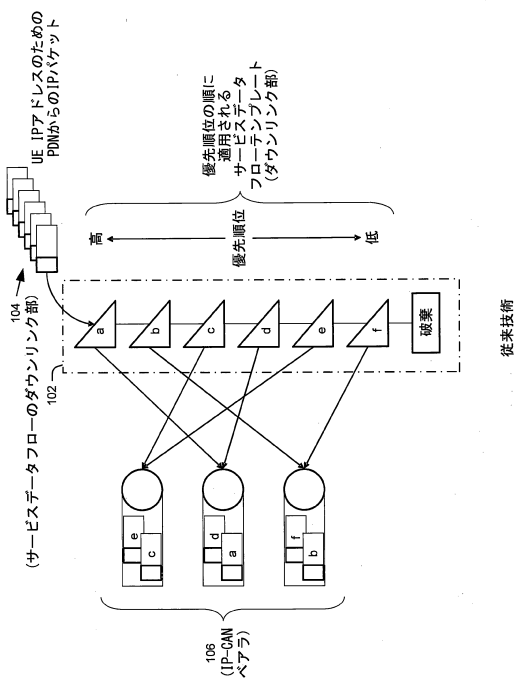
102　SDFテンプレート
104　サービスデータフロー
106　ベアラ
124　サーバ
126　サーバ
128　サーバ
130　サーバ
200　動作環境
202　クライアントデバイス
204　クライアントデバイス
206　アクセスノード
224　サーバ
226　サーバ

228 サーバ
230 サーバ
300 アップリンク動作
302 デバイス
304 アクセスノード
312 アプリケーションサービス
314 IPフロー
318 ベアラ
320 モジュール
322 モジュール
324 SDFテンプレート
400 ダウンリンク動作
402 デバイス
404 アクセスノード
414 ダウンリンクIPフロー
418 ベアラ
420 デバイス
422 デバイス
424 SDFテンプレート
424a テーブル
428 キャッシュ
500 コールフロー
502 デバイス
504 アクセスノード
516 アプリケーションサーバ
600 コールフロー
602 デバイス
604 アクセスノード
616 アプリケーションサーバ
700 コールフロー
702 デバイス
704 アクセスノード
716 アプリケーションサーバ
800 コールフロー
802 デバイス
804 アクセスノード
816 アプリケーションサーバ
900 ユーザプレーンプロトコルスタック
902 クライアントデバイス
904 アクセスノード
906 ゲートウェイデバイス
908 アプリケーションサーバ
910 PHY層
912 MAC層
914 RLC層
916 PDCP層
918 IP層
920 シム層
922 シム層
924 IP層

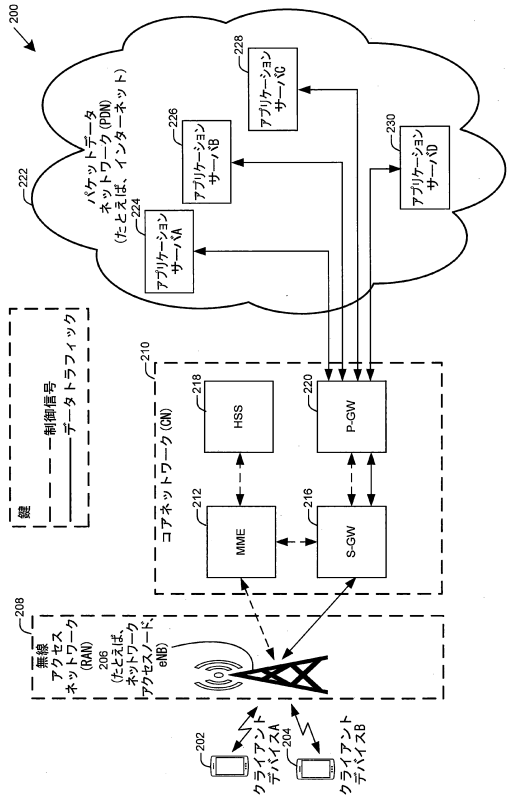
930 PHY層
932 MAC層
934 RLC層
936 PDCP層
958 IP層
960 ネットワークトークン
1000 ユーザプレーンプロトコルスタック
1002 クライアントデバイス
1004 アクセスノード
1006 ゲートウェイデバイス
1008 アプリケーションサーバ
1016 PDCP層
1036 PDCP層
1048 GTP-U層
1060 ネットワークトークン
1100 ユーザプレーンプロトコルスタック
1102 クライアントデバイス
1104 アクセスノード
1106 ゲートウェイデバイス
1108 アプリケーションサーバ
1110 PHY層
1112 MAC層
1114 RLC層
1116 PDCP層
1118 IP層
1124 IP層
1158 IP層
1160 ダウンリンクネットワークトークン
1200 ユーザプレーンプロトコルスタック
1202 クライアントデバイス
1204 アクセスノード
1206 ゲートウェイデバイス
1208 アプリケーションサーバ
1210 PHY層
1212 MAC層
1214 RLC層
1216 PDCP層
1218 IP層
1220 シム層
1222 シム層
1223 シム層
1224 IP層
1258 IP層
1260 ダウンリンクネットワークトークン
1300 デバイス
1302 ネットワーク通信インターフェース回路
1304 処理回路
1306 メモリデバイス
1308 第1の入力/出力モジュール/回路/関数
1310 受信機/送信機モジュール/回路/関数

