

(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2017-538345

(P2017-538345A)

(43) 公表日 平成29年12月21日 (2017. 12. 21)

(51) Int. Cl.	F I	テーマコード (参考)
H O 4 W 48/08 (2009. 01)	H O 4 W 48/08	5 K O 6 7
H O 4 W 12/06 (2009. 01)	H O 4 W 12/06	
H O 4 W 76/02 (2009. 01)	H O 4 W 76/02	
H O 4 W 84/12 (2009. 01)	H O 4 W 84/12	
H O 4 W 88/06 (2009. 01)	H O 4 W 88/06	
審査請求 有 予備審査請求 未請求 (全 38 頁) 最終頁に続く		

(21) 出願番号	特願2017-525578 (P2017-525578)	(71) 出願人	513311642
(86) (22) 出願日	平成26年11月12日 (2014. 11. 12)		ノキア ソリューションズ アンド ネットワークス オサケユキチュア
(85) 翻訳文提出日	平成29年6月29日 (2017. 6. 29)		フィンランド エフイー-02610 エスプー カラボルティ 3
(86) 国際出願番号	PCT/EP2014/074326	(74) 代理人	100099759
(87) 国際公開番号	W02016/074707		弁理士 青木 篤
(87) 国際公開日	平成28年5月19日 (2016. 5. 19)	(74) 代理人	100092624
			弁理士 鶴田 準一
		(74) 代理人	100141162
			弁理士 森 啓
		(74) 代理人	100141254
			弁理士 榎原 正巳
		最終頁に続く	

(54) 【発明の名称】 方法、装置およびシステム

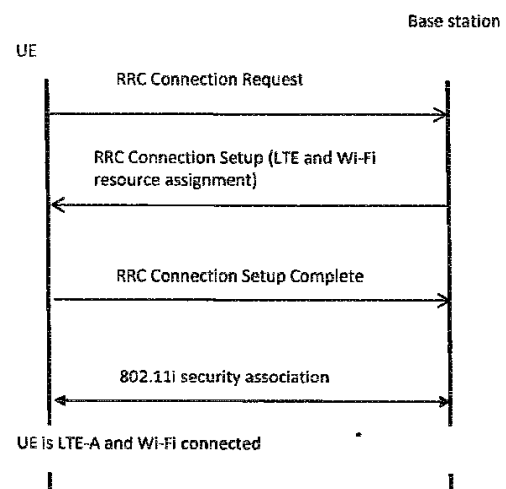
(57) 【要約】

【課題】 セルラ・ネットワークおよび無線ローカル・エリア・ネットワーク (WLAN) アグリゲーション。

【解決手段】 ユーザー機器において、第1のネットワークからのアクセス情報の受信を制御するステップであって、前記アクセス情報は第2のネットワークと結び付けられており、第1および第2のネットワークが異なる無線アクセス技術を使用するステップと、第2のネットワークと通信状態で前記アクセス情報を使用するステップと、を含む方法が提供されている。

【選択図】 図4

Figure 4



【特許請求の範囲】**【請求項 1】**

ユーザー機器において、第 1 のネットワークからのアクセス情報の受信を制御するステップであって、前記アクセス情報は第 2 のネットワークと結び付けられており、前記第 1 および第 2 のネットワークが異なる無線アクセス技術を使用するステップと、

前記第 2 のネットワークと通信状態で前記アクセス情報を使用するステップと、を含む方法。

【請求項 2】

前記第 1 のネットワークおよび前記第 2 のネットワークのうちの少なくとも 1 つに対しユーザー機器識別情報を提供するステップをさらに含む、請求項 1 に記載の方法。

10

【請求項 3】

ユーザー機器識別情報が、メディア・アクセス制御アドレス、一時的ユーザー機器アイデンティティ情報および疑似端末アイデンティティ情報のうちの少なくとも 1 つを含む、請求項 2 に記載の方法。

【請求項 4】

前記第 2 のネットワークでの認証プロシージャにおいて前記アクセス情報を使用するステップを含む、請求項 1 ないし 3 のいずれかに記載の方法。

【請求項 5】

前記認証プロシージャは、拡張可能認証プロトコル・プロシージャ、事前共有鍵に基づく認証システム、高速基本サービス・セット遷移スキーム、およびペアワイズ・マスタ鍵に基づく認証システムのうちの少なくとも 1 つである、請求項 4 に記載の方法。

20

【請求項 6】

前記アクセス情報は、無線ローカル・エリア・ネットワーク・クレデンシャル、疑似端末識別子情報、および一時的ユーザー機器アイデンティティ情報のうちの少なくとも 1 つを含む、請求項 1 ないし 5 のいずれかに記載の方法。

【請求項 7】

第 1 のネットワークによってユーザー機器に対して第 2 のネットワークに結び付けられたアクセス情報を提供するステップであって、前記アクセス情報が前記第 2 のネットワークとの通信用であり、前記第 1 および第 2 のネットワークが異なる無線アクセス技術を使用するステップを含む、方法。

30

【請求項 8】

前記第 1 のネットワークにより、前記第 2 のネットワークからのアクセス情報の要求を制御するステップをさらに含む、請求項 7 に記載の方法。

【請求項 9】

前記第 1 のネットワークにより、前記アクセス情報を割当てするステップと、
前記第 2 のネットワークに対して前記アクセス情報を提供するステップと、
をさらに含む、請求項 7 に記載の方法。

