

(19) 日本国特許庁 (JP)

(12) 公表特許公報 (A)

(11) 特許出願公表番号

特表2016-518046

(P2016-518046A)

(43) 公表日 平成28年6月20日 (2016.6.20)

(51) Int.Cl.		F I		テーマコード (参考)
<b>HO 4W 28/02</b>	<b>(2009.01)</b>	HO 4W	28/02	5 K O 6 7
<b>HO 4W 12/06</b>	<b>(2009.01)</b>	HO 4W	12/06	

審査請求 未請求 予備審査請求 未請求 (全 35 頁)

(21) 出願番号	特願2016-505479 (P2016-505479)	(71) 出願人	507364838
(86) (22) 出願日	平成26年3月11日 (2014.3.11)		クアルコム, インコーポレイテッド
(85) 翻訳文提出日	平成27年9月18日 (2015.9.18)		アメリカ合衆国 カリフォルニア 921
(86) 国際出願番号	PCT/US2014/023347		21 サン ディエゴ モアハウス ドラ
(87) 国際公開番号	W02014/159387		イブ 5775
(87) 国際公開日	平成26年10月2日 (2014.10.2)	(74) 代理人	100108453
(31) 優先権主張番号	61/805,885		弁理士 村山 靖彦
(32) 優先日	平成25年3月27日 (2013.3.27)	(74) 代理人	100163522
(33) 優先権主張国	米国 (US)		弁理士 黒田 晋平
(31) 優先権主張番号	14/203,194	(72) 発明者	ステファノ・ファッテン
(32) 優先日	平成26年3月10日 (2014.3.10)		アメリカ合衆国・カリフォルニア・921
(33) 優先権主張国	米国 (US)		21・サン・ディエゴ・モアハウス・ドラ
			イブ・5775

最終頁に続く

(54) 【発明の名称】 ネットワーク上においてシグナリングストームを制限するための機構

## (57) 【要約】

ワイヤレス通信のためのユーザ機器 (UE) により実行される方法であり、方法は、アクセスポイント (AP) から認証負荷インジケータを受信するステップと、少なくとも部分的には認証負荷インジケータに基づいてネットワークエンティティによる認証を試みるか否かを決定することを含む。

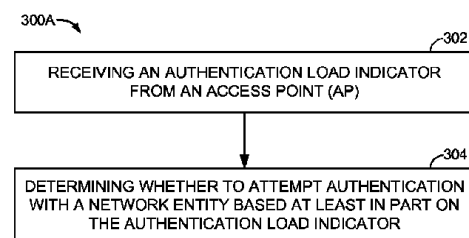


FIG. 3A

**【特許請求の範囲】****【請求項 1】**

ワイヤレス通信のためのユーザ機器(UE)により実行される方法であって、  
アクセスポイント(AP)から認証負荷インジケータを受信するステップと、  
少なくとも部分的には前記認証負荷インジケータに基づいてネットワークエンティティ  
による認証を試みるか否かを決定するステップと  
を含む、方法。

**【請求項 2】**

前記認証を試みるか否かを決定するステップが、前記認証負荷インジケータに基づいて  
前記認証を試みる前に待機するか否かを決定するステップを含み、前記方法は、  
前記APから再試行インジケータを受信するステップと、  
前記再試行インジケータに基づいて期間を決定するステップと、  
待機する決定が行われた場合に前記認証を試みる前に前記期間の間待機するステップと  
をさらに含む、請求項1に記載の方法。

10

**【請求項 3】**

前記認証を試みる前に待機するか否かを決定するステップが、  
前記認証負荷インジケータを閾値と比較するステップと、  
前記認証負荷インジケータが前記閾値より上である場合に前記認証を試みる前に待機す  
ることを決定するステップと  
を含む、請求項2に記載の方法。

20

**【請求項 4】**

前記期間を決定するステップが、前記再試行インジケータおよび前記UEのモバイル識別  
(ID)をハッシュ関数に入力するステップを含む、請求項2に記載の方法。

**【請求項 5】**

前記モバイルIDが前記UEのメディアアクセス制御(MAC)アドレスである、請求項4に記載  
の方法。

**【請求項 6】**

オペレータから管理オブジェクト中の閾値を受信するステップと、  
前記閾値を前記UE上に記憶するステップと  
をさらに含む、請求項3に記載の方法。

30

**【請求項 7】**

ある期間の間、別のUEからのクエリに応答して前記APにより送信されたメッセージにつ  
いてリスンするステップをさらに含み、前記認証負荷インジケータを受信するステップが  
、前記UEが前記期間内に前記メッセージを受信した場合に前記メッセージ中の前記認証負  
荷インジケータを受信するステップを含む、請求項1に記載の方法。

**【請求項 8】**

前記メッセージがアクセスネットワーククエリプロトコル(ANQP)応答である、請求項7  
に記載の方法。

**【請求項 9】**

前記UEが前記メッセージを前記期間内に受信しなかった場合に前記APにネットワーク情  
報についてのクエリを送るステップをさらに含み、前記認証負荷インジケータを受信する  
ステップは前記クエリに応答して前記認証負荷インジケータを受信するステップを含む、  
請求項7に記載の方法。

40

**【請求項 10】**

前記クエリがアクセスネットワーククエリプロトコル(ANQP)クエリである、請求項9に  
記載の方法。

**【請求項 11】**

ワイヤレス通信のための装置であって、  
アクセスポイント(AP)から認証負荷インジケータを受信するための手段と、  
少なくとも部分的には前記認証負荷インジケータに基づいてネットワークエンティティ

50

による認証を試みるか否かを決定するための手段と  
を備える、装置。

【請求項 1 2】

ワイヤレス通信のための装置であって、  
アクセスポイント(AP)から認証負荷インジケータを受信するように構成された受信器と、  
少なくとも部分的には前記認証負荷インジケータに基づいてネットワークエンティティ  
による認証を試みるか否かを決定するように構成された少なくとも1つのプロセッサと、  
前記少なくとも1つのプロセッサに結合された、データを記憶するためのメモリと  
を備える、装置。

10

【請求項 1 3】

ワイヤレス通信のためのユーザ機器(UE)により実行される方法であって、  
第1の期間の間、別のUEからのクエリに応答してアクセスポイント(AP)により送信され  
たメッセージについてリスンするステップと、  
前記UEが前記第1の期間内に前記メッセージを受信した場合に、前記メッセージがネッ  
トワークエンティティによる認証を実行するために前記UEにより必要とされる情報を含む  
か否かを決定するステップと  
を含む、方法。

【請求項 1 4】

前記メッセージが認証負荷インジケータを含み、  
前記メッセージが前記必要とされる情報を含むとの決定が行われた場合に、  
前記認証負荷インジケータが閾値より下である場合に前記認証を試みるステップと、  
前記認証負荷インジケータが前記閾値より上である場合に前記認証を試みる前に第2  
の期間の間待機するステップと  
を実行するステップをさらに含む、請求項13に記載の方法。

20

【請求項 1 5】

前記メッセージが前記必要とされる情報を含まないとの決定が行われた場合に、クエリ  
負荷インジケータに基づいて前記APに前記必要とされる情報についてのクエリを送る前に  
待機するか否かを決定するステップをさらに含む、請求項13に記載の方法。

【請求項 1 6】

前記クエリ負荷インジケータが前記メッセージに含まれている、請求項15に記載の方法  
。

30

【請求項 1 7】

前記必要とされる情報が、前記UEがそれについての認証証明書を有する特定のサービス  
プロバイダまたはネットワークを前記APがサポートするか否かを示す、請求項15に記載の  
方法。

【請求項 1 8】

前記クエリを送る前に待機するか否かを決定するステップが、  
前記クエリ負荷インジケータが閾値より上である場合に前記クエリを送るより前に第2  
の期間の間待機することを決定するステップと、  
前記クエリ負荷インジケータが前記閾値より下である場合に前記クエリを直ちに送るこ  
とを決定するステップと  
を含む、請求項15に記載の方法。

40

【請求項 1 9】

前記クエリ負荷インジケータが前記閾値より上である場合に前記第2の期間中前記APに  
より送信された別のメッセージについてリスンするステップをさらに含む、請求項18に記  
載の方法。

【請求項 2 0】

前記UEが前記第2の期間内に前記別のメッセージを受信した場合に前記別のメッセージ  
が前記必要とされる情報を含むか否かを決定するステップをさらに含む、請求項19に記載

50

の方法。

【請求項 2 1】

ワイヤレス通信のための装置であって、

第1の期間の間、別の装置からのクエリに 응답してアクセスポイント(AP)により送信されたメッセージについてリスンするための手段と、

前記装置が前記第1の期間内に前記メッセージを受信した場合に、前記メッセージがネットワークエンティティによる認証を実行するために前記装置により必要とされる情報を含むか否かを決定するための手段と

を備える、装置。

【請求項 2 2】

ワイヤレス通信のための装置であって、

第1の期間の間、別の装置からのクエリに 응답してアクセスポイント(AP)により送信されたメッセージについてリスンするように構成された受信器と、

前記装置が前記第1の期間内に前記メッセージを受信した場合に、前記メッセージがネットワークエンティティによる認証を実行するために前記装置により必要とされる情報を含むか否かを決定するように構成された少なくとも1つのプロセッサと、

前記少なくとも1つのプロセッサに結合された、データを記憶するためのメモリとを備える、装置。

【請求項 2 3】

ワイヤレス通信のためのネットワークエンティティにより実行される方法であって、

ユーザ機器(UE)からネットワーク情報についてのクエリを受信するステップと、

前記クエリに 응답してメッセージを送信するステップであって、前記メッセージは複数のUEにより受信可能であり、また前記メッセージはクエリ負荷インジケータ、認証負荷インジケータ、および再試行インジケータのうちの少なくとも1つを含む、送信するステップと

を含む、方法。

【請求項 2 4】

前記ネットワークエンティティはアクセスポイント(AP)を含み、

前記方法はネットワーク情報についてのクエリを前記APに送るUEの数に基づいて前記クエリ負荷インジケータを決定するステップをさらに含む、請求項23に記載の方法。

【請求項 2 5】

前記ネットワークエンティティにより認証することを試みるUEの数に基づいて前記認証負荷インジケータを決定するステップをさらに含む、請求項23に記載の方法。

【請求項 2 6】

前記ネットワークエンティティが、アクセスコントローラ(AC)とサービスプロバイダの認証サーバのうちの少なくとも1つを含む、請求項25に記載の方法。

【請求項 2 7】

ワイヤレス通信のための装置であって、

ユーザ機器(UE)からネットワーク情報についてのクエリを受信するための手段と、

前記クエリに 응답してメッセージを送信するための手段であって、前記メッセージは複数のUEにより受信可能であり、また前記メッセージはクエリ負荷インジケータ、認証負荷インジケータ、および再試行インジケータのうちの少なくとも1つを含む、手段とを備える、装置。

【請求項 2 8】

ワイヤレス通信のための装置であって、

ユーザ機器(UE)からネットワーク情報についてのクエリを受信するように構成された受信器と、

前記クエリに 응답してメッセージを生成するように構成された少なくとも1つのプロセッサであって、前記メッセージはクエリ負荷インジケータ、認証負荷インジケータ、および再試行インジケータのうちの少なくとも1つを含む、少なくとも1つのプロセッサと、

10

20

30

40

50

複数のUEにより受信可能である前記メッセージを送信するように構成された送信器と、前記少なくとも1つのプロセッサに結合された、データを記憶するためのメモリとを備える、装置。

【請求項 29】

コンピュータに、

アクセスポイント(AP)から認証負荷インジケータを受信させ、かつ

少なくとも部分的には前記認証負荷インジケータに基づいてネットワークエンティティによる認証を試みるか否かを決定させるためのコードを備える、コンピュータプログラム。

【請求項 30】

10

コンピュータに、

第1の期間の間、別のユーザ機器(UE)からのクエリに応答してアクセスポイント(AP)により送信されたメッセージについてリスンさせ、かつ

前記UEが前記第1の期間内に前記メッセージを受信した場合に、前記メッセージがネットワークエンティティによる認証を実行するために前記UEにより必要とされる情報を含むか否かを決定させる

ためのコードを備える、コンピュータプログラム。

【請求項 31】

コンピュータに、

ユーザ機器(UE)からネットワーク情報についてのクエリを受信させ、かつ

20

前記クエリに応答してメッセージを送信させる

ためのコードを備え、前記メッセージは複数のUEにより受信可能であり、また前記メッセージはクエリ負荷インジケータ、認証負荷インジケータ、および再試行インジケータのうちの少なくとも1つを含む、コンピュータプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