1312 ネットワークトークンハンドリングモジュール/回路/関数
1314 ネットワークトークン抽出/埋込みモジュール/回路関数
1316 暗号バリデーション/検証モジュール/回路/関数
1320 ネットワークトークンハンドリング命令
1322 ネットワークトークン抽出/埋込み命令
1324 暗号バリデーション/検証命令
1326 暗号バリデーション/検証命令
1334 通信バス
1600 ゲートウェイデバイス
1602 ネットワーク通信インターフェース回路
1604 処理回路
1606 メモリデバイス
1608 第1の入力/出力回路/関数/モジュール
1610 第2の入力/出力回路/関数/モジュール
1612 ネットワークトークン導出/検証回路/関数/モジュール
1614 鍵導出回路/関数/モジュール
1616 判断および処理回路/関数/モジュール
1618 暗号バリデーションおよびトラフィックステアリング回路/関数/モジュール
1620 ネットワークトークン導出/検証命令
1622 鍵導出命令
1624 判断および処理命令
1626 暗号バリデーションおよびトラフィックステアリング命令
1630 暗号バリデーション/検証モジュール/回路/関数
1634 通信バス
1910 決定
2000 アプリケーションサーバ
2002 ネットワーク通信インターフェース回路
2004 処理回路
2006 メモリデバイス
2008 第1の入力/出力モジュール/回路/関数
2010 受信機/送信機モジュール/回路/関数
2012 ネットワークトークンハンドリングモジュール/回路/関数
2014 ネットワークトークン抽出/埋込みモジュール/回路関数
2016 暗号バリデーション/検証メモリデバイス
2020 ネットワークトークンハンドリング命令
2022 ネットワークトークン抽出/埋込み命令
2024 暗号バリデーション/検証命令
2026 共有および非共有の秘密鍵記憶および命令
2034 通信バス
2102 決定

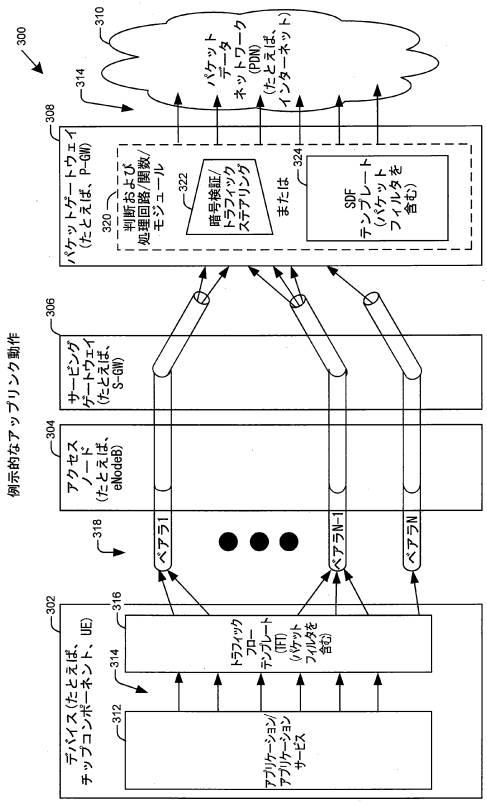
【図１】


UE IPアドレスのための
PDNからのIPパケット
優先順位の順に
適用される
サービスデータ
フローテンプレート
(ダウンリンク部)
高
優先順位
低
104
102
a
b
c
d
e
f
破棄
(サービスデータフローのダウンリンク部)
106
(IP-CAN
ベアラ)
従来技術