【請求項 10】

前記ユーザー機器からユーザー機器識別情報を受信するステップをさらに含む、請求項 7 ないし 9 のいずれか 1 項に記載の方法。

40

【請求項 11】

第 2 のネットワークにおいて、前記第 2 のネットワークと通信するユーザー機器を検出するステップであって、前記ユーザー機器が第 1 のネットワークで認証され、前記第 1 および第 2 のネットワークが異なる無線アクセス技術を使用しているステップと、

前記第 1 のネットワークでの前記ユーザー機器認証において使用されるアクセス情報に基づいて前記ユーザー機器が前記第 2 のネットワークにアクセスできるようにするステップと、
を含む方法。

【請求項 12】

前記第 1 のネットワークからのアクセス情報の受信を制御するステップであって、前記

50

アクセス情報が前記第 1 のネットワークにより割当てられているステップをさらに含む、請求項 1 1 に記載の方法。

【請求項 1 3】

前記第 1 のネットワークからの要求に応答して、前記第 1 のネットワークに対しアクセス情報を提供するステップをさらに含む、請求項 1 1 に記載の方法。

【請求項 1 4】

アクセス情報に基づいて前記ユーザー機器が前記第 2 のネットワークにアクセスできるようにするステップは、前記ユーザー機器での認証プロシージャにおいて前記アクセス情報を使用するステップを含む、請求項 1 2 または 1 3 に記載の方法。

【請求項 1 5】

前記ユーザー機器からのユーザー機器識別情報の受信を制御するステップをさらに含む、請求項 1 1 ないし 1 4 のいずれか 1 項に記載の方法。

【請求項 1 6】

アクセス情報に基づいて前記ユーザー機器が前記第 2 のネットワークにアクセスできるようにするステップは、前記ユーザー機器での認証プロシージャにおいて前記ユーザー機器識別情報を使用するステップを含む、請求項 1 5 に記載の方法。

【請求項 1 7】

前記第 1 のネットワークは無線アクセス・ネットワークであり、前記第 2 のネットワークは無線ローカル・エリア・ネットワークである、請求項 1 ないし 1 6 のいずれかに記載の方法。

【請求項 1 8】

請求項 1 ないし 1 7 のいずれか 1 項に記載の方法を行なうための手段を含む装置。

【請求項 1 9】

コンピュータ上で実行された場合に請求項 1 ないし 1 7 のいずれかに記載のステップを行なうためのソフトウェア・コード部分を含む、コンピュータ向けのコンピュータ・プログラム・プロダクト。

【請求項 2 0】

少なくとも 1 つのプロセッサと、コンピュータ・プログラム・コードを含む少なくとも 1 つのメモリとを含む装置において、前記少なくとも 1 つのメモリおよび前記コンピュータ・プログラム・コードは、前記少なくとも 1 つのプロセッサを用いて、前記装置に、少なくとも、

ユーザー機器において第 1 のネットワークからのアクセス情報の受信を制御させ、ここで前記アクセス情報は第 2 のネットワークに結び付けられ、前記第 1 および第 2 のネットワークは異なる無線アクセス技術を使用し、

前記第 2 のネットワークと通信状態で前記アクセス情報を使用させる、ように構成されている、装置。

【請求項 2 1】

前記第 1 のネットワークおよび前記第 2 のネットワークのうちの少なくとも 1 つに対して、ユーザー機器識別情報を提供するように構成されている、請求項 2 0 に記載の装置。

【請求項 2 2】

ユーザー機器識別情報が、メディア・アクセス制御アドレス、一時的ユーザー機器アイデンティティ情報および疑似端末アイデンティティ情報のうちの少なくとも 1 つを含む、請求項 2 1 に記載の装置。

【請求項 2 3】

前記第 2 のネットワークでの認証プロシージャにおいて前記アクセス情報を使用するように構成されている、請求項 2 0 ないし 2 2 のいずれかに 1 項に記載の装置。

【請求項 2 4】

前記認証プロシージャは、拡張可能認証プロトコル・プロシージャ、事前共有鍵に基づく認証システム、高速基本サービス・セット遷移スキーム、およびペアワイズ・マスタ鍵に基づく認証システムのうちの少なくとも 1 つである、請求項 2 3 に記載の装置。

10

20

30

40

50

【請求項 25】

前記アクセス情報は、無線ローカル・エリア・ネットワーク・クレデンシャル、疑似端末識別子情報、および一時的ユーザー機器アイデンティティ情報のうちの少なくとも1つを含む、請求項20ないし24のいずれか1項に記載の装置。

【請求項 26】

少なくとも1つのプロセッサと、コンピュータ・プログラム・コードを含む少なくとも1つのメモリとを含む装置において、前記少なくとも1つのメモリおよび前記コンピュータ・プログラム・コードは、前記少なくとも1つのプロセッサを用いて、前記装置に、少なくとも、

第1のネットワークによってユーザー機器に対して第2のネットワークに結び付けられたアクセス情報を提供させるように構成されており、ここで前記アクセス情報は前記第2のネットワークとの通信用であり、前記第1および第2のネットワークは異なる無線アクセス技術を使用する、装置。

10

【請求項 27】

前記第1のネットワークにより、前記第2のネットワークからのアクセス情報の要求を制御するように構成されている、請求項26に記載の装置。

【請求項 28】

前記第1のネットワークにより、前記アクセス情報を割当て、
前記第2のネットワークに対して前記アクセス情報を提供する、
ように構成されている、請求項27に記載の装置。