関連出願の相互参照

本特許出願は、2013年3月27日に提出された「Mechanism to Limit Signaling Storms Over A Network」と題された本願の権利者が所有する米国仮出願第61/805,885号に対する優先権を主張し、その開示は本明細書における参照によりここに明確に組み込まれる。

30

【0002】

本開示の態様は、一般にワイヤレス通信システムに関し、より具体的には、ネットワーク上において信号ストームを制限するための技術に関する。

【背景技術】

【0003】

ホットスポットは、ユーザ機器(UE)が地理的領域上に分布されたアクセスポイント(AP)を介してネットワークにアクセスすることを可能にする。APはUEとワイヤレスに通信するためにWi-Fi技術を使用する。従来、UEがホットスポットを介したネットワークアクセスを得るためにユーザの介入が必要とされる。たとえば、UEはホットスポットを検出して検出されたホットスポットに接続するか否かをユーザに尋ね得る。このケースでは、ユーザはUEをホットスポットに接続するか否かの決定を行うことを必要とされる。加えて、ユーザはネットワークアクセスを得るためにホットスポットを介してネットワークに対して認証するために証明書(たとえばユーザ名および/またはパスワード)を提供することを必要とされ得る。

40

【0004】

Wi-Fiアライアンスからのホットスポット2.0は、ネットワークアクセスを得るために、UEがホットスポットを自動的に選択してホットスポットを介してネットワークに対してUEを自動的に認証することを可能にする技術である。しかし、現在のホットスポット2.0の実施は、極めて重要なネットワークノード(たとえばAP、アクセスコントローラ(AC)、認

50

証、許可およびアカウントティング(AAA)サーバ等)における大量のシグナリングトラフィックをもたらし得る。このことは、これらのネットワークノードに過負荷を与え、これらのネットワークノードを正しく機能させず、結果として他のUEからの正当な認証要求へのアクセスを阻止または拒否させる可能性を有する。

【発明の概要】

【課題を解決するための手段】

【0005】

本発明のシステム、方法およびデバイスは、それぞれ数個の態様を有し、これらのうちのどの単一のものも、その所望される属性について単独では責任を有しない。添付の請求項により述べられるような本発明の範囲を限定することなく、いくつかの特徴がここで簡潔に説明される。この説明を考慮した後に、特に「発明を実施するための形態」と題された節を読んだ後に、本発明の特徴がどのように複数のエアインターフェース上における同時通信を含む利点を提供するかが理解されるであろう。

10

【0006】

ワイヤレス通信のためのユーザ機器(UE)により実行される方法であり、アクセスポイント(AP)から認証負荷インジケータを受信するステップと、少なくとも部分的には認証負荷インジケータに基づいてネットワークエンティティによる認証を試みるべきか否かを決定するステップとを含む。

【0007】

ワイヤレス通信のための装置であり、アクセスポイント(AP)から認証負荷インジケータを受信するための手段と、少なくとも部分的には認証負荷インジケータに基づいてネットワークエンティティによる認証を試みるべきか否かを決定するための手段とを備える。

20

【0008】

ワイヤレス通信のための装置であり、アクセスポイント(AP)から認証負荷インジケータを受信するように構成された受信器と、少なくとも部分的には認証負荷インジケータに基づいてネットワークエンティティによる認証を試みるべきか否かを決定するように構成された少なくとも1つのプロセッサと、少なくとも1つのプロセッサに結合された、データを記憶するためのメモリとを備える。

【0009】

ワイヤレス通信のためのUEにより実行される方法であり、第1の期間の間、別のUEからのクエリに回答してアクセスポイント(AP)により送信されたメッセージについてリスンするステップと、UEがメッセージを第1の期間内に受信した場合に当該メッセージがネットワークエンティティによる認証を実行するためにUEにより必要とされる情報を含むか否かを決定するステップとを含む。

30

【0010】

ワイヤレス通信のための装置であり、第1の期間の間、別の装置からのクエリに回答してアクセスポイント(AP)により送信されたメッセージについてリスンするための手段と、装置がメッセージを第1の期間内に受信した場合に当該メッセージがネットワークエンティティによる認証を実行するために装置により必要とされる情報を含むか否かを決定するための手段とを備える。

40

【0011】

ワイヤレス通信のための装置であり、第1の期間の間、別の装置からのクエリに回答してアクセスポイント(AP)により送信されたメッセージについてリスンするように構成された受信器と、装置がメッセージを第1の期間内に受信した場合に当該メッセージがネットワークエンティティによる認証を実行するために装置により必要とされる情報を含むか否かを決定するように構成された少なくとも1つのプロセッサと、少なくとも1つのプロセッサに結合された、データを記憶するためのメモリとを備える。

【0012】

ワイヤレス通信のためのネットワークエンティティにより実行される方法であり、UEからネットワーク情報についてのクエリを受信するステップと、クエリに回答してメッセー

50

ジを送信するステップとを含み、ここでメッセージは複数のUEにより受信可能であって、またメッセージはクエリ負荷インジケータ、認証負荷インジケータ、および再試行インジケータのうちの少なくとも1つを含む。

【0013】

ワイヤレス通信のための装置であり、UEからネットワーク情報についてのクエリを受信するための手段と、クエリに応答してメッセージを送信するための手段とを備えており、ここでメッセージは複数のUEにより受信可能であって、またメッセージはクエリ負荷インジケータ、認証負荷インジケータ、および再試行インジケータのうちの少なくとも1つを含む。

【0014】

ワイヤレス通信のための装置であり、UEからネットワーク情報についてのクエリを受信するように構成された受信器と、クエリに応答してメッセージを生成するように構成された少なくとも1つのプロセッサを備えており、ここでメッセージはクエリ負荷インジケータ、認証負荷インジケータ、および再試行インジケータのうちの少なくとも1つを含む。この装置は、複数のUEにより受信可能であるメッセージを送信するように構成された送信器と、少なくとも1つのプロセッサに結合された、データを記憶するためのメモリとをさらに備える。

【0015】

コンピュータプログラム製品であり、コンピュータに、アクセスポイント(AP)からの認証負荷インジケータを受信させ、少なくとも部分的には認証負荷インジケータに基づいてネットワークエンティティによる認証を試みるか否かを決定させるためのコードを備える非一時的なコンピュータ可読媒体を備える。

【0016】

コンピュータプログラム製品であり、コンピュータに、第1の期間の間、別のUEからのクエリに応答してアクセスポイント(AP)により送信されたメッセージについてリスンさせ、第1の期間内にUEがメッセージを受信した場合に当該メッセージがネットワークエンティティによる認証を実行するためにUEにより必要とされる情報を含むか否かを決定させるためのコードを備える非一時的なコンピュータ可読媒体を備える。

【0017】

コンピュータプログラム製品であり、コンピュータに、UEからのネットワーク情報についてのクエリを受信させ、クエリに応答してメッセージを送信させるためのコードを備える非一時的なコンピュータ可読媒体を備え、ここでメッセージは複数のUEにより受信可能であって、メッセージはクエリ負荷インジケータ、認証負荷インジケータ、および再試行インジケータのうちの少なくとも1つを含む。

【図面の簡単な説明】

【0018】

【図1A】本開示の実施形態が実施され得る、ネットワークアーキテクチャの例を示す図である。

【図1B】UEが図1Aに示されるアクセスポイント(AP)の間において移動するときのネットワーク接続における変化を示す表である。

【図2】本開示の実施形態が実施され得るアーキテクチャの例を示す図である。

【図3A】本開示の実施形態に従ってUEにより実行され得る技法の実施形態を図示する図である。

【図3B】本開示の実施形態に従ってUEにより実行され得る技法の実施形態を図示する図である。

【図4A】本開示の実施形態に従ってAPにより実行され得る技法の実施形態を図示する図である。

【図4B】本開示の実施形態に従ってAPにより実行され得る技法の実施形態を図示する図である。

【図5A】本開示の実施形態に従ってネットワークエンティティにより実行され得る技法

10

20

30

40

50

の実施形態を図示する図である。

【図5B】本開示の実施形態に従ってネットワークエンティティにより実行され得る技法の実施形態を図示する図である。

【図6】本開示の種々の実施形態を実施するように構成され得るUEおよびAPを図示するブロック図である。

【発明を実施するための形態】

【0019】

添付の図面との関係において以下に述べられる詳細な説明は、種々の構成の説明として意図され、本明細書において説明された概念が実施され得る唯一の構成を表すことは意図されない。詳細な説明は、種々の概念の完全な理解を提供する目的のための特定の詳細を含む。しかし、これらの概念はこれらの特定の詳細なしに実施され得ることが当業者には明白であろう。いくつかの例においては、そのような概念を曖昧にすることを回避するために、周知の構造および構成要素がブロック図の形態において示される。

10

【0020】

Wi-Fiアライアンスからのパスポイント(Passpoint)プログラム(WFAホットスポット2.0)の出現により、どのようにデバイスがWi-Fiネットワークに対して認証するかということにおいて変化が起こるであろう。デバイスは、自己のSIMカードに基づく認証を使用するであろう。デバイスは、ユーザからの入力を必要とせずにシームレスに認証を実行する一方、他の形態の証明書(たとえばユーザ名およびパスワード)を使用する現在の公衆ホットスポットへの認証は、明示のユーザ入力を必要とする。

20

【0021】

いくつかの状況下において、このことはいくつかの極めて重要なネットワークノードにおける大量のシグナリングトラフィックをもたらし得る。このことは、ユーザにとってネットワークアクセスが拒否される可能性とともに、これらのネットワークノードが正しく機能することをできなくして、結果として他のUEからの正当な認証要求へのアクセスを阻止または拒否させる可能性を有する。ホットスポット2.0の現在の実施が特定の状況下において大量のシグナリングトラフィックを作り出す可能性を有する、少なくとも3つのケースが存在する。

1. 共同体Wi-Fi配置
2. 公衆輸送ハブ-地下鉄または鉄道駅
3. スポーツ競技場

30

【0022】

共同体Wi-Fi配置のケースでは、車内のホットスポット2.0承認UEは赤の交通信号で停止し、ホットスポット2.0APを検出する。UEは、自動的にAPに対して認証する。その後交通信号は青に変わり、車とUEは次の赤の交通信号まで道路を移動する。UEは異なるホットスポット2.0APを発見し、UEは新しいAPに対して自動的に認証する。都市において、共同住宅のブロックは通常高い密度の数のAPを有し、このことはUEが建物の近くを動き回ると多数のシグナリング要求を引き起こし得る。同一の交通列内に全てホットスポット2.0UEを有する数台の車が存在することは、非常に起こりそうなことである。大都市内の交通信号の数を追加して、また(何千もの)ホットスポット2.0APの数を追加すると、このことはネットワークに開始されている多数の認証要求を結果として生じるであろうことが容易に理解され得る。しかし、UEが運転手または乗客のポケット内にあるとUEは使用されていない可能性が高いが、これらのUEは依然可視のAPに対する認証を試みるであろう。車内のUEとは異なり、ホットスポット2.0APカバレッジ内に入りつつある歩行者のUEは、ホットスポット2.0APにアクセスすることが長く維持されるべきではない。

40

【0023】

公衆輸送ハブのケースでは、地下鉄ネットワークは通常多数の駅を有し、典型的な配置においては駅にはWi-Fiカバレッジがよく存在するが、トンネルには存在しない。通常は、特にラッシュアワー中には、地下鉄の列車は乗車した数百人の乗客とともに1~2分毎に到着し得る。列車上には、多数のホットスポット2.0UEが存在するであろう。これらの全

50



てのUEは駅内のホットスポット2.0APを検出して、これらの全てのUEはネットワークに向かって自動的に認証およびアクセス要求を開始する。このことは多数の別個の認証要求を作り出し、これがネットワーク内の多数の列車および駅により掛け合わされると、短期間中にネットワーク内に多数の認証およびアクセス要求が作り出され得ることが理解され得る。同様の状況は、路面鉄道ネットワークおよび他の輸送ハブにおいて発生し得る。列車内のUEとは異なり、駅のWi-Fiカバレッジ内に入りつつある歩行者のUEは、ホットスポット2.0APにアクセスすることが長く維持されるべきではない。

#### 【0024】

スポーツ競技場のケースでは、スポーツ競技場は複数のホットスポット2.0APが有効にされている。観客により持ち込まれる数千ものホットスポット2.0UEが、競技場内に存在する。自己のUEを使用していない観客が、立ち上がって軽食を買いに行く。途中で彼らは数個の異なるAPを通過する可能性があり、多数の別個の認証要求を作り出す。多数の人々が全て一度に移動する間隔において、このことは多数の認証要求を結果として生じ得る。しかし、観客が競技場を動き回るとき、UEの多くは使用中でない可能性がある。