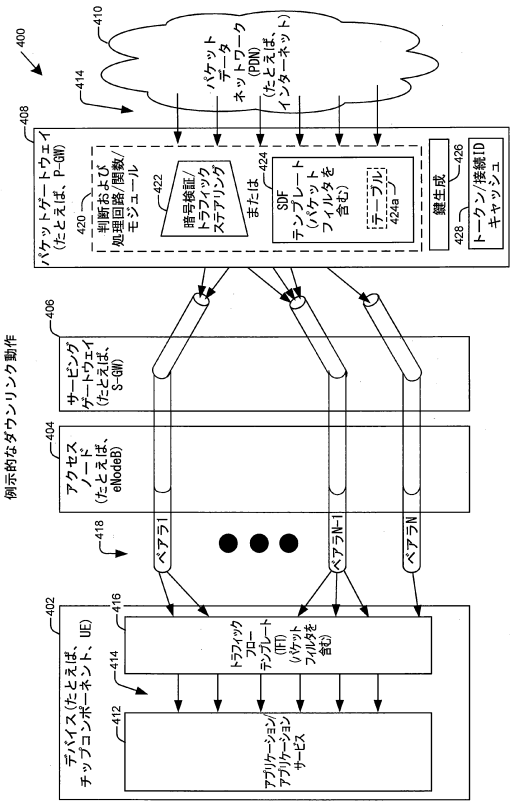
【図２】


200
パケットデータ
ネットワーク(PDN)
(たとえば、インターネット)
222
アプリケーション
サーバA
224
アプリケーション
サーバB
226
アプリケーション
サーバC
228
アプリケーション
サーバD
230
鍵
制御信号
データトラフィック
コアネットワーク(CN)
210
HSS
218
P-GW
220
MME
212
S-GW
216
無線
アクセス
ネットワーク
(RAN)
206
(たとえば、
ネットワーク
アクセスノード、
eNB)
208
クライアント
デバイスA
202
クライアント
デバイスB
204

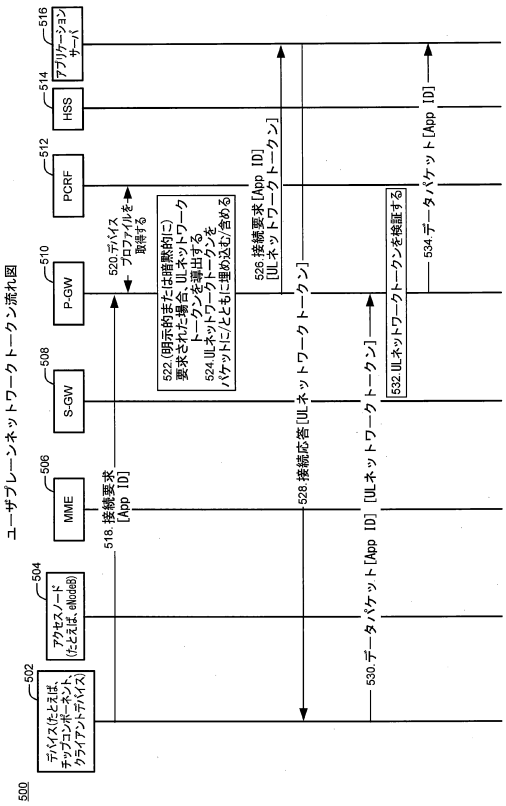
【図３】


例示的なアップリンク動作
300
パケット
データ
ネットワーク
(PDN)
(たとえば、
インターネット)
310
314
パケットゲートウェイ
(たとえば、P-GW)
308
判断および
処理回路/関数/
モジュール
320
暗号検証/
トラフィック
ステアリング
322
または
324
SDF
テンプレート
(パケット
フィルタを
含む)
サービング
ゲートウェイ
(たとえば、
S-GW)
306
アクセス
ノード
(たとえば、
eNodeB)
304
318
ベアラ1
ベアラN-1
ベアラN
デバイス(たとえば、
チップコンポーネント、UE)
302
316
トラフィック
フローテンプレート
(TFT)
(パケット
フィルタを
含む)
314
312
アプリケーション/
アプリケーション
サービス

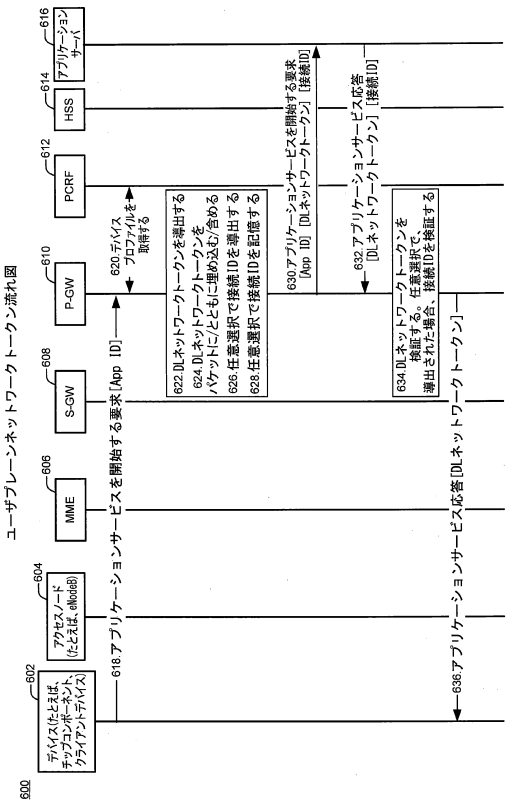
【図４】


例示的なダウンリンク動作
400
パケット
データ
ネットワーク
(PDN)
(たとえば、
インターネット)
410
414
パケットゲートウェイ
(たとえば、P-GW)
408
判断および
処理回路/関数/
モジュール
420
暗号検証/
トラフィック
ステアリング
422
または
424
SDF
テンプレート
(パケット
フィルタを
含む)
テーブル
424a
鍵生成
426
トークン/接続ID
キャッシュ
428
サービング
ゲートウェイ
(たとえば、
S-GW)
406
アクセス
ノード
(たとえば、
eNodeB)
404
418
ベアラ1
ベアラN-1
ベアラN
デバイス(たとえば、
チップコンポーネント、UE)
402
416
トラフィック
フローテンプレート
(TFT)
(パケット
フィルタを
含む)
414
412
アプリケーション/
アプリケーション
サービス