20

【請求項 29】

前記ユーザー機器からユーザー機器識別情報を受信するように構成されている、請求項26ないし28のいずれか1項に記載の装置。

【請求項 30】

少なくとも1つのプロセッサと、コンピュータ・プログラム・コードを含む少なくとも1つのメモリとを含む装置において、前記少なくとも1つのメモリおよび前記コンピュータ・プログラム・コードは、前記少なくとも1つのプロセッサを用いて、前記装置に、少なくとも、

第2のネットワークにおいて、前記第2のネットワークと通信するユーザー機器を検出させ、ここで前記ユーザー機器は第1のネットワークで認証され、前記第1および第2のネットワークは異なる無線アクセス技術を使用しており、

30

前記第1のネットワークでの前記ユーザー機器認証において使用されるアクセス情報に基づいて前記ユーザー機器が前記第2のネットワークにアクセスできるようにさせる、
ように構成されている、装置。

【請求項 31】

前記第1のネットワークからのアクセス情報の受信を制御するように構成され、ここで前記アクセス情報は前記第1のネットワークにより割当てられる、請求項30に記載の装置。

【請求項 32】

前記第1のネットワークからの要求に応答して、前記第1のネットワークに対しアクセス情報を提供するように構成されている、請求項30に記載の装置。

40

【請求項 33】

前記ユーザー機器での認証プロシージャにおいて前記アクセス情報を使用するように構成されている、請求項31または32に記載の装置。

【請求項 34】

前記ユーザー機器からのユーザー機器識別情報の受信を制御するように構成されている、請求項30ないし33のいずれか1項に記載の装置。

【請求項 35】

前記ユーザー機器での認証プロシージャにおいて前記ユーザー機器識別情報を使用するように構成されている、請求項34に記載の装置。

50

【請求項 36】

前記第1のネットワークは無線アクセス・ネットワークであり、前記第2のネットワークは無線ローカル・エリア・ネットワークである、請求項20ないし35のいずれか1項に記載の装置。

【請求項 37】

非一時的コンピュータ可読記憶媒体上で具体化されるコンピュータ・プログラムにおいて、プロセスを実行するべくプロセスを制御するためのプログラム・コードを含み、前記プロセスは、ユーザー機器において、第1のネットワークからのアクセス情報の受信を制御するステップであって、前記アクセス情報は第2のネットワークと結び付けられており、前記第1および第2のネットワークが異なる無線アクセス技術を使用するステップと、前記第2のネットワークと通信状態で前記アクセス情報を使用するステップと、を含む、コンピュータ・プログラム。

10

【請求項 38】

前記プロセスは、前記第1のネットワークおよび前記第2のネットワークのうちの少なくとも1つに対しユーザー機器識別情報を提供するステップをさらに含む、請求項37に記載のコンピュータ・プログラム。

【請求項 39】

ユーザー機器識別情報が、メディア・アクセス制御アドレス、一時的ユーザー機器アイデンティティ情報および疑似端末アイデンティティ情報のうちの少なくとも1つを含む、請求項38に記載のコンピュータ・プログラム。

20

【請求項 40】

前記プロセスは、前記第2のネットワークでの認証プロシージャにおいて前記アクセス情報を使用するステップを含む、請求項37ないし39のいずれか1項に記載のコンピュータ・プログラム。

【請求項 41】

前記認証プロシージャは、拡張可能認証プロトコル・プロシージャ、事前共有鍵に基づく認証システム、高速基本サービス・セット遷移スキーム、およびペアワイズ・マスタ鍵に基づく認証システムのうちの少なくとも1つである、請求項40に記載のコンピュータ・プログラム。

【請求項 42】

前記アクセス情報は、無線ローカル・エリア・ネットワーク・クレデンシャル、疑似端末識別子情報、および一時的ユーザー機器アイデンティティ情報のうちの少なくとも1つを含む、請求項37ないし41のいずれか1項に記載のコンピュータ・プログラム。

30

【請求項 43】

非一時的コンピュータ可読記憶媒体上で具体化されるコンピュータ・プログラムにおいて、プロセスを実行するべくプロセスを制御するためのプログラム・コードを含み、前記プロセスは、第1のネットワークによってユーザー機器に対して第2のネットワークに結び付けられたアクセス情報を提供するステップを含み、ここで、前記アクセス情報は前記第2のネットワークとの通信用であり、前記第1および第2のネットワークは異なる無線アクセス技術を使用する、コンピュータ・プログラム。

40

【請求項 44】

前記プロセスは、前記第1のネットワークにより、前記第2のネットワークからのアクセス情報の要求を制御するステップを含む、請求項43に記載のコンピュータ・プログラム。

【請求項 45】

前記プロセスは、前記第1のネットワークにより、前記アクセス情報を割当てするステップと、

前記第2のネットワークに対して前記アクセス情報を提供するステップと、を含む、請求項43に記載のコンピュータ・プログラム。

【請求項 46】

50

前記プロセスは、前記ユーザー機器からユーザー機器識別情報を受信するステップを含む、請求項 43 ないし 45 のいずれか 1 項に記載のコンピュータ・プログラム。

【請求項 47】

非一時的コンピュータ可読記憶媒体上で具体化されるコンピュータ・プログラムにおいて、プロセスを実行するべくプロセスを制御するためのプログラム・コードを含み、前記プロセスは、第 2 のネットワークにおいて、前記第 2 のネットワークと通信するユーザー機器を検出するステップであって、前記ユーザー機器が第 1 のネットワークで認証され、前記第 1 および第 2 のネットワークが異なる無線アクセス技術を使用しているステップと、