#### 【0025】

本開示の実施形態は、以下にさらに説明されるように、ホットスポット2.0の現在の実施に伴うこれらのおよび追加の問題に対処する。

#### 【0026】

図1Aは、本開示の実施形態が実施され得る、ネットワークアーキテクチャの例を示す。他のアーキテクチャもまた可能である。図1Aは認証において関与する接続を図示するのみにあることに留意されたい。図1Aは、UEにワイヤレスカバレッジを提供するために地理的領域上において分布され得る、Wi-Fiアクセスポイント(AP)を図示する。図1Aはまたアクセスコントローラ(AC)を図示し、各ACはAPのグループを管理し得る。図1Aはまた、オペレータゲートウェイ(GW)および認証、許可およびアカウントティング(AAA)サーバを図示する。各GWは、APおよび/またはACをAAAサーバのうちの1つに接続する。各AAAサーバは、それぞれのオペレータネットワークへのアクセスを要求するUEを認証し得る。図1Aはまた、それぞれのオペレータネットワークについて加入者情報を記憶するホームロケーションレジスタ(HLR)を図示する。図1Bは、図1Aに示されるAPの間をUEが移動するときのネットワーク接続における変化の例を示す表である。

#### 【0027】

図2は、本開示の実施形態が実施され得る、アーキテクチャの例を示す。図2は、UEがAPに接続するか否かの決定を行うローカルキャンピング決定(local camping decision)を図示する。APは、住宅のユーザにより操作される住宅APであるか、企業により運用される専門のAPであり得る。UEは、以下にさらに説明されるように、APにより送信されるビーコン(beacon)および/またはアクセスネットワーククエリプロトコル(ANQP)応答に基づいて、APに接続するか否かの決定を行い得る。図2はまた、完全な認証および高速再認証を図示する。完全な認証はUEが最初にネットワークに対して認証されるときに実行され得て、高速再認証は(たとえばUEがネットワークとの接続を失った後にネットワークに再接続するとき)UEがネットワークに対して再認証されるときに実行され得る。図2に示されるように、高速再認証は完全な認証よりも少ないネットワークノードに関与する。図2はまた、前の認証からのセキュリティマテリアル(material)がローカル認証を実行するために使用される、対マスターキー(PMK)キャッシングを図示する。

#### 【0028】

いくつかのネットワークノードはより動作に重要であると考えることができ、そのためシグナリング過負荷からの保護を必要とするように優先順位を付けられるべきである。潜在的なコストは、順不同で、以下の指標を使用することにより考慮され得る。

- ・ 影響を受けるユーザの数
- ・ 収益の損失
- ・ 障害の周知度/困惑度(publicity/embarassment)

#### 【0029】

このことを考慮に入れると、ノードの障害が最大の影響を有するであろう保護の順序にノードを格付けすることが可能である。たとえば、この順序は、

1. HLR/HSS
2. 3GPP AAA
3. WLAN AAA
4. WLCまたはWLAN GW
5. AP

であり得る。

【 0 0 3 0 】

本開示の実施形態は、AP、WLC(WLAN ACアクセスコントローラ)またはWLAN GW(たとえば 3GPP SaMOGアーキテクチャにおけるTWAG)およびWLAN AAAを保護するために使用され得る。これらのノードに対する影響は、

WLAN AAA: まだ認証されていないデバイスについての家庭ネットワークにおけるWLANユーザのためのアクセスはないこと。

WLAN/GW: 全てのWLANユーザのためのアクセスはないこと。

AP: 影響を受けるAP上のユーザのためのWLANアクセスはないこと。  
を含み得る。

【 0 0 3 1 】

ホットスポット2.0は、UEがAPに関連付けられたネットワーク情報を発見することを可能にするアクセスネットワーククエリプロトコル(ANQP)をサポートする。UEが(たとえばAPにより送信されるビーコンを検出することにより)APを発見するとき、UEはAPに関連付けられたネットワーク情報についてのANQPクエリをAPに自動的に送る。応答して、APはネットワーク情報とともにANQP応答を送信する。ネットワーク情報は、APを介してアクセス可能であるサービスプロバイダ(たとえばローミングパートナー)のリストを含む、APによりサポートされた機能/能力についての情報を含み得る。ANQP応答を受信すると、UEは、UEがこれに対する証明書を有するサービスプロバイダがANQP応答においてリストされたサービスプロバイダのうちの1つに一致するか否かを決定し得る。一致が存在する場合、UEは、ネットワークアクセスを得るためにAPを介して一致するサービスプロバイダに対して自動的に認証する。

【 0 0 3 2 】

いくつかのケースでは、UEは2つ以上のサービスプロバイダのための証明書を有し得る。これらのサービスプロバイダは異なる優先順位が割り当てられてよく、前記優先順位においてより高い優先順位を有するサービスプロバイダはより低い優先順位を有するサービスプロバイダに対して優先される。これらのケースでは、これらのサービスプロバイダのうちの2つ以上がANQP応答においてリストされたサービスプロバイダに一致する場合、UEは最も高い優先順位を有する一致するサービスプロバイダを選択する。

【 0 0 3 3 】

UEからのANQPクエリは、1つまたは複数の特定のサービスプロバイダがAPを介してアクセス可能であるか否かを問い合わせ得る。このケースでは、対応するANQP応答は、これらのサービスプロバイダのそれぞれについて、APを介してアクセス可能である全てのサービスプロバイダをリストする代わりに、サービスプロバイダがAPを介してアクセス可能であるか否かを示し得る。このことは、ANQP応答を短縮する利点を有し得る。

【 0 0 3 4 】

上記において説明されたように、現在の実施においては、UEはAPを発見すると自動的にANQPクエリをAPに送る。このことは特定の状況においてAPにおいて過度のANQPトラフィックを作り出すことができ、したがって潜在的にAPに過負荷を与え、かつ/またはユーザデータから貴重な帯域幅を奪う可能性がある。たとえば、APは地下鉄駅内に配置され得る。この例では、列車はホットスポット2.0が有効にされたUEを有する多数のユーザを運んで駅に入り得る。これらのUEは、列車が駅に入るとAPを発見し、短期間内に多数のANQPクエリをAPに送り、大量のANQPトラフィックを作り出し得る。現在のANQPの実施がAPにおける

過度のANQPトラフィックにつながり得る他の状況が存在する。現在、APはそれ自体を過度のANQPトラフィックから保護することはできず、ANQPトラフィックが高くなり過ぎたときに多数のユーザを単に拒否する。

【0035】

従って、本開示の実施形態は、ANQPトラフィックを制御するための解決策を提供する。1つの実施形態において、UEはAPを発見すると直ちにANQPクエリをAPに送るのではない。代わりに、UEはある期間(たとえば数秒)について、別のUEからのANQPクエリに応答してAPにより送信されたANQP応答についてリスンする。

【0036】

UEが当該期間内にANQP応答を受信した場合、UEは、ANQP応答がAPを介してネットワークにアクセスするためにUEにより必要とされるネットワーク情報を含むか否かを決定するために、ANQP応答を検査する。たとえば、UEは、UEがそれについての証明書を有するサービスプロバイダをANQPがリストするか否かを決定するために、ANQP応答を検査し得る。ANQP応答が必要とされる情報を含む場合、UEはそれ自体のANQPクエリを送ることなしに当該情報に基づいてAPを介したネットワークに対する認証を進め得る。

【0037】

ANQP応答が必要とされる情報を含まない場合、UEは当該期間内に別のANQP応答についてリスンし続け得る。たとえば、ANQP応答は、APを介してアクセス可能である全てのサービスプロバイダをリストする代わりに、他のUEからのANQPクエリにより識別される特定のサービスプロバイダがAPを介してアクセス可能であるか否かを示し得る。この例においては、識別されたサービスプロバイダがUEがそれについての証明書を有するサービスプロバイダと一致しない場合、UEは別のANQPについてリスンし続け得る。UEが当該期間内に別のANQPを受信した場合、UEは、この別のANQPが必要とされる情報を含むか否かを決定するためにこの別のANQPを検査し得る。この別のANQPが必要とされる情報を含む場合、UEはそれ自体のANQPクエリを送ることなくAPを介したネットワークに対する認証を進め得る。そうでない場合、UEは当該期間が終了するまでリスンし続け得る。

【0038】

UEがANQP応答を当該期間内に受信しないか、当該期間内に必要とされる情報を有するANQP応答を受信しない場合、UEはANQPクエリをAPに送信し、ANQPクエリに応答するANQP応答を受信し得る。

【0039】

従って、APを発見すると直ちにANQPクエリを送信する代わりに、UEはある期間の間、別のUEからのANQPクエリに応答して送信されるANQP応答についてリスンする。UEが別のUEからANQPクエリに応答して送信されたANQP応答から必要とする情報を取得することが可能である場合、UEは別個のANQPクエリを送信しない。このことは、APに送られるANQPクエリ数を削減することによりAPにおけるANQPトラフィックを削減する。

【0040】

APは、多数のUEにより共有されている共通チャネル上においてANQP応答を送信し得る。このことは、多数のUEが1つのUEからのANQPクエリに応答してAPにより送信されるANQP応答についてリスンしてANQP応答を受信することを可能にする。このことは、別個のANQPクエリをAPに送る必要なしに複数のUEが同一のANQP応答からネットワーク情報を受信することを可能にすることにより、ANQPトラフィックを削減する。

【0041】

いくつかの実施形態において、ANQP応答はANQPトラフィックを制御するために使用され得る追加の情報を含むように拡大され得る。1つの実施形態において、ANQP応答はそれぞれのAPにおけるANQP負荷を示すANQP負荷インジケータを含み得る。APは、APにおけるANQPトラフィックの量に基づいて(たとえばAPに送られたANQPクエリ数および/またはAPにより送信されたANQP応答の数に基づいて)、ANQP負荷を計算し得る。ANQP負荷インジケータは、(たとえば1が高いANQP負荷を示し0が低いANQP負荷を示す)2進インジケータであり得る。あるいは、ANQP負荷は負荷値(たとえば1と10との間の値)であり得る。

## 【 0 0 4 2 】

ANQP応答はまた、ANQP負荷が高いときにAPにANQPクエリを送ることをどれだけ長くバックオフする(back off)かをUEに示す、ANQP再試行インジケータを含み得る。以下にさらに説明されるように、ANQP再試行インジケータはタイマ値またはUEがタイマ値を計算するために使用するシード値であり得る。ANQP負荷インジケータおよび/またはANQP再試行インジケータは、各ANQP応答に含まれ得る。

## 【 0 0 4 3 】

1つの実施形態において、UEはAPを発見すると、ある期間の間、別のUEからのANQPクエリに回答してAPにより送信されたANQP応答についてリスンする。UEが当該期間内にANQP応答を受信した場合、UEは、ANQP応答がAPを介してネットワークにアクセスするためにUEにより必要とされるネットワーク情報を含むか否かを決定するために、ANQP応答を検査する。ANQP応答が必要とされる情報を含む場合、UEはそれ自体のANQPクエリを送ることなく当該情報に基づいてAPを介したネットワークに対する認証を進め得る。そうでない場合、UEは当該期間の間リスンし続け得る。ANQP応答はANQP負荷インジケータおよび/またはANQP再試行インジケータを含み、UEはこれらをメモリ内に記憶する。

## 【 0 0 4 4 】

UEが当該期間内にANQP応答を受信したがANQP応答がUEにより必要とされる情報を含まない場合、UEはANQP応答中のANQP負荷インジケータおよび/またはANQP再試行インジケータに基づいてAPにANQPクエリをいつ送るかを決定し得る。

## 【 0 0 4 5 】

ANQP負荷インジケータが2進インジケータである場合、2進インジケータが低ANQP負荷を示すときにはUEは直ちにANQPクエリを送り、2進インジケータが高ANQP負荷を示すときにはANQPクエリを送ることをバックオフする。この例において、2進インジケータはANQP応答において送信される前にAPによって設定され得て、このANQP応答においては、APにおけるANQP負荷が閾値より上であるときにAPは高負荷を示すように2進インジケータを設定し、APにおけるANQP負荷が閾値に等しいか閾値より下であるときにAPは低負荷を示すように2進インジケータを設定し得る。

## 【 0 0 4 6 】

ANQP負荷インジケータが負荷値である場合、UEは負荷値を閾値と比較し得る。負荷値が閾値と等しいか閾値より下である場合、UEは直ちにANQPクエリを送る。負荷値が閾値より上である場合、UEはANQPクエリを送ることをバックオフする。閾値は、オペレータからUEにより受信されてUE上に記憶された管理オブジェクト(たとえばホットスポット2.0管理オブジェクト)により特定され得る。このことは、オペレータが閾値を構成することを可能にする。