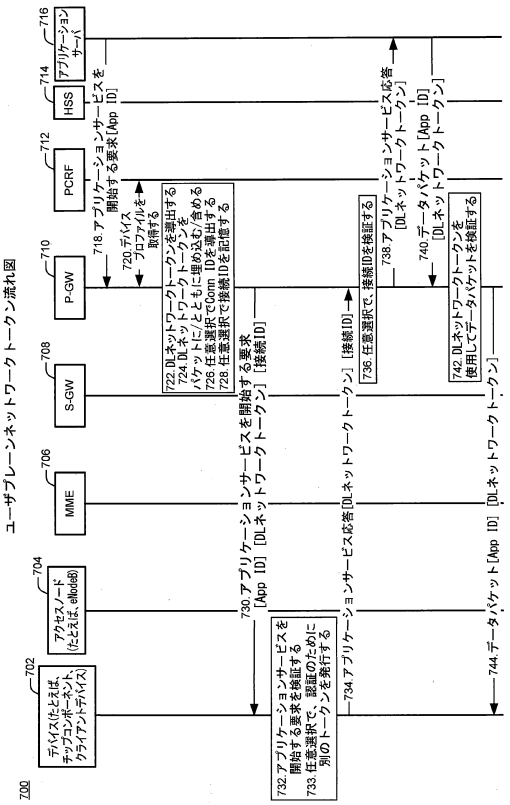
【図５】


ユーザプレーンネットワークトークン流れ図
500
502 デバイス(たとえば、チップコンポーネント、クライアントデバイス)
504 アクセスノード(たとえば、eNodeB)
506 MME
508 S-GW
510 P-GW
512 PCRF
514 HSS
516 アプリケーションサーバ
518. 接続要求 [App ID]
520.デバイスプロファイルを取得する
522.(明示的または暗黙的に)要求された場合、UEネットワークトークンを導出する
524.ULネットワークトークンをパケットにとともに埋め込む/含める
526.接続要求 [App ID] [ULネットワークトークン]
528.接続応答 [ULネットワークトークン]
530.データパケット [App ID] [ULネットワークトークン]
532.ULネットワークトークンを検証する
534.データパケット [App ID]

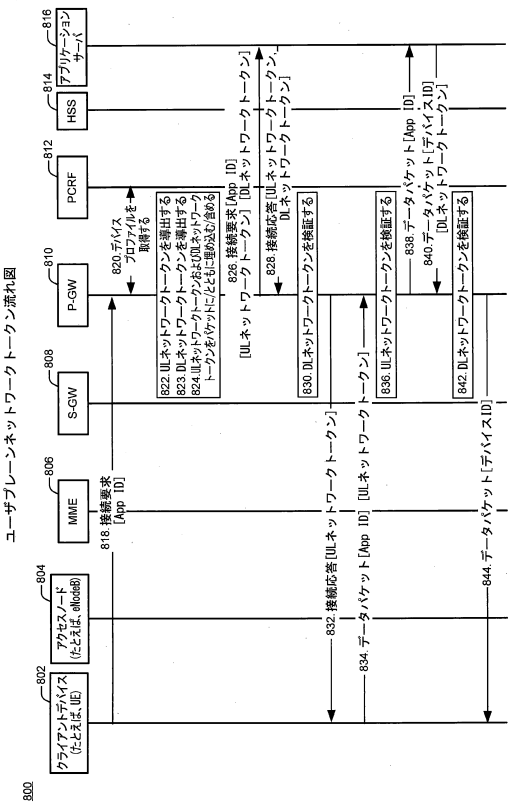
【図６】


ユーザプレーンネットワークトークン流れ図
600
602 デバイス(たとえば、チップコンポーネント、クライアントデバイス)
604 アクセスノード(たとえば、eNodeB)
606 MME
608 S-GW
610 P-GW
612 PCRF
614 HSS
616 アプリケーションサーバ
618.アプリケーションサービスを開始する要求 [App ID]
620.デバイスプロファイルを取得する
622.DLネットワークトークンを導出する
624.DLネットワークトークンをパケットにとともに埋め込む/含める
626.任意選択で接続IDを導出する
628.任意選択で接続IDを記憶する
630.アプリケーションサービスを開始する要求 [App ID] [DLネットワークトークン] [接続ID]
632.アプリケーションサービス応答 [DLネットワークトークン] [接続ID]
634.DLネットワークトークンを検証する。任意選択で、接続IDを検証する
636.アプリケーションサービス応答 [DLネットワークトークン]