前記第 1 のネットワークでの前記ユーザー機器認証において使用されるアクセス情報に基づいて前記ユーザー機器が前記第 2 のネットワークにアクセスできるようにするステップと、

を含む、コンピュータ・プログラム。

【請求項 48】

前記プロセスは、前記第 1 のネットワークからのアクセス情報の受信を制御するステップ含み、ここで、前記アクセス情報は前記第 1 のネットワークにより割当てられている、請求項 47 に記載のコンピュータ・プログラム。

【請求項 49】

前記プロセスは、前記第 1 のネットワークからの要求に応答して、前記第 1 のネットワークに対しアクセス情報を提供するステップを含む、請求項 47 に記載のコンピュータ・プログラム。

【請求項 50】

前記プロセスは、前記ユーザー機器での認証プロシージャにおいて前記アクセス情報を使用するステップを含む、請求項 48 または 49 に記載のコンピュータ・プログラム。

【請求項 51】

前記プロセスは、前記ユーザー機器からのユーザー機器識別情報の受信を制御するステップを含む、請求項 47 ないし 50 のいずれか 1 項に記載のコンピュータ・プログラム。

【請求項 52】

前記プロセスは、前記ユーザー機器での認証プロシージャにおいて前記ユーザー機器識別情報を使用するステップを含む、請求項 51 に記載のコンピュータ・プログラム。

【請求項 53】

前記第 1 のネットワークは、無線アクセス・ネットワークであり、前記第 2 のネットワークは無線ローカル・エリア・ネットワークである、請求項 37 ないし 52 のいずれか 1 項に記載のコンピュータ・プログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本出願は、方法、装置およびシステムに関し、詳細には、非排他的にセルラ・ネットワークおよび無線ローカル・エリア・ネットワーク（WLAN）アグリゲーションに関する。

【背景技術】

【0002】

通信システムとは、通信経路に関与するさまざまなエンティティ間にキャリアを提供することにより、ユーザー端末、基地局および／または他のノードなどの 2 つ以上のエンティティ間の通信セッションを可能にする設備と考えることができる。例えば通信ネットワークおよび 1 つ以上の互換性ある通信デバイスを用いて、通信システムを提供することができる。通信は、例えば音声、電子メール（Eメール）、テキスト・メッセージ、マルチメディアおよび／またはコンテンツ・データなどの通信を搬送するためのデータの通信を含むことができる。提供されるサービスの非限定的な例としては、双方向または多方向呼出し、データ通信またはマルチメディア・サービスおよび、インターネットなどのデータ

10

20

30

40

50

ネットワークシステムへのアクセスがある。

【0003】

無線通信システムにおいて、少なくとも2つの局間の通信の少なくとも一部分は、無線リンク上で発生する。無線システムの例としては、移動体ネットワーク、衛星通信システム、および異なる無線ローカル・ネットワーク、例えば無線ローカル・エリア・ネットワーク（WLAN）が含まれる。移動体ネットワークは、典型的に、セルに分割でき、したがって、多くの場合セルラ・システムと呼ばれる。

【0004】

ユーザーは、適切な通信デバイスまたは端末を用いて通信システムにアクセスすることができる。ユーザーの通信デバイスは、多くの場合ユーザー機器（UE）と呼ばれる。通信デバイスには、通信を可能にするため、例えば通信ネットワークへのアクセスまたは他のユーザーとの直接通信を可能にするための適切な信号受信および伝送用装置が備えられている。通信デバイスは、1つの局、例えばセルの基地局により提供されるキャリアにアクセスし、このキャリア上で通信を伝送および／または受信することができる。

【発明の概要】

【0005】

第1の態様では、ユーザー機器において、第1のネットワークからのアクセス情報の受信を制御するステップであって、前記アクセス情報は第2のネットワークと結び付けられており、第1および第2のネットワークが異なる無線アクセス技術を使用するステップと、第2のネットワークと通信状態で前記アクセス情報を使用するステップと、を含む方法が提供されている。

【0006】

この方法は、第1のネットワークおよび第2のネットワークのうちの少なくとも1つに対しユーザー機器識別情報を提供するステップを含むことができる。

【0007】

ユーザー機器識別情報は、メディア・アクセス制御アドレス、一時的ユーザー機器アイデンティティ情報および疑似端末アイデンティティ情報のうちの少なくとも1つを含むことができる。

【0008】

この方法は、第2のネットワークでの認証プロシージャにおいて前記アクセス情報を使用するステップを含むことができる。

【0009】

認証プロシージャは、拡張可能認証プロトコル・プロシージャ、事前共有鍵に基づく認証システム、高速基本サービス・セット遷移スキーム、およびペアワイズ・マスタ鍵に基づく認証システムのうちの少なくとも1つであることができる。

【0010】

前記アクセス情報は、無線ローカル・エリア・ネットワーク・クレデンシャル、疑似端末識別子情報、および一時的ユーザー機器アイデンティティ情報のうちの少なくとも1つを含むことができる。

【0011】

第1のネットワークは無線アクセス・ネットワークであることができ、第2のネットワークは無線ローカル・エリア・ネットワークであることができる。

【0012】

第2の態様では、第1のネットワークによってユーザー機器に対して第2のネットワークに結び付けられたアクセス情報を提供するステップであって、前記アクセス情報が第2のネットワークとの通信用であり、前記第1および第2のネットワークが異なる無線アクセス技術を使用するステップを含む、方法が提供されている。