## 【 0 0 4 7 】

そのため、ANQP負荷インジケータは、APがANQP負荷が高いときにUEにANQPクエリを送ることをバックオフさせることを可能にする。このことは、APがそれ自体を過度のANQPトラフィックから保護することを可能にする。

## 【 0 0 4 8 】

UEがANQP負荷インジケータに基づいてANQPクエリを送ることをバックオフすることを決定した場合、UEはANQP再試行インジケータに基づいてバックオフ(backoff)期間を決定し得る。UEは、ANQPクエリを送る前にバックオフ期間の間待機し得る。

## 【 0 0 4 9 】

ANQP再試行インジケータがタイマ値である場合、UEはタイマ値に基づいてタイマを設定してタイマが終了したときにANQPクエリを送り得る。ANQP再試行インジケータがシード値である場合、UEはタイマ値を計算するためのアルゴリズムにシード値を入力して、計算されたタイマ値に従ってタイマを設定し得る。たとえば、前記アルゴリズムはハッシュ関数を実施し、該シード値およびUEの移動体識別情報(ID)が、タイマ値を計算するためにハッシュ関数に入力され得る。移動体IDは、メディアアクセス制御(MAC)アドレスまたはUEまたはUEのグループを一意に識別する別のタイプの移動体IDであり得る。

## 【 0 0 5 0 】

移動体IDをハッシュ関数に入力することは、(各移動体IDがUEを一意に識別するとき)異なるUEが異なるタイマ値を計算するか、(各移動体IDがUEのグループを一意に識別するとき)異なるUEのグループが異なるタイマ値を計算することを確実にする。異なるタイマ値は、多過ぎるUEが同時にAPにANQPクエリを送ることを試みることを防止する。タイマ値を計算するために、他のアルゴリズムが採用され得る。

## 【 0 0 5 1 】

1つの実施形態において、UEがANQPクエリを送ることをバックオフ期間の間バックオフすることを決定した場合、UEはバックオフ期間中に別のUEからのANQPクエリに応答してAPにより送信されたANQP応答についてリスンし続け得る。UEがバックオフ期間内にANQP応答を受信した場合、UEは、ANQP応答がAPを介してネットワークにアクセスするためにUEにより必要とされるネットワーク情報を含むか否かを決定するために、ANQP応答を検査する。ANQP応答が必要とされる情報を含む場合、UEはそれ自体のANQPクエリを送ることなく当該情報に基づいてAPを介したネットワークに対する認証を進め得る。このケースでは、UEは必要とする情報を有するので、UEはバックオフ期間の終わりにANQPクエリを送らない。UEは、たとえばより短いバックオフ期間を有する別のUEからのANQPクエリに応答してANQP応答がAPにより送信されたときに、バックオフ期間内にANQP応答を受信し得る。

## 【 0 0 5 2 】

1つの実施形態において、ANQP負荷インジケータがANQP負荷が高いことを示すとき、UEは別の利用可能なAPを選択して別のUEからのANQPクエリに応答してこの別の利用可能なAPにより送信されるANQP応答についてリスンし得る。従って、UEは高ANQP負荷指示(high ANQP load indication)を、より低いANQP負荷を潜在的に有する別の利用可能なAPを試すための指示として取り扱い得る。上記において説明されたANQP負荷を制御するためのいくつかのまたは全てのステップは、この別の利用可能なAPのために実行され得る。

## 【 0 0 5 3 】

上記において説明されたように、ホットスポット2.0は、ネットワークに対するデバイス認証が、ユーザによる入力を必要とされることなくシームレスに実行されることを可能にする。典型的には、モバイルがホットスポットを発見するときにはいつでも、アクティブ(たとえばWi-Fiがアクティブ)であるUEはネットワークへの接続を自動的に試みる。いくつかのケースでは、このことは多過ぎるUEにほぼ同時に認証を試みさせ得る。これは認証に参与するネットワークノード(たとえばAAAサーバ、AC等)に正しく機能させず、結果として他のUEからの正当な認証要求へのアクセスを阻止または拒否させる可能性を有する。

## 【 0 0 5 4 】

従って、本開示の実施形態は認証負荷を制御するための解決策を提供する。1つの実施形態において、ネットワークエンティティは認証負荷を示す認証負荷インジケータを提供する。ネットワークエンティティは、ネットワーク(たとえばサービスプロバイダネットワーク)について認証を実行するために協働する1つのネットワークノード(たとえばAAAサーバ、AC等)または複数のネットワークノードを含み得る。認証処理は、UEから証明書を受信して証明書を検証するためにデータベースに対して受信された証明書をチェックするネットワークエンティティに参与し得る。認証処理はまた、ネットワークエンティティとUEとの間のキーを含むセキュリティマテリアルの転送と、UEとネットワークとの間の安全な接続を確立するためのセキュリティマテリアルの使用を含み得る。

## 【 0 0 5 5 】

ネットワークエンティティは、たとえばネットワークエンティティに対して認証することを試みるUEの数に基づいて、認証負荷を計算し得る。認証負荷インジケータは、(たとえば1が高い負荷を示し0が低い負荷を示す)2進インジケータであり得る。あるいは、認証負荷は負荷値(たとえば1と10の間の値)であり得る。ネットワークエンティティはまた、認証負荷が高いときにUEが認証を試みることをどれだけ長くバックオフするべきかを示す認証再試行インジケータを提供し得る。

## 【 0 0 5 6 】

いくつかの実施形態において、認証負荷インジケータはAPにとって一般的(すなわち特定のサービスプロバイダに関係していない)であり得る。これらの実施形態において、APがローカルAAAサーバまたはAC/TWAGの負荷を制御することを意図する場合、APは認証負荷インジケータを供給し得る。いくつかの実施形態において、認証負荷インジケータは特定のサービスプロバイダまたはPLMNにとって特有であり得る。これらの実施形態において、認証負荷インジケータは、それが適用されるサービスプロバイダまたはPLMNの指示とともに、UEに伝達され得る。いくつかの実施形態において、両方のタイプの認証負荷インジケータがUEに伝達され得る。

## 【 0 0 5 7 】

10

1つの実施形態において、APは認証負荷インジケータおよび/または認証再試行インジケータをANQP応答に含めることにより、これらのインジケータをUEにブロードキャストし得る。このことは、UEが別のUEからのANQPクエリに応答して送信されるANQP応答についてリスンすることにより認証負荷インジケータおよび/または認証再試行インジケータを受信することを可能にする。UEはまた、ANQPクエリをAPに送ってANQPクエリに応答するANQP応答を受信することにより、認証負荷インジケータおよび/または認証再試行インジケータを受信し得る。特定のサービスプロバイダについて特有である認証負荷インジケータおよび/または認証再試行インジケータのために、ANQP応答はサービスプロバイダの指示を含み得る。

## 【 0 0 5 8 】

20

UEが認証負荷インジケータを受信するとき、UEは認証負荷インジケータに基づいて直ちに認証を試みるか否かを決定する。認証負荷インジケータが(たとえば1が高負荷を示し0が低負荷を示す)2進インジケータである場合、2進インジケータが低負荷を示すときにUEは直ちに認証を試み得る。UEは、拡張認証プロトコル(EAP)認証または別の認証の形態を使用して認証を試み得る。UEは、認証要求をネットワークエンティティに送ることにより認証を開始し得る。UEは、2進インジケータが高負荷を示すときに認証を試みることをバックオフする。このことは、APにとって一般的であるか、特定のサービスプロバイダ/PLMNに特有である認証負荷インジケータの両方に適用される。

## 【 0 0 5 9 】

30

認証負荷インジケータが負荷値である場合、UEは負荷値を閾値と比較し得る。負荷値が閾値に等しいか閾値より下である場合、UEは直ちに認証を試みる。負荷値が閾値より上である場合、モバイルステーションは認証を試みることをバックオフする。このことは、APにとって一般的であるか、特定のサービスプロバイダ/PLMNに特有である認証負荷インジケータの両方に適用される。閾値はUEによりオペレータから受信されてUE上に記憶された管理オブジェクト(たとえばホットスポット2.0管理オブジェクト)により特定され得る。このことは、オペレータが閾値を構成することを可能にする。

## 【 0 0 6 0 】

40

このように、認証負荷インジケータは、認証負荷が高いときにネットワークエンティティがUEに認証を試みることをバックオフさせ、これにより認証要求の数を削減することを可能にする。

## 【 0 0 6 1 】

UEが認証負荷インジケータに基づいて認証を試みることをバックオフすることを決定した場合、UEは認証再試行インジケータに基づいてバックオフ期間を決定し得る。UEは認証を試みる前にバックオフ期間の間待機し得る。

## 【 0 0 6 2 】

認証再試行インジケータがタイマ値である場合、UEはタイマ値に基づいてタイマを設定してタイマが終了するときに認証を試み得る。認証再試行インジケータがシード値である場合、UEはタイマ値を計算して計算されたタイマ値に従ってタイマを設定するためにシード値をアルゴリズムに入力し得る。たとえば、アルゴリズムはハッシュ関数を実施し、UEのシード値とモバイルIDはタイマ値を計算するためにハッシュ関数に入力され得る。モバ

50

イルIDは、メディアアクセス制御(MAC)アドレスまたはUEまたはUEのグループを一意に識別する別のタイプのモバイルIDであり得る。

【0063】

モバイルIDをハッシュ関数に入力することは、(各モバイルIDがUEを一意に識別するときに)異なるUEが異なるタイマ値を計算すること、または(各モバイルIDがUEのグループを一意に識別するときに)異なるUEのグループが異なるタイマ値を計算することを確実にする。異なるタイマ値は、多過ぎるUEが同時に認証を試みることを防止する。タイマ値を計算するために、他のアルゴリズムが採用され得る。

【0064】

上記で説明されたように、認証負荷インジケータは、特定のサービスプロバイダにとって特有であり得る。このケースでは、APは2つ以上の認証負荷インジケータを送信することができ、この認証負荷インジケータにおいて各負荷インジケータは異なるサービスプロバイダにとって特有である。各認証負荷インジケータについて、APはまた、それぞれのサービスプロバイダの指示を送信し得る。APはそれぞれのサービスプロバイダのための認証を取り扱うネットワークエンティティ(たとえばAAAサーバ)から各認証負荷インジケータを受信し得る。異なるサービスプロバイダのための認証負荷インジケータは、それぞれのネットワークエンティティにおける負荷に応じて異なり得る。

【0065】

UEが異なるサービスプロバイダにとって特有である認証負荷インジケータを受信したとき、UEはいずれの認証負荷インジケータがUEがそれについての証明書を持するサービスプロバイダに対応するかを決定し得る。これらの認証負荷インジケータの各々について、UEは、対応するサービスプロバイダについての認証負荷が高いか否かを決定するために、各認証負荷インジケータを検査し得る。たとえば、認証負荷インジケータのうちの1つが高負荷を示して認証負荷インジケータのうちの別の1つが低負荷を示す場合、UEは認証のための低負荷を示す認証負荷インジケータに対応するサービスプロバイダを選択し得る。両方の認証負荷インジケータが低負荷を示す場合、モバイルステーションは最も高い優先順位を有する対応するサービスプロバイダを選択し得る。

【0066】

1つの実施形態において、認証負荷インジケータが認証負荷が高いことを示すとき、UEは別の利用可能なAPを選択して(たとえばこの別の利用可能なAPからの認証負荷インジケータを含むANQP応答についてリスンすることにより)この別の利用可能なAPから認証負荷インジケータを受信し得る。このように、UEは潜在的により低い認証負荷を有する別の利用可能なAPを試すための指示として、高認証負荷指示を処理し得る。上記で説明された認証負荷を制御するためのいくつかまたは全てのステップは、この別の利用可能なAPについて実行され得る。

【0067】

いくつかのケースでは、2つのAPが同一のサービスプロバイダへのアクセスを提供するとき、当該サービスプロバイダについての認証負荷インジケータは両方のAPについて同一であり得る。これは、両方のAPが認証を実行するために同一のネットワークエンティティ(たとえばAAAサーバ、AC等)に接続し得るためである。このように、UEが高負荷を示すサービスプロバイダについてAPのうちの1つから認証負荷インジケータを受信するとき、UEは、同一サービスプロバイダについての他方のAPからの認証負荷インジケータも高負荷を示すであろうことを仮定し得る。このケースでは、UEは直ちにこの他方のAPを試さないことを選び、認証のための試みをバックオフし得る。バックオフ期間の後に、UEはいずれかのAPを使用して認証を試み得る。この例において、UEはサービスプロバイダについて認証を実行するために両方のAPが同一のネットワークエンティティに接続することを示す情報を記憶し得る。