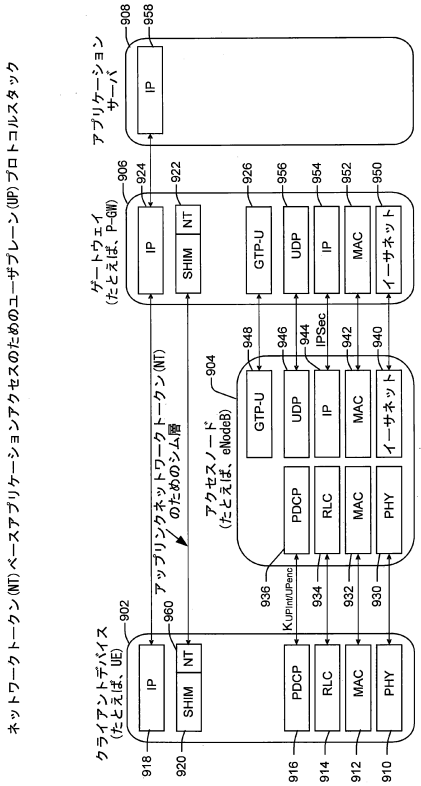
【図７】


ユーザプレーンネットワークトークン流れ図
700
702 デバイス(たとえば、チップコンポーネント、クライアントデバイス)
704 アクセスノード(たとえば、eNodeB)
706 MME
708 S-GW
710 P-GW
712 PCRF
714 HSS
716 アプリケーションサーバ
718.アプリケーションサービスを開始する要求 [App ID]
720.デバイスプロファイルを取得する
722.DLネットワークトークンを導出する
724.DLネットワークトークンをパケットにとともに埋め込む/含める
726.任意選択で(Conn ID)を導出する
728.任意選択で接続IDを記憶する
730.アプリケーションサービスを開始する要求 [App ID] [DLネットワークトークン] [接続ID]
732.アプリケーションサービスを開始する要求を検証する
733.任意選択で、認証のために別のトークンを発行する
734.アプリケーションサービス応答 [DLネットワークトークン] [接続ID]
736.任意選択で、接続IDを検証する
738.アプリケーションサービス応答 [DLネットワークトークン]
740.データパケット [App ID] [DLネットワークトークン]
742.DLネットワークトークンを使用してデータパケットを検証する
744.データパケット [App ID] [DLネットワークトークン]

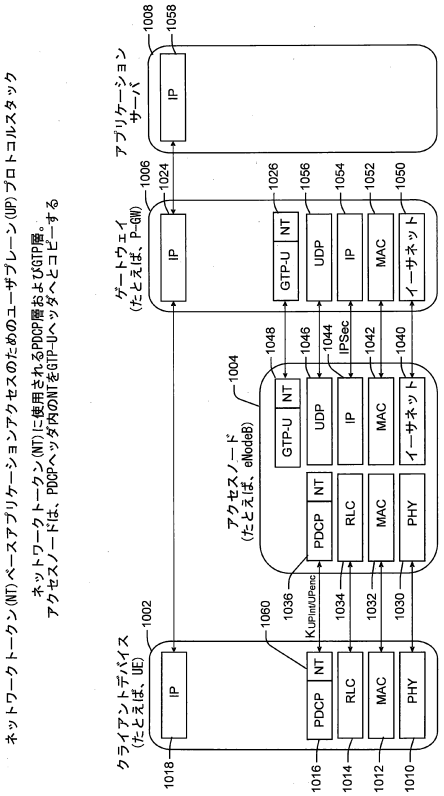
【図８】


ユーザプレーンネットワークトークン流れ図
800
802 クライアントデバイス(たとえば、UE)
804 アクセスノード(たとえば、eNodeB)
806 MME
808 S-GW
810 P-GW
812 PCRF
814 HSS
816 アプリケーションサーバ
818.接続要求 [App ID]
820.デバイスプロファイルを取得する
822.DLネットワークトークンを導出する
823.DLネットワークトークンおよびDLネットワークトークンをパケットにとともに埋め込む/含める
824.ULネットワークトークンをパケットにとともに埋め込む/含める
826.接続要求 [App ID] [DLネットワークトークン] [ULネットワークトークン]
828.接続応答 [ULネットワークトークン] DLネットワークトークン]
830.DLネットワークトークンを検証する
832.接続応答 [ULネットワークトークン]
834.データパケット [App ID] [ULネットワークトークン]
836.ULネットワークトークンを検証する
838.データパケット [App ID] [デバイスID] [DLネットワークトークン]
840.データパケット [デバイスID] [DLネットワークトークン]
842.DLネットワークトークンを検証する
844.データパケット [デバイスID]