【0013】

この方法は、第1のネットワークにより、第2のネットワークからのアクセス情報の要求を制御するステップをさらに含むことができる。

10

20

30

40

50

【0014】

この方法は、第1のネットワークにより、前記アクセス情報を割当てするステップと、第2のネットワークに対して前記アクセス情報を提供するステップと、を含むことができる。

【0015】

この方法は、ユーザー機器からユーザー機器識別情報を受信するステップを含むことができる。

【0016】

ユーザー機器識別情報は、メディア・アクセス制御アドレス、一時的ユーザー機器アイデンティティ情報および疑似端末アイデンティティ情報のうちの少なくとも1つを含むことができる。

10

【0017】

前記アクセス情報は、無線ローカル・エリア・ネットワーク・クレデンシャル、疑似端末識別子情報、および一時的ユーザー機器アイデンティティ情報のうちの少なくとも1つを含むことができる。

【0018】

第1のネットワークは無線アクセス・ネットワークであることができ、第2のネットワークは無線ローカル・エリア・ネットワークであることができる。

【0019】

第3の態様では、第2のネットワークにおいて、第2のネットワークと通信するユーザー機器を検出するステップであって、前記ユーザー機器が第1のネットワークで認証され、第1および第2のネットワークが異なる無線アクセス技術を使用しているステップと、第1のネットワークでのユーザー機器認証において使用されるアクセス情報に基づいてユーザー機器が第2のネットワークにアクセスできるようにするステップと、を含む方法が提供されている。

20

【0020】

この方法は、第1のネットワークからのアクセス情報の受信を制御するステップであって、前記アクセス情報が第1のネットワークにより割当てられているステップを含むことができる。

【0021】

この方法は、第1のネットワークからの要求に応答して、第1のネットワークに対しアクセス情報を提供するステップを含むことができる。

30

【0022】

アクセス情報に基づいてユーザー機器が第2のネットワークにアクセスできるようにするステップは、ユーザー機器での認証プロシージャにおいて前記アクセス情報を使用するステップを含むことができる。

【0023】

認証プロシージャは、拡張可能認証プロトコル・プロシージャ、事前共有鍵に基づく認証システム、高速基本サービス・セット遷移スキーム、およびペアワイズ・マスタ鍵に基づく認証システムのうちの少なくとも1つであることができる。

40

【0024】

この方法は、ユーザー機器からユーザー機器識別情報の受信を制御するステップを含むことができる。

【0025】

ユーザー機器識別情報は、メディア・アクセス制御アドレス、一時的ユーザー機器アイデンティティ情報および疑似端末アイデンティティ情報のうちの少なくとも1つを含むことができる。

【0026】

アクセス情報に基づいてユーザー機器が第2のネットワークにアクセスできるようにするステップは、ユーザー機器での認証プロシージャにおいて前記ユーザー機器識別情報を

50

使用するステップを含むことができる。

【0027】

前記アクセス情報は、無線ローカル・エリア・ネットワーク・クレデンシャル、疑似端末識別子情報、および一時的ユーザー機器アイデンティティ情報のうちの少なくとも1つを含むことができる。

【0028】

第1のネットワークは無線アクセス・ネットワークであることができ、第2のネットワークは無線ローカル・エリア・ネットワークであることができる。

【0029】

第4の態様では、第1ないし第3の態様のいずれか1つに記載の方法を行なうための手段を含む装置が提供されている。

10

【0030】

第5の態様では、コンピュータ上で実行された場合に第1ないし第3の態様のいずれか1つに記載のステップを行なうためのソフトウェア・コード部分を含む、コンピュータ向けのコンピュータ・プログラム・プロダクトが提供されている。

【0031】

第6の態様では、少なくとも1つのプロセッサと、コンピュータ・プログラム・コードを含む少なくとも1つのメモリとを含む装置において、少なくとも1つのメモリおよびコンピュータ・プログラム・コードは、少なくとも1つのプロセッサを用いて、装置に、少なくとも、ユーザー機器において第1のネットワークからのアクセス情報の受信を制御させ、ここで前記アクセス情報は第2のネットワークに結び付けられ、第1および第2のネットワークは異なる無線アクセス技術を使用し、第2のネットワークと通信状態で前記アクセス情報を使用させる、ように構成されている、装置が提供されている。

20

【0032】

この装置は、第1のネットワークおよび第2のネットワークのうちの少なくとも1つに対して、ユーザー機器識別情報を提供するように構成されることができる。

【0033】

ユーザー機器識別情報は、メディア・アクセス制御アドレス、一時的ユーザー機器アイデンティティ情報および疑似端末アイデンティティ情報のうちの少なくとも1つを含むことができる。

30

【0034】

この装置は、第2のネットワークでの認証プロシージャにおいて前記アクセス情報を使用するように構成されることができる。

【0035】

認証プロシージャは、拡張可能認証プロトコル・プロシージャ、事前共有鍵に基づく認証システム、高速基本サービス・セット遷移スキーム、およびペアワイズ・マスタ鍵に基づく認証システムのうちの少なくとも1つであることができる。

【0036】

前記アクセス情報は、無線ローカル・エリア・ネットワーク・クレデンシャル、疑似端末識別子情報、および一時的ユーザー機器アイデンティティ情報のうちの少なくとも1つを含むことができる。