【0068】

いくつかの実施形態において、UEがネットワークエンティティ(たとえばAAAサーバ、AC等)に対する認証を試みるとき、ネットワークエンティティは認証を実行して次に対応す

10

20

30

40

50

るネットワークまたはAPへの接続をバックオフすべきか否かをUEに示す。たとえば、ネットワークエンティティは対応するネットワークの制御および/またはデータトラフィックを監視することにより、ネットワークの負荷を決定してネットワーク負荷が高いときにネットワークへの接続をバックオフすべきことをUEに対して示し得る。別の例において、ネットワークエンティティはAPの制御および/またはデータトラフィックを監視することにより、対応するAPの負荷を決定して負荷が高いときに当該APへの接続をバックオフすべきことをUEに示し得る。このケースでは、ネットワークエンティティはAPを含み得る。

#### 【0069】

ネットワークエンティティは、UEとネットワークエンティティが(たとえばEAP認証を使用して)互いに認証した後にバックオフすべきか否かをUEに示し得る。このことは、UEがネットワークエンティティの同一性を確認して、従ってネットワークエンティティからのバックオフ指示を信頼することを可能にする。言い換えれば、ネットワークエンティティは、安全な方法により、対応する負荷が高いときに対応するネットワークまたはAPに接続することをバックオフすべきことをUEに示すことが可能である。この追加されたセキュリティは、悪意のあるユーザが、他のユーザからの正当な認証要求を妨げる偽のバックオフ指示を送信することをより困難にする。

#### 【0070】

1つの実施形態において、ネットワークエンティティはEAP認証を使用してUEを認証し得る。認証処理は、暗号化キーの生成と、ネットワークエンティティとUEとの間における暗号化キーの転送と、ネットワークエンティティとUEとの間における安全な接続を確立するためのこれらのキーの使用を含み得る。EAP認証が成功した後に、ネットワークエンティティは対応するネットワークまたはAPへの接続をバックオフすべきか否かをUEに対して示し得る。

#### 【0071】

1つの実施形態において、ネットワークエンティティはRADIUS(Remote Authentication Dial In User Service)サーバを含み得る。(たとえば高負荷に起因して)UEが対応するネットワークまたはAPへの接続をバックオフすべきであることをネットワークエンティティが決定した場合、RADIUSサーバはRADIUSメッセージにおいてバックオフ指示を対応するAPに送ることができる。次に、APは、EAP認証中に生成されたキーにより保護されているため堅固であるWNM通知フレームにおいて、バックオフ指示をUEに伝達し得る。

#### 【0072】

1つの実施形態において、ネットワークまたはAP負荷が高い場合に、ネットワークエンティティは認証処理の最後におけるEAP認証に失敗し、当該失敗をUEに通知し得る。ネットワークエンティティは、失敗通知が安全であるように、ネットワークエンティティとUEとの間のキーを含むセキュリティマテリアルの転送後にこれを行い得る。失敗通知は、対応するネットワークまたはAPへの接続をバックオフするようにUEに示すエラーコードを含み得る。

#### 【0073】

ネットワークエンティティがバックオフ指示をUEに送るとき、バックオフ指示はタイム値を含み得る。UEは、タイム値に設定されたタイマが終了した後に、ネットワークまたはAPに接続する別の試みを行い得る。あるいは、UEがバックオフ指示を受信したときに、UEはネットワークまたはAPに接続する別の試みを行う前に、ある期間待機し得て、ここで当該期間はUEにおいて構成され得る。

#### 【0074】

UEがネットワークまたはAPに接続する第2の試みを行うとき、ネットワークエンティティは第2の試みについての認証処理を加速するために、第1の試みについての認証処理中に生成されたセキュリティマテリアル(たとえばキー)を使用し得る。たとえば、UEがネットワークまたはAPに接続する第1の試みを行うとき、ネットワークエンティティは完全な認証を実行し得る。完全な認証は、ネットワークエンティティとUEとの間のセキュリティマ

10

20

30

40

50



テリアル(たとえばキー)の生成および転送を含み得る。UEが(たとえばバックオフ後に)ネットワークまたはAPに接続する第2の試みを行うとき、ネットワークエンティティは完全な認証中に生成されたセキュリティマテリアルを使用して高速再認証を実行し得る。完全な認証中に生成されたキーは、一定の期間(たとえば数時間)について有効であることができ、このケースでは高速再認証は完全な認証後のこの期間内に実行され得る。

【0075】

種々の実施形態によりANQP負荷を制御して認証負荷を制御するための技法は組み合わせられ得る。たとえば、UEは種々の実施形態に従ってANQP負荷を制御するための技法を最初に実行し得る。UEが(たとえばANQP応答から)APを介してネットワークに対して認証するために必要とする情報を取得すると、UEは種々の実施形態に従って認証負荷を制御するための技法の実行を進め得る。たとえば、UEが、このUEまたは別のUEからのANQPクエリに応答して送信されるANQP応答から必要とされる情報を取得すると、UEは、ANQP応答中の認証負荷インジケータに基づいて、直ちに認証を試みるべきか認証を試みる前に待機するべきかを決定し得る。

【0076】

例として、開示された主題に従って実施され得る技法は、種々のフローチャートを参照してより良く理解され得る。説明の単純化の目的のために、技法は一連の作用/動作として示されて説明される。しかし、いくつかの動作は本明細書において図示されて説明されるものとは異なる順序により、かつ/または他の動作と実質的に同時に発生し得るため、請求項に記載された主題は動作の数または順序により限定されない。さらに、全ての図示された動作が本明細書において説明された技法を実施するために必要とされる訳ではない場合がある。動作に関連付けられた機能が、ソフトウェア、ハードウェア、これらの組み合わせまたは任意の他の適切な手段(たとえばデバイス、システム、プロセスまたは構成要素)により実施され得ることが理解されるべきである。加えて、本明細書の全体に亘って開示された技法が、そのような技法を種々のデバイスが転送および移動しやすいように、製造品上に符号化された命令および/またはデータとして記憶されることが可能であることが、さらに理解されるべきである。当業者は、状態図におけるような一連の相互関連する状態またはイベントとして方法が代替的に表現され得ることを理解および評価するであろう。

【0077】

図3Aは、UEによりネットワーク内の認証負荷を制御するために実行され得る方法300Aを図示する。方法300Aは、302においてアクセスポイント(AP)から認証負荷インジケータを受信するステップを含み得る。たとえば、UEは当該UEまたは別のUEからのANQPクエリに回答してAPにより送信されるANQP応答中の認証負荷を受信し得る。方法300Aは、304において少なくとも部分的には認証負荷インジケータに基づいてネットワークエンティティによる認証を試みるか否かを決定するステップをさらに含み得る。

【0078】

認証負荷を制御するための追加の動作300Bが、図3Bに図示されている。図3B中の動作300Bのうちの1つまたは複数は、方法300Aの一部としてオプションで実行され得る。図3Bを参照すると、追加の動作300Bは、310において認証負荷インジケータに基づいて認証を試みる前に待機するか否かを決定するステップを含み得る。たとえば、UEは認証負荷インジケータが閾値より上である場合に認証を試みる前に待機(バックオフ)することを決定し得る。追加の動作300Bはまた、312においてAPから再試行インジケータを受信するステップと、314において再試行インジケータに基づいて期間を決定するステップを含み得る。追加の動作300Bは、待機するための決定が行われた場合に316において認証を試みる前にこの期間の間待機するステップをさらに含み得る。

【0079】

図4Aは、APにおける負荷(たとえばANQP負荷)を制御するためにUEにより実行され得る方法400Aを図示する。方法400Aは、402において、ある期間の間、別のUEからのクエリに回答してAPにより送信されるメッセージについてリスンするステップを含み得る。たとえば

、UEは別のUEからのANQPクエリに応答してAPにより送信されるANQP応答についてリスンし得る。方法400Aは、UEがこの期間内にメッセージを受信した場合に、404において、メッセージがネットワークエンティティによる認証を実行するためにUEにより必要とされる情報を含むか否かを決定するステップをさらに含み得る。たとえば、必要とされる情報は、UEがそれについての認証証明書を有するサービスプロバイダをAPがサポートするか否かを含み得る。

【0080】

APにおける負荷を制御するための追加の動作400Bは、図4Bに図示されている。図4B中の動作400Bのうちの1つまたは複数は、方法400Aの一部としてオプションで実行され得る。図4Bを参照すると、追加の動作400Bは、UEが当該期間内にメッセージを受信した場合に、410においてメッセージ中のクエリ負荷インジケータを受信するステップを含み得る。たとえば、クエリ負荷インジケータはANQP負荷インジケータであり得る。追加の動作400Bはまた、メッセージが必要とされる情報を含まないとの決定が行われた場合に、412においてクエリ負荷インジケータに基づいて必要とされる情報についてのクエリをAPに送る前に待機するか否かを決定するステップを含み得る。たとえば、UEはクエリ負荷インジケータが閾値より上である場合にクエリを送る前に待機することを決定し、またクエリ負荷インジケータが閾値より下である場合に直ちにクエリを送ることを決定し得る。

【0081】

図5Aは、負荷を管理するためにネットワークエンティティにより実行され得る方法500Aを図示する。方法500Aは、502においてUEからネットワーク情報についてのクエリを受信するステップを含み得る。たとえば、クエリはANQPクエリであり得る。方法500Aは、504においてクエリに応答してメッセージを送信するステップをさらに含むことができ、ここでメッセージは複数のUEにより受信可能であり、またメッセージはクエリ負荷インジケータ、認証インジケータ、および再試行インジケータのうちの少なくとも1つを含む。たとえば、メッセージは複数のUEにより共有される共通チャネル上において送信され得る。

【0082】

方法500Aの一部としてオプションで実行され得る追加の動作500Bは、図5Bに図示されている。図5Bを参照すると、追加の動作500Bは、510において、ネットワーク情報についてのクエリをAPに送るUEの数に基づいてクエリ負荷インジケータを決定するステップを含み得る。たとえば、クエリ負荷インジケータはANQPクエリをAPに送るUEの数に基づき得る。追加の動作500Bはまた、512において、ネットワークエンティティにより認証を試みるUEの数に基づいて認証負荷インジケータを決定するステップを含み得る。

【0083】

図6は、本開示の種々の実施形態を実施するように構成され得るAP650とUE610を図示するブロック図である。UE610は、アクセス端末、モバイルステーション、加入者ユニット、等とも呼ばれ得る。UE610は、セルラー電話、携帯情報端末(PDA)、ワイヤレスモデム、ワイヤレス通信デバイス、携帯デバイス、ラップトップコンピュータ、タブレットまたは別のモバイルデバイスであり得る。

【0084】

UE610は、受信モジュール615と、送信モジュール620と、AP(たとえばAP650)とワイヤレスに通信するための1つまたは複数のアンテナ625を備える。受信モジュール615は、1つまたは複数のワイヤレス技術を使用してアンテナ625を介してAPからの送信を受信するように構成され得る。たとえば、受信モジュール615はセルラーベースの送信とWi-Fi送信を受信することが可能なデュアルモード受信モジュール、またはWi-Fi専用受信モジュールであり得る。受信モジュール615は、(たとえばAP650から)1つまたは複数のワイヤレスチャネル上において制御および/またはデータ信号を受信するための(たとえばLNA、ダウンコンバータ、イコライザ等の)フロントエンドRF回路構成、復調器および/またはDSP等を含み得る。1つの実施形態において、受信モジュール615は(たとえばIEEE802.11n標準に基づくWi-Fi技術をサポートするために)MIMO信号を処理するための多入力多出力(MIMO)プロセッサを含み得る。本実施形態において、UE610は複数のアンテナを備える。

## 【0085】

送信モジュール620は、(たとえばWi-Fi、セルラーベースの技術等の)1つまたは複数のワイヤレス技術を使用して、アンテナ625を介して制御および/またはデータ信号をAPに送信するように構成され得る。送信モジュール620は、(たとえば電力増幅器、アップコンバータ等の)フロントエンドRF回路構成、変調器および/またはDSP等を含み得る。

## 【0086】

UE610はまた、プロセッサ630とメモリ640を備え得る。プロセッサ630は、バスシステム612を介して受信モジュール615と送信モジュール620とメモリ640とに動作可能に結合されている。バスシステム612は、UE610の種々の構成要素の間において信号を通信するための1つもしくは複数のバスおよび/または他の構造を含み得る。