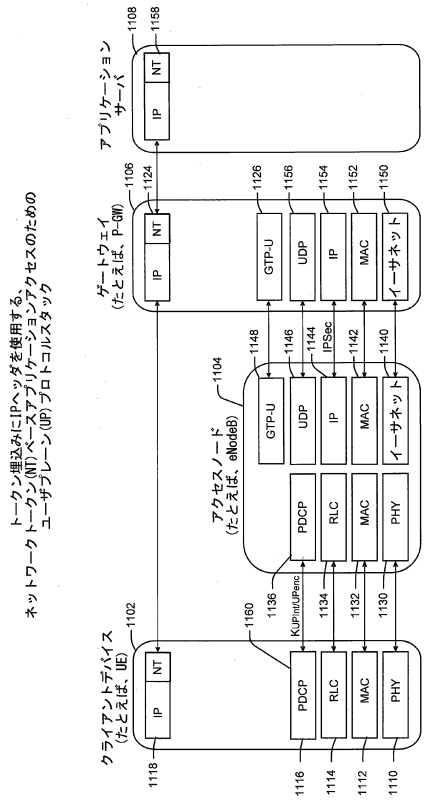
【図９】



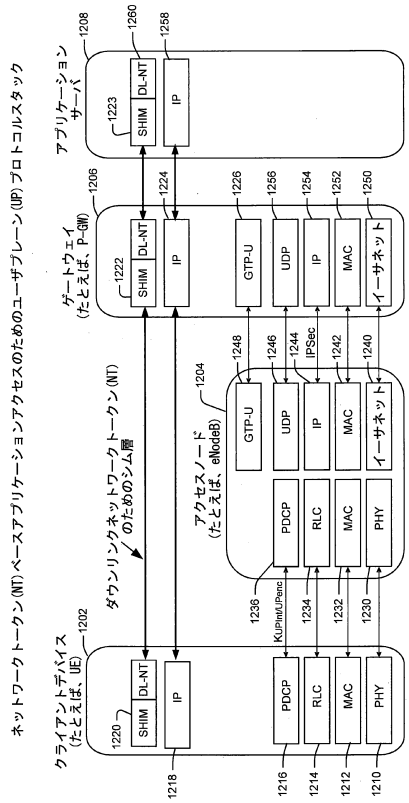
【図１０】



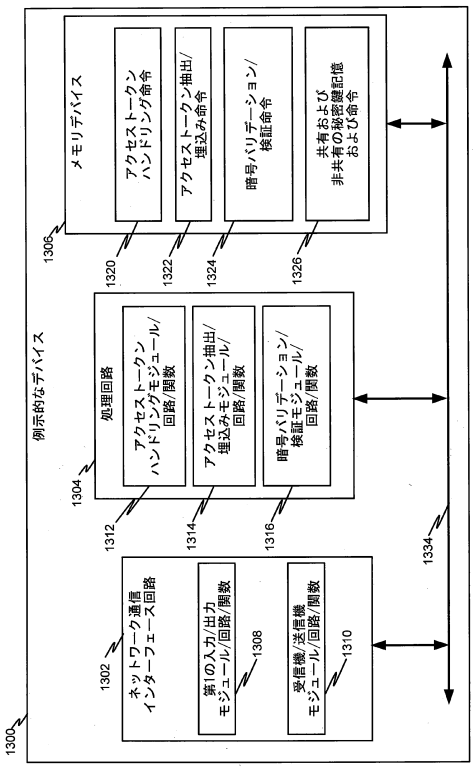
【図１１】



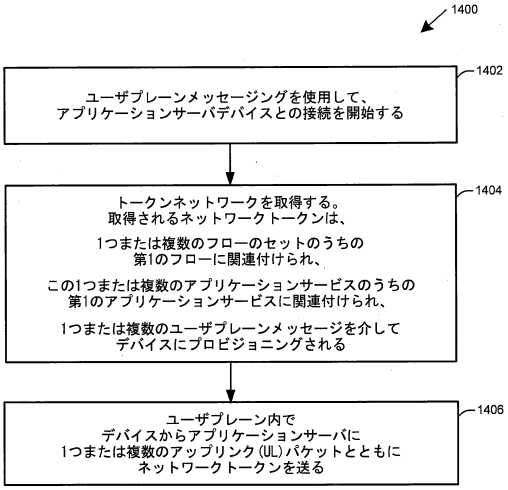
【図１２】



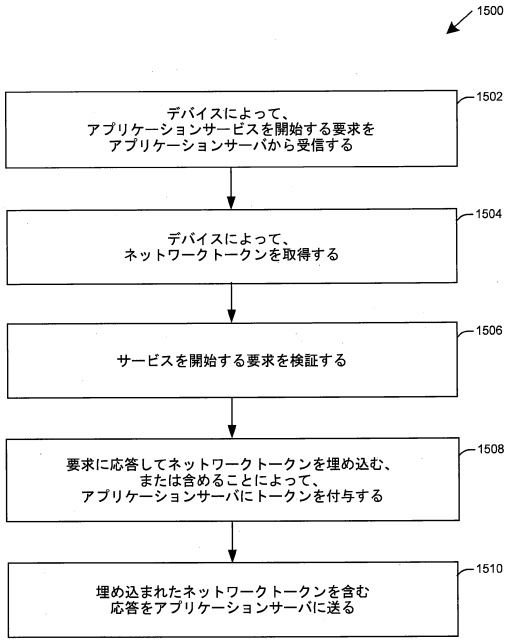
【図１３】



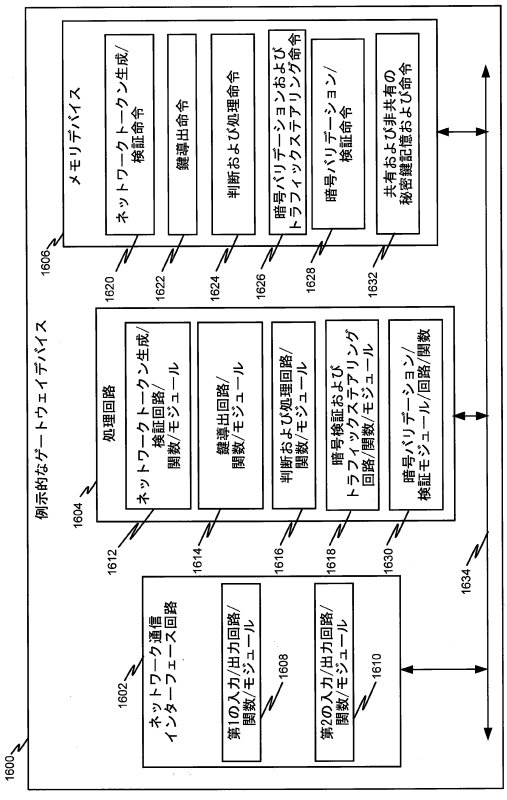
【図１４】



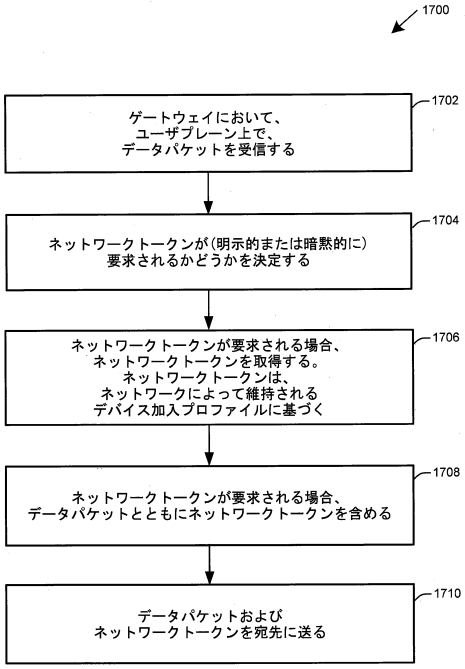
【図１５】



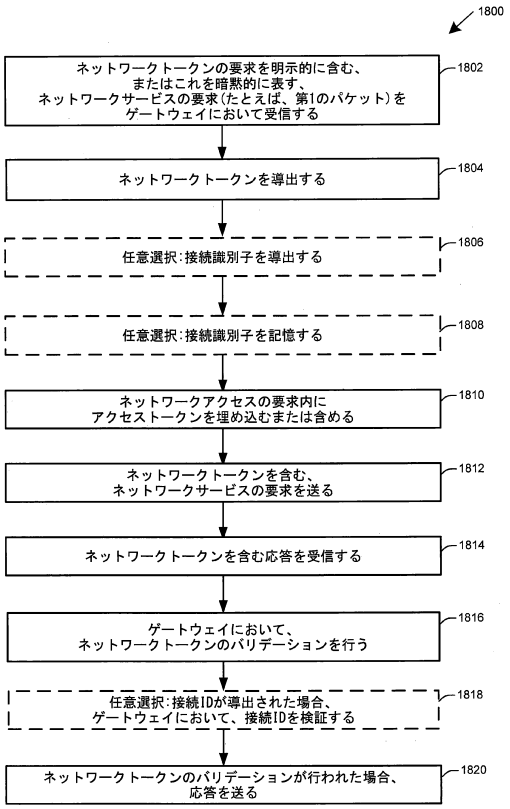
【図１６】



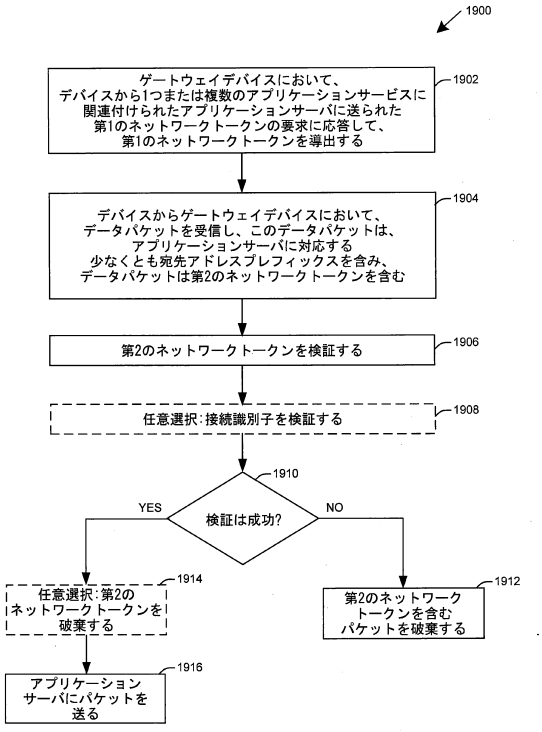