40

【0037】

第1のネットワークは無線アクセス・ネットワークであることができ、第2のネットワークは無線ローカル・エリア・ネットワークであることができる。

【0038】

第7の態様では、少なくとも1つのプロセッサと、コンピュータ・プログラム・コードを含む少なくとも1つのメモリとを含む装置において、少なくとも1つのメモリおよびコンピュータ・プログラム・コードは、少なくとも1つのプロセッサを用いて、装置に、少なくとも、第1のネットワークによってユーザー機器に対して第2のネットワークに結び付けられたアクセス情報を提供させるように構成されており、ここで前記アクセス情報は

50

第2のネットワークとの通信用であり、前記第1および第2のネットワークは異なる無線アクセス技術を使用する、装置が提供されている。

【0039】

この装置は、第1のネットワークにより、第2のネットワークからのアクセス情報の要求を制御するように構成されることができる。

【0040】

この装置は、第1のネットワークにより、前記アクセス情報を割当て、第2のネットワークに対して前記アクセス情報を提供するように構成されることができる。

【0041】

この装置は、ユーザー機器からユーザー機器識別情報を受信するように構成されることができる。

10

【0042】

ユーザー機器識別情報は、メディア・アクセス制御アドレス、一時的ユーザー機器アイデンティティ情報および疑似端末アイデンティティ情報のうちの少なくとも1つを含むことができる。

【0043】

前記アクセス情報は、無線ローカル・エリア・ネットワーク・クレデンシャル、疑似端末識別子情報、および一時的ユーザー機器アイデンティティ情報のうちの少なくとも1つを含むことができる。

【0044】

第1のネットワークは無線アクセス・ネットワークであり、第2のネットワークは無線ローカル・エリア・ネットワークであることができる。

20

【0045】

第8の態様では、少なくとも1つのプロセッサと、コンピュータ・プログラム・コードを含む少なくとも1つのメモリとを含む装置において、少なくとも1つのメモリおよびコンピュータ・プログラム・コードは、少なくとも1つのプロセッサを用いて、装置に、少なくとも、第2のネットワークにおいて、第2のネットワークと通信するユーザー機器を検出させ、ここで前記ユーザー機器は第1のネットワークで認証され、第1および第2のネットワークは異なる無線アクセス技術を使用しており、第1のネットワークでのユーザー機器認証において使用されるアクセス情報に基づいてユーザー機器が第2のネットワークにアクセスできるようにさせるように構成されている装置が提供されている。

30

【0046】

この装置は、第1のネットワークからのアクセス情報の受信を制御するように構成されることができる、ここで前記アクセス情報は第1のネットワークにより割当てられる。

【0047】

この装置は、第1のネットワークからの要求に応答して、第1のネットワークに対しアクセス情報を提供するように構成されることができる。

【0048】

この装置は、ユーザー機器での認証プロシージャにおいて前記アクセス情報を使用するように構成されることができる。

40

【0049】

この装置は、ユーザー機器からのユーザー機器識別情報の受信を制御するように構成されることができる。

【0050】

ユーザー機器識別情報は、メディア・アクセス制御アドレス、一時的ユーザー機器アイデンティティ情報および疑似端末アイデンティティ情報のうちの少なくとも1つを含むことができる。

【0051】

この装置は、ユーザー機器での認証プロシージャにおいて前記ユーザー機器識別情報を使用するように構成されることができる。

50

【0052】

認証プロシージャは、拡張可能認証プロトコル・プロシージャ、事前共有鍵に基づく認証システム、高速基本サービス・セット遷移スキーム、およびペアワイズ・マスタ鍵に基づく認証システムのうちの少なくとも1つであることができる。

【0053】

前記アクセス情報は、無線ローカル・エリア・ネットワーク・クレデンシャル、疑似端末識別子情報、および一時的ユーザー機器アイデンティティ情報のうちの少なくとも1つを含むことができる。

【0054】

第1のネットワークは無線アクセス・ネットワークであることができ、第2のネットワークは無線ローカル・エリア・ネットワークであることができる。

10

【0055】

第9の態様では、非一時的コンピュータ可読記憶媒体上で具体化されるコンピュータ・プログラムにおいて、プロセスを実行するべくプロセスを制御するためのプログラム・コードを含み、プロセスは、ユーザー機器において、第1のネットワークからのアクセス情報の受信を制御するステップであって、前記アクセス情報は第2のネットワークと結び付けられており、第1および第2のネットワークが異なる無線アクセス技術を使用するステップと、第2のネットワークと通信状態で前記アクセス情報を使用するステップと、を含むコンピュータ・プログラムが提供されている。

20

【0056】

プロセスは、第1のネットワークおよび第2のネットワークのうちの少なくとも1つに対しユーザー機器識別情報を提供するステップを含むことができる。

【0057】

ユーザー機器識別情報は、メディア・アクセス制御アドレス、一時的ユーザー機器アイデンティティ情報および疑似端末アイデンティティ情報のうちの少なくとも1つを含むことができる。

【0058】

プロセスは、第2のネットワークでの認証プロシージャにおいて前記アクセス情報を使用するステップを含むことができる。

【0059】

認証プロシージャは、拡張可能認証プロトコル・プロシージャ、事前共有鍵に基づく認証システム、高速基本サービス・セット遷移スキーム、およびペアワイズ・マスタ鍵に基づく認証システムのうちの少なくとも1つであることができる。

30

【0060】

前記アクセス情報は、無線ローカル・エリア・ネットワーク・クレデンシャル、疑似端末識別子情報、および一時的ユーザー機器アイデンティティ情報のうちの少なくとも1つを含むことができる。