10

## 【0087】

プロセッサ630は、本明細書において説明された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ム可能な論理デバイス、離散ゲートもしくはトランジスタ論理、離散ハードウェア構成要素、またはこれらの任意の組み合わせを含み得る。プロセッサ630は、受信モジュール615を介してAPから(たとえばANQP応答、セキュリティマテリアル等の)制御および/またはデータ信号を受信することができ、送信モジュール620を介して(たとえばANQPクエリ、認証証明書等の)制御および/またはデータ信号をAPに送信することができる。

## 【0088】

メモリ640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またはこれらの任意の組み合わせを含み得る。メモリ640は、本明細書において説明された本開示の種々の実施形態による動作を実行するためにプロセッサ630により実行され得るコンピュータ可読コードを記憶し得る。メモリ640は、負荷インジケータ、閾値、再試行値、認証証明書、等を含む、プロセッサ630による使用のためのパラメータを記憶し得る。

20

## 【0089】

UE610はまた、ユーザとプロセッサ630のインターフェースを取るためのユーザインターフェース645を備える。ユーザインターフェース645は、ディスプレイ、タッチスクリーン、キーパッドまたはこれらの任意の組み合わせを含み得る。本開示の種々の実施形態による動作は、ユーザインターフェース645からの明示のユーザ入力なしにUE610により自動的に実行され得る。

30

## 【0090】

UE610は、種々の実施形態により本明細書において説明される動作を実行し得る。たとえば、メモリ640は、プロセッサ630により実行されたときに、方法300Aおよび400Aのうちの1つまたは複数の動作をプロセッサ630に実行させるコンピュータ可読コードを記憶し得る。

## 【0091】

UE610は、方法300Aを実行し得る。たとえば、受信モジュール615はAP(たとえばAP650)から認証負荷インジケータを受信する動作302を実行し得る。プロセッサ630は、バスシステム612を介して受信モジュール615から認証負荷インジケータを受信することができ、少なくとも部分的には認証負荷インジケータに基づいて認証を試みるか否かを決定する動作304を実行することができる。受信モジュール615はまた、APから再試行インジケータを受信するオプションの動作312を実行し得、またプロセッサ630は受信モジュール615により受信された再試行インジケータを使用してオプションの動作310、314および316を実行し得る。

40

## 【0092】

UE610はまた、方法400Aを実行し得る。たとえば、受信モジュール615はある期間の間、別のUEからのクエリに回答してAPにより送信されるメッセージについてリスンする動作402を実行し得、またプロセッサ630は当該期間内にUEがメッセージを受信した場合にメッセ

50

ージがUEにより必要とされる情報を含むか否かを決定する動作404を実行し得る。受信モジュール615はクエリ負荷インジケータを受信するオプションの動作410を実行し得、またプロセッサ630はまた、受信モジュール615により受信されたクエリ負荷インジケータを使用してオプションの動作412を実行し得る。

【0093】

AP650は、受信モジュール655と、送信モジュール660と、1つまたは複数のUE(たとえばUE610)とワイヤレスに通信するための1つまたは複数のアンテナ665とを備える。受信モジュール655は、1つまたは複数のワイヤレス技術(たとえばWi-Fi)を使用してアンテナ665を介して1つまたは複数のUEからの送信を受信するように構成され得る。受信モジュール655は、UEに複数のワイヤレスアクセスを提供するために、複数のワイヤレスチャネル上において複数のUEからの送信を受信し得る。送信モジュール660は、1つまたは複数のワイヤレス技術(たとえばWi-Fi)を使用してアンテナ665を介して1つまたは複数のUEに制御および/またはデータ信号を送信するように構成され得る。送信モジュール660は、UEに複数のワイヤレスアクセスを提供するために、複数のワイヤレスチャネル上において複数のUEに制御および/またはデータ信号を送信し得る。送信モジュール660はまた、複数のUEが信号を受信できるように、共通チャネル上において信号(たとえばANQP応答)を送信し得る。共通チャネル上の送信は、ブロードキャストとも呼ばれ得る。

【0094】

AP650はまた、プロセッサ670およびメモリ675を備える。プロセッサ670は、バスシステム652を介して受信モジュール655、送信モジュール660、およびメモリ675に動作可能に結合されている。バスシステム652は、1つもしくは複数のバスおよび/またはAPの種々の構成要素の間において信号を通信するための他の構造を含み得る。

【0095】

プロセッサ670は、本明細書において説明された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ム可能な論理デバイス、離散ゲートもしくはトランジスタ論理、離散ハードウェア構成要素、またはこれらの任意の組み合わせを含み得る。プロセッサ670は、受信モジュール655を介してUEから(たとえばANQPクエリ、認証証明書等の)制御および/またはデータ信号を受信し得、また送信モジュール660を介して(たとえばANQP応答、セキュリティマテリアル等の)制御および/またはデータ信号をUEに送信し得る。

【0096】

メモリ675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またはこれらの任意の組み合わせを含み得る。メモリ675は、本明細書において説明される本開示の種々の実施形態による動作を実行するためにプロセッサ670により実行され得るコンピュータ可読コードを記憶し得る。

【0097】

AP650はまた、ネットワーク内の(たとえばAC、ゲートウェイ、AAAサーバ等の)1つまたは複数のネットワークノードにAP650を接続するためのネットワークインターフェース680を備える。ネットワークインターフェース680は、(たとえばイーサネット(登録商標)接続、ケーブル、デジタル加入者線(DSL)等の)1つまたは複数の有線接続を介して1つまたは複数のネットワークノードにAP650を接続するように構成され得る。AP650は、ネットワークインターフェースを通じて1つまたは複数のネットワークノードへのアクセスをUEに提供し得る。たとえば、プロセッサ670はUEから受信された認証証明書をAAAサーバに転送したAAAサーバから受信されたセキュリティマテリアル(たとえばキー)をUEに転送するために、ネットワークインターフェース680を使用し得る。AP650は、UEがネットワークに対して認証されることに成功したときにUEにネットワークアクセスを提供するためにネットワークインターフェース680を使用し得る。

【0098】

10

20

30

40

50

AP650は、種々の実施形態により本明細書において説明される動作を実行し得る。たとえば、メモリ675は、プロセッサ670により実行されたときに、方法550Aのうちの1つまたは複数の動作をプロセッサ670に実行させるコンピュータ可読コードを記憶し得る。

【0099】

AP650は、方法500Aを実行し得る。たとえば、受信モジュール655はUEからネットワーク情報についてのクエリを受信する動作502を実行し得る。プロセッサ675と送信モジュール660は、クエリに応答して、プロセッサ630にメッセージを生成させてメッセージを、送信のための送信モジュール660に送らせることにより、動作504を実行し得る。プロセッサ630はまた、オプションの動作510および512を実行し得る。

【0100】

10

あるいは、動作510および512は(たとえばAP650を含む)複数の協働するネットワークノードにより実行され得、ここでこれらの動作の実行は協働するネットワークノードの間で分散される。ネットワークノードのそれぞれは、他のネットワークノードと通信するためのネットワークインターフェースと、プロセッサと、メモリとを備えることができ、ここでメモリは、プロセッサにより実行されたときに、プロセッサに動作のうちの1つまたは複数を実行させるコンピュータ可読コードを記憶し得る。

【0101】

当業者は、種々の異なる技術および手法のいずれかを使用して情報および信号が表され得ることを理解するであろう。たとえば、上記説明の全体を通じて参照され得るデータ、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、光場もしくは光粒子、またはこれらの任意の組み合わせにより表現され得る。

20

【0102】

当業者は、本明細書における開示との関係において説明された種々の例示的な論理ブロック、モジュール、回路およびアルゴリズムステップが電子ハードウェア、コンピュータソフトウェアまたは両者の組み合わせとして実施され得ることをさらに理解するであろう。このハードウェアとソフトウェアの相互交換可能性を明確に例示するために、種々の例示的な構成要素、ブロック、モジュール、回路およびステップは一般にそれらの機能によって上述されている。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は、全体のシステムに課される設計制約および特定の用途に依存する。当業者は、各特定の用途のために種々の方法により説明された機能を実施し得るが、そのような実施決定は本開示の範囲からの逸脱を引き起こすものとして解釈されるべきではない。

30

【0103】

本明細書における開示に関して説明された種々の例示的な論理ブロック、モジュールおよび回路は、本明細書において説明された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ム可能な論理デバイス、離散ゲートもしくはトランジスタ論理、離散ハードウェア構成要素、またはこれらの任意の組み合わせにより実施または実行され得る。汎用プロセッサはマイクロプロセッサであり得るが、代替例においては、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り得る。プロセッサは、たとえばDSPとマイクロプロセッサの組み合わせ、複数のマイクロプロセッサ、DSPコアと関係する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のような、計算デバイスの組み合わせとしても実施され得る。

40

【0104】

本明細書における開示に関して説明された方法またはアルゴリズムのステップは、ハードウェアにより直接的に、プロセッサにより実行されるソフトウェアモジュールにおいて、またはこれら2つの組み合わせにおいて具体化され得る。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、

50

ハードディスク、リムーバブルディスク、CD-ROMまたは当該技術において知られる任意の他の形態の記憶媒体内に存在し得る。例示の記憶媒体は、プロセッサが記憶媒体から情報を読み出し、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得る。代替例においては、記憶媒体はプロセッサと一体であり得る。プロセッサと記憶媒体とは、ASIC内に存在し得る。ASICは、ユーザ端末内に存在し得る。代替例においては、プロセッサと記憶媒体はユーザ端末内の離散した構成要素として存在し得る。

【0105】

1つまたは複数の例示の設計において、説明された機能はハードウェア、ソフトウェア、ファームウェアまたはこれらの任意の組み合わせにおいて実施され得る。ソフトウェアにおいて実施される場合、機能はコンピュータ可読媒体上の1つまたは複数の命令またはコードとして記憶されまたは送信され得る。コンピュータ可読媒体は、1つの場所から別の場所へのコンピュータプログラムの転送を容易にする任意の媒体を含む通信媒体とコンピュータ記憶媒体の両方を含む。記憶媒体は、汎用目的または特別目的のコンピュータによりアクセスされ得る任意の利用可能な媒体であり得る。限定ではなく例として、そのようなコンピュータ可読媒体はRAM、ROM、EEPROM、CD-ROMもしくは他の光学ディスク記憶装置、磁気ディスク記憶装置もしくは他の磁気記憶デバイス、あるいは、命令もしくはデータ構造の形態において所望のプログラムコード手段を搬送もしくは記憶するために使用され得るとともに汎用目的もしくは特別目的のコンピュータまたは汎用目的もしくは特別目的のプロセッサによりアクセスされ得る任意の他の媒体を含み得る。また、任意の接続は、送信された信号の非一時的な記憶を含む範囲において、コンピュータ可読媒体と適切に呼ばれ得る。たとえば、ソフトウェアが同軸ケーブル、光ファイバケーブル、ツイストペア、デジタル加入者線(DSL)、または赤外線、無線およびマイクロ波のようなワイヤレス技術を使用して、ウェブサイト、サーバまたは他の遠隔ソースから送信される場合、同軸ケーブル、光ファイバケーブル、ツイストペア、DSL、または赤外線、無線およびマイクロ波のようなワイヤレス技術は、任意の非一時的な時間の長さについて記憶媒体またはデバイスメモリ上の送信チェーン内に信号が保持される範囲において、媒体の定義に含まれる。本明細書において使用されるように、ディスク(disk)およびディスク(disc)はコンパクトディスク(CD)、レーザーディスク(登録商標)、光学ディスク、デジタル多用途ディスク(DVD)、フロッピー(登録商標)ディスク、およびブルーレイディスクを含み、ここでディスク(disk)は通常データを磁氣的に再生する一方、ディスク(disc)はデータをレーザにより光学的に再生する。上記の組み合わせもまた、コンピュータ可読媒体の範囲内に含まれるべきである。

【0106】

本開示の上記の説明は、任意の当業者が本開示を使用または作成することを可能にするために提供されている。本開示に対する種々の変更は当業者に容易に明白になり、本明細書において定義された一般的原理は本開示の精神または範囲から逸脱することなく他の変形に適用され得る。従って、本開示は本明細書において説明された例および設計に限定されることが意図されておらず、本明細書において開示された原理および新規な特徴と一致する最大の範囲に認められるべきである。