【図１７】



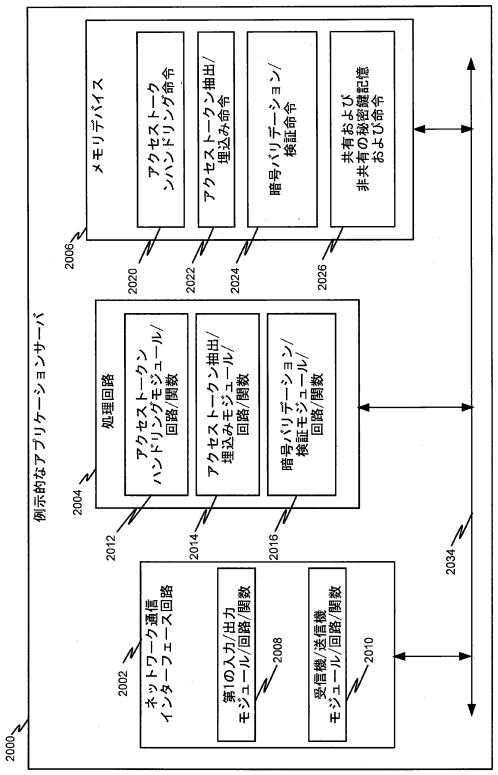
【図１８】



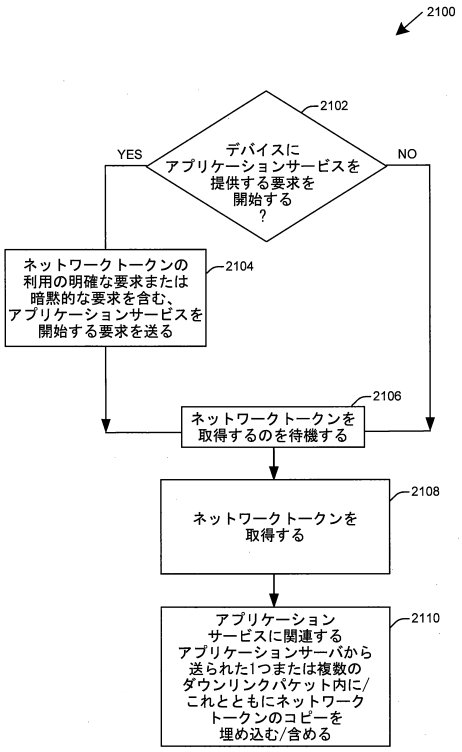
【図１９】



【図２０】



【図２１】


2100
2102
デバイスに
アプリケーションサービスを
提供する要求を
開始する
?
YES
NO
ネットワークトークンの
利用の明確な要求または
暗黙的な要求を含む、
アプリケーションサービスを
開始する要求を送る
2104
2106
ネットワークトークンを
取得するのを待機する
2108
ネットワークトークンを
取得する
2110
アプリケーション
サービスに関連する
アプリケーションサーバから
送られた1つまたは複数の
ダウンリンクパケット内に/
これとともにネットワーク
トークンのコピーを
埋め込む/含める

フロントページの続き

(31)優先権主張番号　14/866,425
(32)優先日　　平成27年9月25日(2015.9.25)
(33)優先権主張国・地域又は機関
　　米国(US)

(72)発明者　ギャヴィン・バーナード・ホーン
　　アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５
(72)発明者　ジョン・ナシールスキー
　　アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５
(72)発明者　ステファノ・ファッチン
　　アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５

審査官　森田　充功

(56)参考文献　特開２０１１－１５５５４５（ＪＰ，Ａ）
　　特開平０７－３０７７５２（ＪＰ，Ａ）
　　特表２０１２－５１１８４６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
　　Ｈ０４Ｌ　１２／９１１
　　Ｈ０４Ｌ　１２／６６
　　Ｈ０４Ｗ　８８／１６