【0061】

第1のネットワークは無線アクセス・ネットワークであることができ、第2のネットワークは無線ローカル・エリア・ネットワークであることができる。

40

【0062】

第10の態様では、非一時的コンピュータ可読記憶媒体上で具体化されるコンピュータ・プログラムにおいて、プロセスを実行するべくプロセスを制御するためのプログラム・コードを含み、該プロセスは、第1のネットワークによってユーザー機器に対して第2のネットワークに結び付けられたアクセス情報を提供するステップを含み、ここで、前記アクセス情報は第2のネットワークとの通信用であり、前記第1および第2のネットワークは異なる無線アクセス技術を使用する、コンピュータ・プログラムが提供されている。

【0063】

プロセスは、第1のネットワークにより、第2のネットワークからのアクセス情報の要求を制御するステップを含むことができる。

50

【0064】

プロセスは、第1のネットワークにより、前記アクセス情報を割当てするステップと、第2のネットワークに対して前記アクセス情報を提供するステップと、を含むことができる。

【0065】

プロセスは、ユーザー機器からユーザー機器識別情報を受信するステップを含むことができる。

【0066】

ユーザー機器識別情報は、メディア・アクセス制御アドレス、一時的ユーザー機器アイデンティティ情報および疑似端末アイデンティティ情報のうちの少なくとも1つを含むことができる。

10

【0067】

前記アクセス情報は、無線ローカル・エリア・ネットワーク・クレデンシャル、疑似端末識別子情報、および一時的ユーザー機器アイデンティティ情報のうちの少なくとも1つを含むことができる。

【0068】

第1のネットワークは無線アクセス・ネットワークであることができ、第2のネットワークは無線ローカル・エリア・ネットワークであることができる。

【0069】

第11の態様では、非一時的コンピュータ可読記憶媒体上で具体化されるコンピュータ・プログラムにおいて、プロセスを実行するべくプロセスを制御するためのプログラム・コードを含み、プロセスは、第2のネットワークにおいて、第2のネットワークと通信するユーザー機器を検出するステップであって、前記ユーザー機器が第1のネットワークで認証され、第1および第2のネットワークが異なる無線アクセス技術を使用しているステップと、第1のネットワークでのユーザー機器認証において使用されるアクセス情報に基づいてユーザー機器が第2のネットワークにアクセスできるようにするステップと、を含む、コンピュータ・プログラムが提供されている。

20

【0070】

該プロセスは、第1のネットワークからのアクセス情報の受信を制御するステップを含むことができ、ここで前記アクセス情報は第1のネットワークにより割当てられている。

30

【0071】

プロセスは、第1のネットワークからの要求に応答して、第1のネットワークに対しアクセス情報を提供するステップを含むことができる。

【0072】

アクセス情報に基づいてユーザー機器が第2のネットワークにアクセスできるようにするステップは、ユーザー機器での認証プロシージャにおいて前記アクセス情報を使用するステップを含むことができる。

【0073】

認証プロシージャは、拡張可能認証プロトコル・プロシージャ、事前共有鍵に基づく認証システム、高速基本サービス・セット遷移スキーム、およびペアワイズ・マスタ鍵に基づく認証システムのうちの少なくとも1つであることができる。

40

【0074】

プロセスは、ユーザー機器からのユーザー機器識別情報の受信を制御するステップを含むことができる。

【0075】

ユーザー機器識別情報は、メディア・アクセス制御アドレス、一時的ユーザー機器アイデンティティ情報および疑似端末アイデンティティ情報のうちの少なくとも1つを含むことができる。

【0076】

アクセス情報に基づいてユーザー機器が第2のネットワークにアクセスできるようにす

50

るステップは、ユーザー機器での認証プロシージャにおいて前記ユーザー機器識別情報を使用するステップを含むことができる。

【0077】

前記アクセス情報は、無線ローカル・エリア・ネットワーク・クレデンシャル、疑似端末識別子情報、および一時的ユーザー機器アイデンティティ情報のうちの少なくとも1つを含むことができる。

【0078】

第1のネットワークは無線アクセス・ネットワークであることができ、第2のネットワークは無線ローカル・エリア・ネットワークであることができる。

【0079】

以上では、多くの異なる実施形態が説明されてきた。上述の実施形態のいずれか2つ以上を組み合わせることによりさらなる実施形態を提供できるということを認識すべきである。

【0080】

ここで単なる一例として、添付図面を参照しながら、実施形態を説明する。

【図面の簡単な説明】

【0081】

【図1】基地局および複数の通信デバイスを含む例示的通信システムの概略図を示す。

【図2】例示的移動体通信デバイスの概略図を示す。

【図3A】UEを認証する方法のいくつかの例示の流れ図を示す。

【図3B】UEを認証する方法のいくつかの例示の流れ図を示す。

【図3C】UEを認証する方法のいくつかの例示の流れ図を示す。

【図4】UEを認証する例示的方法の例示的タイミング図を示す。

【図5】例示的制御装置の概略図を示す。

【図6】UEを認証するための例示的装置を示す。

【図7】UEを認証するための例示的装置を示す。

【図8】UEを認証するための例示的装置を示す。

【発明を実施するための形態】

【0082】

実施例について詳述する前に、記載されている実施例の根本的な技術を理解する上で一助となるように、例証的な図1～2を参照しながら、無線通信システムおよび移動体通信デバイスのいくつかの一般的原理を簡単に説明する。