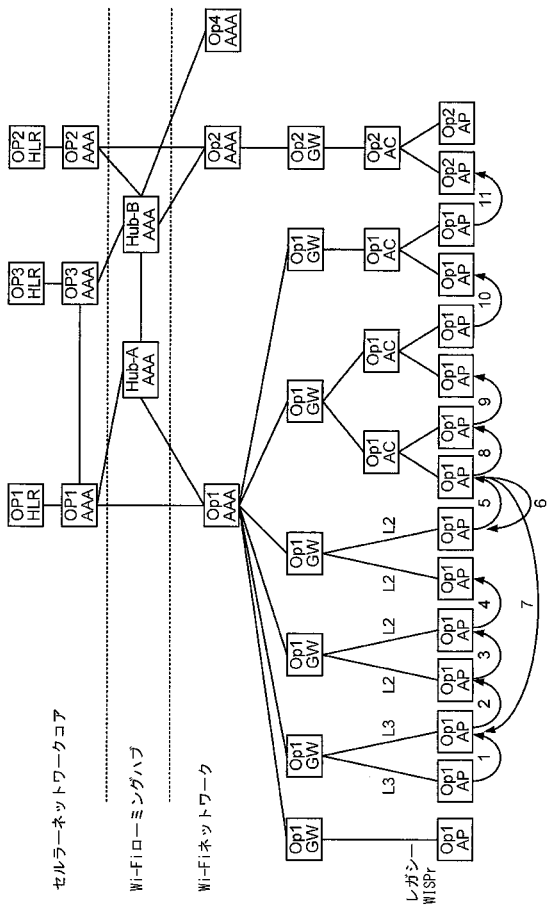
【符号の説明】

【0107】

- 300A 方法
- 300B 追加の動作
- 400A 方法
- 400B 追加の動作
- 500A 方法
- 500B 追加の動作
- 610 UE
- 612 バスシステム
- 615 受信モジュール

- 620 送信モジュール
- 625 アンテナ
- 630 プロセッサ
- 640 メモリ
- 645 ユーザインターフェース
- 650 AP
- 652 バスシステム
- 655 受信モジュール
- 660 送信モジュール
- 665 アンテナ
- 670 プロセッサ
- 675 メモリ
- 680 ネットワークインターフェース

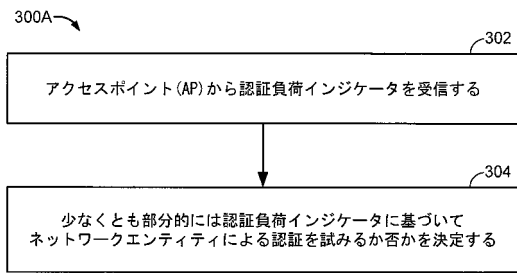
【 図 1 A 】



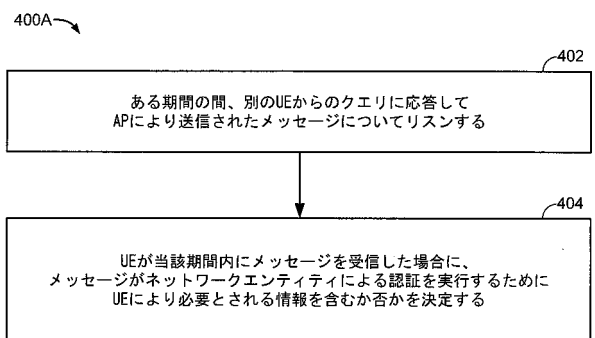
【 図 1 B 】

テストケース	AP	AP コントローラ	WLAN ゲートウェイ	WiFi AAA	Wi-Fi ローミングハブ	セルラー/HSP AAA	セルラー HLR
1	L3->L3		同一	同一	同一/NA*	同一	同一/NA*
2	L3->L2		変更	同一	同一/NA*	同一	同一/NA*
3	L2->L2		同一	同一	同一/NA*	同一	同一/NA*
4	L2->L2		変更	同一	同一/NA*	同一	同一/NA*
5	L2-LWAP	到達	変更	同一	同一/NA*	同一	同一/NA*
6	LWAP->L2	出発	変更	同一	同一/NA*	同一	同一/NA*
7	LWAP->L3	出発	変更	同一	同一/NA*	同一	同一/NA*
8	LWAP->LWAP	同一	同一	同一	同一/NA*	同一	同一/NA*
9	LWAP->LWAP	変更	同一	同一	同一/NA*	同一	同一/NA*
10	LWAP->LWAP	変更	変更	同一	同一/NA*	同一	同一/NA*
11	LWAP-LWAP	変更	変更	変更	変更	同一	同一/NA*

【 図 3 A 】



【 図 4 A 】



```
graph TD; 410[UEが当該期間内にメッセージを受信した場合、  
メッセージ中のクエリ負荷インジケータを受信する] --> 412[メッセージが必要とされる情報を含まないという決定が行われた場合、  
クエリ負荷インジケータに基づいて必要とされる情報についての  
クエリをAPに送る前に待機するか否かを決定する];
```

400B

410

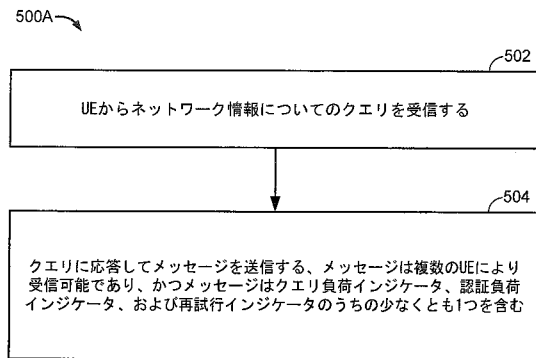
UEが当該期間内にメッセージを受信した場合、  
メッセージ中のクエリ負荷インジケータを受信する

412

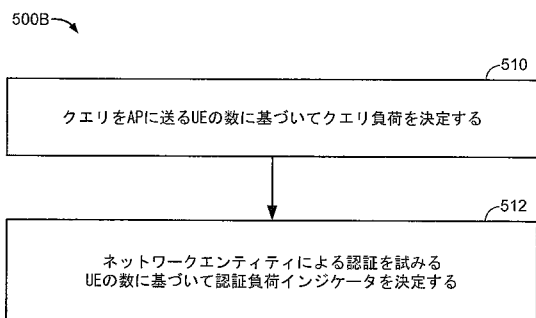
メッセージが必要とされる情報を含まないという決定が行われた場合、  
クエリ負荷インジケータに基づいて必要とされる情報についての  
クエリをAPに送る前に待機するか否かを決定する



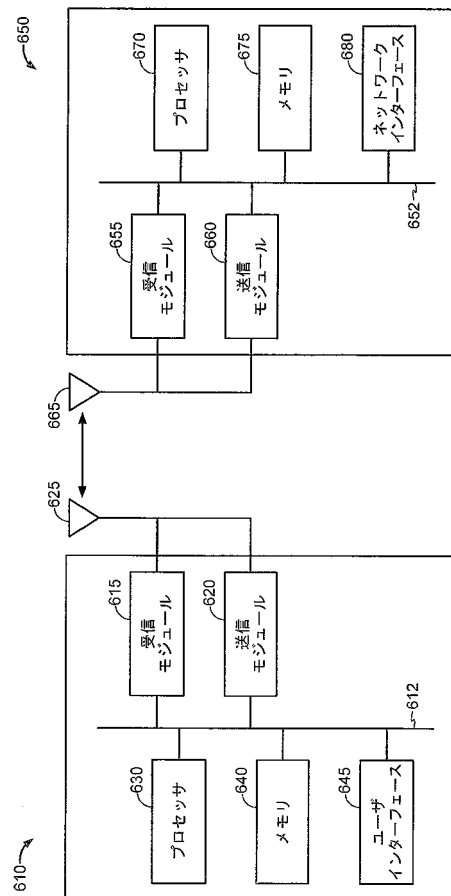
【図 5 A】



【図 5 B】



【図 6】



## 【手続補正書】

【提出日】平成27年1月27日(2015.1.27)

## 【手続補正 1】

【補正対象書類名】特許請求の範囲

【補正対象項目名】全文

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項 1】

ワイヤレス通信のためのユーザ機器(UE)により実行される方法であって、  
 アクセスポイント(AP)から認証負荷インジケータを受信するステップと、  
 少なくとも部分的には前記認証負荷インジケータに基づいてネットワークエンティティ  
 による認証を試みるか否かを決定するステップと  
 を含む、方法。

【請求項 2】

前記認証を試みるか否かを決定するステップが、前記認証負荷インジケータに基づいて  
 前記認証を試みる前に待機するか否かを決定するステップを含み、前記方法は、  
 前記APから再試行インジケータを受信するステップと、  
 前記再試行インジケータに基づいて期間を決定するステップと、  
 待機する決定が行われた場合に前記認証を試みる前に前記期間の間待機するステップと  
 をさらに含む、請求項1に記載の方法。

【請求項 3】

前記認証を試みる前に待機するか否かを決定するステップが、  
 前記認証負荷インジケータを閾値と比較するステップと、  
 前記認証負荷インジケータが前記閾値より上である場合に前記認証を試みる前に待機す

ることを決定するステップと  
を含む、請求項2に記載の方法。

【請求項4】

前記期間を決定するステップが、前記再試行インジケータおよび前記UEのモバイル識別(ID)をハッシュ関数に入力するステップを含む、請求項2に記載の方法。

【請求項5】

前記モバイルIDが前記UEのメディアアクセス制御(MAC)アドレスである、請求項4に記載の方法。

【請求項6】

オペレータから管理オブジェクト中の閾値を受信するステップと、  
前記閾値を前記UE上に記憶するステップと  
をさらに含む、請求項3に記載の方法。

【請求項7】

ある期間の間、別のUEからのクエリに応答して前記APにより送信されたメッセージについてリスンするステップをさらに含み、前記認証負荷インジケータを受信するステップが、前記UEが前記期間内に前記メッセージを受信した場合に前記メッセージ中の前記認証負荷インジケータを受信するステップを含む、請求項1に記載の方法。

【請求項8】

前記メッセージがアクセスネットワーククエリプロトコル(ANQP)応答である、請求項7に記載の方法。

【請求項9】

前記UEが前記メッセージを前記期間内に受信しなかった場合に前記APにネットワーク情報についてのクエリを送るステップをさらに含み、前記認証負荷インジケータを受信するステップは前記クエリに応答して前記認証負荷インジケータを受信するステップを含む、請求項7に記載の方法。

【請求項10】

前記クエリがアクセスネットワーククエリプロトコル(ANQP)クエリである、請求項9に記載の方法。

【請求項11】

ワイヤレス通信のための装置であって、  
アクセスポイント(AP)から認証負荷インジケータを受信するための手段と、  
少なくとも部分的には前記認証負荷インジケータに基づいてネットワークエンティティによる認証を試みるか否かを決定するための手段と  
を備える、装置。

【請求項12】

ワイヤレス通信のための装置であって、  
アクセスポイント(AP)から認証負荷インジケータを受信するように構成された受信器と、  
、  
少なくとも部分的には前記認証負荷インジケータに基づいてネットワークエンティティによる認証を試みるか否かを決定するように構成された少なくとも1つのプロセッサと、  
前記少なくとも1つのプロセッサに結合された、データを記憶するためのメモリと  
を備える、装置。

【請求項13】

ワイヤレス通信のためのユーザ機器(UE)により実行される方法であって、  
第1の間、別のUEからのクエリに応答してアクセスポイント(AP)により送信された、認証負荷インジケータを含むメッセージについてリスンするステップと、  
前記UEが前記第1の期間内に前記メッセージを受信した場合に、前記メッセージがネットワークエンティティによる認証を実行するために前記UEにより必要とされる情報を含むか否かを決定するステップと、  
前記メッセージが前記必要とされる情報を含むとの決定が行われた場合に、

前記認証負荷インジケータが閾値より下である場合に前記認証を試みるステップと、  
前記認証負荷インジケータが前記閾値より上である場合に前記認証を試みる前に第2  
の期間の間待機するステップと  
を実行するステップと  
を含む、方法。

【請求項 14】

前記メッセージが前記必要とされる情報を含まないとの決定が行われた場合に、クエリ負荷インジケータに基づいて前記APに前記必要とされる情報についてのクエリを送る前に待機するか否かを決定するステップをさらに含む、請求項13に記載の方法。

【請求項 15】

前記クエリ負荷インジケータが前記メッセージに含まれている、請求項14に記載の方法。

【請求項 16】

前記必要とされる情報が、前記UEがそれについての認証証明書を有する特定のサービスプロバイダまたはネットワークを前記APがサポートするか否かを示す、請求項14に記載の方法。

【請求項 17】

前記クエリを送る前に待機するか否かを決定するステップが、  
前記クエリ負荷インジケータが閾値より上である場合に前記クエリを送るより前に第2の期間の間待機することを決定するステップと、  
前記クエリ負荷インジケータが前記閾値より下である場合に前記クエリを直ちに送ることを決定するステップと  
を含む、請求項14に記載の方法。

【請求項 18】

前記クエリ負荷インジケータが前記閾値より上である場合に前記第2の期間中前記APにより送信された別のメッセージについてリスンするステップをさらに含む、請求項17に記載の方法。

【請求項 19】

前記UEが前記第2の期間内に前記別のメッセージを受信した場合に前記別のメッセージが前記必要とされる情報を含むか否かを決定するステップをさらに含む、請求項18に記載の方法。

【請求項 20】

ワイヤレス通信のための装置であって、  
第1の期間の間、別の装置からのクエリに応答してアクセスポイント(AP)により送信された、認証負荷インジケータを含むメッセージについてリスンするための手段と、  
前記装置が前記第1の期間内に前記メッセージを受信した場合に、前記メッセージがネットワークエンティティによる認証を実行するために前記装置により必要とされる情報を含むか否かを決定するための手段と、  
前記認証負荷インジケータが閾値より下である場合に前記認証を試みるための手段と、  
前記認証負荷インジケータが前記閾値より上である場合に前記認証を試みる前に第2の  
期間の間待機するための手段と  
を備える、装置。

【請求項 21】

ワイヤレス通信のための装置であって、  
第1の期間の間、別の装置からのクエリに応答してアクセスポイント(AP)により送信された、認証負荷インジケータを含むメッセージについてリスンするように構成された受信器と、  
前記装置が前記第1の期間内に前記メッセージを受信した場合に、前記メッセージがネットワークエンティティによる認証を実行するために前記装置により必要とされる情報を含むか否かを決定するように構成された少なくとも1つのプロセッサと、

前記少なくとも1つのプロセッサに結合された、データを記憶するためのメモリとを備え、前記プロセッサが、  
前記メッセージが前記必要とされる情報を含むことの決定が行われた場合に、  
前記認証負荷インジケータが閾値より下である場合に前記認証を試み、  
前記認証負荷インジケータが前記閾値より上である場合に前記認証を試みる前に第2の  
期間の間待機するように、さらに構成される、装置。

【請求項 2 2】

ワイヤレス通信のためのネットワークエンティティにより実行される方法であって、ユーザ機器(UE)からネットワーク情報についてのクエリを受信するステップと、前記クエリに応答してメッセージを送信するステップであって、前記メッセージは複数のUEにより受信可能であり、また前記メッセージはクエリ負荷インジケータ、認証負荷インジケータ、ANQP再試行インジケータ、および認証再試行インジケータのうちの少なくとも1つを含む、送信するステップとを含む、方法。

【請求項 2 3】

前記ネットワークエンティティはアクセスポイント(AP)を含み、前記方法はネットワーク情報についてのクエリを前記APに送るUEの数に基づいて前記クエリ負荷インジケータを決定するステップをさらに含む、請求項22に記載の方法。

【請求項 2 4】

前記ネットワークエンティティにより認証することを試みるUEの数に基づいて前記認証負荷インジケータを決定するステップをさらに含む、請求項22に記載の方法。

【請求項 2 5】

前記ネットワークエンティティが、アクセスコントローラ(AC)とサービスプロバイダの認証サーバのうちの少なくとも1つを含む、請求項24に記載の方法。

【請求項 2 6】

ワイヤレス通信のための装置であって、ユーザ機器(UE)からネットワーク情報についてのクエリを受信するための手段と、前記クエリに応答してメッセージを送信するための手段であって、前記メッセージは複数のUEにより受信可能であり、また前記メッセージはクエリ負荷インジケータ、認証負荷インジケータ、ANQP再試行インジケータ、および認証再試行インジケータのうちの少なくとも1つを含む、手段とを備える、装置。

【請求項 2 7】

ワイヤレス通信のための装置であって、ユーザ機器(UE)からネットワーク情報についてのクエリを受信するように構成された受信器と、前記クエリに応答してメッセージを生成するように構成された少なくとも1つのプロセッサであって、前記メッセージはクエリ負荷インジケータ、認証負荷インジケータ、ANQP再試行インジケータ、および認証再試行インジケータのうちの少なくとも1つを含む、少なくとも1つのプロセッサと、

複数のUEにより受信可能である前記メッセージを送信するように構成された送信器と、前記少なくとも1つのプロセッサに結合された、データを記憶するためのメモリとを備える、装置。

【請求項 2 8】

コンピュータに、アクセスポイント(AP)から認証負荷インジケータを受信させ、かつ少なくとも部分的には前記認証負荷インジケータに基づいてネットワークエンティティによる認証を試みるか否かを決定させるためのコードを備える、コンピュータプログラム。

【請求項 2 9】

コンピュータに、

第1の期間の間、別のユーザ機器(UE)からのクエリに 응답してアクセスポイント(AP)により送信された、認証負荷インジケータを含むメッセージについてリスンさせ、

前記UEが前記第1の期間内に前記メッセージを受信した場合に、前記メッセージがネットワークエンティティによる認証を実行するために前記UEにより必要とされる情報を含むか否かを決定させ、かつ

前記メッセージが前記必要とされる情報を含むことの決定が行われた場合に、

前記認証負荷インジケータが閾値より下である場合に前記認証を試みるステップと

、

前記認証負荷インジケータが前記閾値より上である場合に前記認証を試みる前に第2の期間の間待機するステップとを実行させる

ためのコードを備える、コンピュータプログラム。

【請求項30】

コンピュータに、

ユーザ機器(UE)からネットワーク情報についてのクエリを受信させ、かつ

前記クエリに 응답してメッセージを送信させる

ためのコードを備え、前記メッセージは複数のUEにより受信可能であり、また前記メッセージはクエリ負荷インジケータ、認証負荷インジケータ、ANQP再試行インジケータ、および認証再試行インジケータのうちの少なくとも1つを含む、コンピュータプログラム。

## 【国際調査報告】

## INTERNATIONAL SEARCH REPORT

International application No

PCT/US2014/023347

<b>A. CLASSIFICATION OF SUBJECT MATTER</b> INV. H04W28/02 H04W48/06 H04W48/16 H04W12/06 ADD.		
According to International Patent Classification (IPC) or to both national classification and IPC		
<b>B. FIELDS SEARCHED</b> Minimum documentation searched (classification system followed by classification symbols) H04L H04W		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) EPO-Internal, WPI Data, INSPEC		
<b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b>		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	US 2013/070739 A1 (MCCANN STEPHEN [GB] ET AL) 21 March 2013 (2013-03-21) abstract paragraph [0011] paragraph [0016] - paragraph [0039] paragraph [0109] paragraphs [0116] - [0118] figures 1-4,7-9 -----	1,11,12, 23-29,31 2-6,10, 13-22,30
X Y	WO 2012/139075 A1 (QUALCOMM INC [US]; DHANDA MUNGAL SINGH [GB]; CHILDREN PHILIP J [GB]; J) 11 October 2012 (2012-10-11) abstract paragraph [0110] - paragraph [0182]; figures 8-14 ----- -/--	23,24, 27,28,31 2-6,10, 13-22,30
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input checked="" type="checkbox"/> See patent family annex.		
* Special categories of cited documents : *A* document defining the general state of the art which is not considered to be of particular relevance *E* earlier application or patent but published on or after the international filing date *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) *O* document referring to an oral disclosure, use, exhibition or other means *P* document published prior to the international filing date but later than the priority date claimed *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art *&* document member of the same patent family		
Date of the actual completion of the international search		Date of mailing of the international search report
30 September 2014		07/10/2014
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016		Authorized officer  Dujardin, Corinne

## INTERNATIONAL SEARCH REPORT

International application No

PCT/US2014/023347

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2008/170497 A1 (JEONG MOO RYONG [US] ET AL) 17 July 2008 (2008-07-17)	1-3,6, 11,12, 23-29,31
Y	abstract paragraph [0003] - paragraph [0010] paragraph [0016] - paragraph [0037] paragraph [0048] - paragraph [0083] figures 2, 4, 7-9	7-9
X	US 2010/061232 A1 (ZHOU WEI HUA [CN] ET AL) 11 March 2010 (2010-03-11)	23, 25-28,31
A	abstract paragraph [0005] - paragraph [0006] paragraph [0015] - paragraph [0073] figures 1-6	1,11,12, 29
X	US 2013/072248 A1 (BAJKO GABOR [US]) 21 March 2013 (2013-03-21)	13-23, 27,28, 30,31
Y	abstract paragraph [0059] - paragraph [0109] paragraph [0005] - paragraph [0043] figures 1-4B	7-9
X	US 2012/311686 A1 (MEDINA ALEXANDER A [US] ET AL) 6 December 2012 (2012-12-06)	23,27, 28,31
	abstract paragraph [0162] - paragraph [0163] paragraph [0169] paragraph [0177] figures 15-16	
X	Yongqiang Liu, shijian Li, Junqing xie, Xunteng Xu: "Keyword(s): Abstract: Security Analysis and Improvements of IEEE802.11u Security Analysis and Improvements of IEEE802.11u", 21 December 2012 (2012-12-21), XP055143372, Retrieved from the Internet: URL:http://www.hpl.hp.com/techreports/2012/HPL-2012-243.pdf [retrieved on 2014-09-29] abstract page 2, left-hand column, line 1 - right-hand column, line 7 page 3, left-hand column, line 25 - right-hand column, line 17 figure 1	23,27, 28,31

## INTERNATIONAL SEARCH REPORT

International application No.  
PCT/US2014/023347**Box No. II Observations where certain claims were found unsearchable (Continuation of Item 2 of first sheet)**

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:  
because they relate to subject matter not required to be searched by this Authority, namely:
  
2. ☐ Claims Nos.:  
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
  
3. ☐ Claims Nos.:  
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

**Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)**

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
  
2. ☐ As all searchable claims could be searched without effort justifying an additional fees, this Authority did not invite payment of additional fees.
  
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
  
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

**Remark on Protest**

- ☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.
- ☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.
- ☒ No protest accompanied the payment of additional search fees.



International Application No. PCT/US2014/023347

**FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210**

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-12, 29

Method performed by a user equipment for wireless communication, the method comprising: receiving an authentication load indicator from an access point; and determining whether to attempt authentication with a network entity based at least in part on the authentication load indicator.

---

2. claims: 13-22, 30

Method performed by a user equipment for wireless communication, the method comprising: listening for a message transmitted by an access point in response to a query from another UE for a first time period; and determining whether the message includes information needed by the UE to perform authentication with a network entity if the UE receives the message within the first time period.

---

3. claims: 23-28, 31(all partially)

Method performed by a network entity for wireless communication, the method comprising: receiving a query for network information from a user equipment; and transmitting a message in response to the query, wherein the message is receivable by a plurality of UEs and the message includes at least a query load indicator.

---

4. claims: 23-28, 31(all partially)

Method performed by a network entity for wireless communication, the method comprising: receiving a query for network information from a user equipment; and transmitting a message in response to the query, wherein the message is receivable by a plurality of UEs and the message includes at least a retry indicator.

---

**INTERNATIONAL SEARCH REPORT**

Information on patent family members

International application No

PCT/US2014/023347

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2013070739 A1	21-03-2013	NONE	
WO 2012139075 A1	11-10-2012	CN 103563411 A EP 2695407 A1 JP 2014510507 A KR 20140009476 A US 2013095863 A1 WO 2012139075 A1	05-02-2014 12-02-2014 24-04-2014 22-01-2014 18-04-2013 11-10-2012
US 2008170497 A1	17-07-2008	EP 2119262 A1 JP 5025736 B2 JP 2010516192 A US 2008170497 A1 WO 2008088964 A1	18-11-2009 12-09-2012 13-05-2010 17-07-2008 24-07-2008
US 2010061232 A1	11-03-2010	NONE	
US 2013072248 A1	21-03-2013	CN 103002545 A EP 2571319 A1 US 2013072248 A1	27-03-2013 20-03-2013 21-03-2013
US 2012311686 A1	06-12-2012	NONE	

## フロントページの続き

(81)指定国 AP(BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), EA(AM, AZ, BY, KG, KZ, RU, TJ, TM), EP(AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG), AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US

(72)発明者 アルノー・メイラン

アメリカ合衆国・カリフォルニア・9 2 1 2 1・サン・ディエゴ・モアハウス・ドライヴ・5 7 7  
5

(72)発明者 ジェラルド・ジャレット

アメリカ合衆国・カリフォルニア・9 2 1 2 1・サン・ディエゴ・モアハウス・ドライヴ・5 7 7  
5

Fターム(参考) 5K067 AA28 DD11 EE02 EE10 EE22 FF18