【0083】

以下の実施形態は単なる一例にすぎない。明細書では、複数の場所において、「1つの(anまたはone)」または「いくつかの(some)」実施形態について言及されている場合があるが、これは必ずしも、このような言及の各々が同じ実施形態に対するものであること、あるいは特徴が単独の実施形態のみにあてはまることを意味するわけではない。異なる実施形態の単独の特徴を組合せて他の実施形態を提供することもできる。さらに「含む、備える(comprising)」および「含む(including)」なる用語は、説明された実施形態を、記載されたこれらの特徴のみで構成されるように限定するものとして理解されるべきではなく、このような実施形態は同様に、具体的に記載されていない特徴、構造、ユニット、モジュールなども含むことができる。

【0084】

例えば図1に示されているもののような無線通信システム100において、移動体通信デバイスまたはユーザー機器(UE)102、104、105には、少なくとも1つの基地局または類似の無線伝送および/または受信ノードまたはポイントを介した無線アクセスが提供されている。基地局は典型的に、基地局の動作および基地局と通信状態にある移動体通信デバイスの管理を可能にするため、少なくとも1つの適切なコントローラ装置によって制御される。コントローラ装置を、無線アクセス・ネットワーク(例えば無線通信システム100)内またはコア・ネットワーク(図示せず)内に位置設定し、1つの中央

10

20

30

40

50

装置として実装することができ、あるいは複数の装置全体にわたりその機能性を分散させることもできる。コントローラ装置は、基地局の一部であり得、および／または無線ネットワークコントローラなどの別個のエンティティによりこの装置を提供することができる。図1において、制御装置108および109は、それぞれのマクロ・レベルの基地局106および107を制御するものとして示されている。基地局の制御装置は、他の制御エンティティと相互接続できる。制御装置には、典型的に、メモリ容量および少なくとも1つのデータ・プロセッサが備えられる。制御装置および制御機能は、複数の制御ユニット間に分散させることができる。いくつかのシステムでは、制御装置を、付加的にまたは代替的に、無線ネットワークコントローラ内に備えることができる。制御装置は、図5に関連して論述されるものなどの装置を提供することができる。

10

【0085】

しかしながら、LTEシステムを、RNCを備えることなく、いわゆる「フラット」アーキテクチャを有するものとして考慮することができる。むしろ、(e)NBは、コア・ネットワークすなわちシステム・アーキテクチャ・エボリューション・ゲートウェイ(SAE-GW)および移動性管理エンティティ(MME)と直接通信状態にあり、これらのエンティティをプールすることもでき、この事実は、複数のこれらのノードが複数の(1組の)(e)NBにサービス提供することができるということを意味している。各UEは、一度に1つのMMEおよび／またはS-GWのみからサービスの提供を受け、(e)NBは、現行の結びつきを追跡する。SAE-GWは、S-GWおよびP-GW(それぞれゲートウェイおよびパケット・データ・ネットワーク・ゲートウェイにサービス提供する)で構成され得るLTE内の「高レベル」ユーザー・プレーン・コア・ネットワーク要素である。S-GWおよびP-GWの機能性は分離され、コロケートされるようには求められない。

20

【0086】

図1において、基地局またはノード106および107は、ゲートウェイ112を介してより広域の通信ネットワークに接続されている状態で示されている。別のネットワークに接続するために、さらなるゲートウェイ機能を提供することができる。

【0087】

例えば別個のゲートウェイ機能によっておよび／またはマクロ・レベル局のコントローラを介して、ネットワーク113に対して、より小さい基地局またはノード(アクセス・ノード、AP)116、118および120を接続することもできる。基地局116、118および120は、ピコまたはフェムト・レベルの基地局などであり得る。実施例中、局116および118は、ゲートウェイ111を介して接続され、一方局120はコントローラ装置108を介して接続している。いくつかの実施形態において、より小さい局は備えられない可能性がある。

30

【0088】

しかしながら、実施形態は、一例として与えられているシステムに限定されず、当業者であれば、必要な特性を備えた他の通信システムに対し該ソリューションを応用することができる。好適な通信システムの別の例は、5Gコンセプトである。5G内のネットワーク・アーキテクチャは、LTE-アドバンスドのものとかかなり類似するものと仮定される。5Gは、より小さい局と協働して動作し、おそらくは同様により優れたカバレッジおよび強化されたデータ・レートのために多様な無線技術をも利用するマクロ・サイトを含め、多重入出力(MIMO)アンテナ、LTE(いわゆる小セル・コンセプト)よりもさらに多くの基地局またはノードを使用する確率が高い。

40

【0089】

将来のネットワークは、共に動作的に接続またはリンクされてサービスを提供することのできる「ビルディング・ブロック」またはエンティティの形へとネットワーク・ノード機能を仮想化することを提案するネットワーク・アーキテクチャ・コンセプトであるネットワーク機能仮想化(NFV)を使用する可能性が最も高い。仮想化ネットワーク機能(VNF)は、カスタマイズされたハードウェアの代りに標準的または一般的タイプのサー

50

バーを用いるコンピュータ・プログラム・コードを実行する1つ以上の仮想マシンを含むことができる。クラウド・コンピューティングまたはデータ記憶も同様に利用可能である。無線通信においては、これは、遠隔無線ヘッドに動作的に結合されたサーバー、ホストまたはノード内で少なくとも部分的にノード・動作が実施されることを意味することができる。ノード・動作が複数のサーバー、ノードまたはホストの間で分配されることも同様に可能である。同様に、コア・ネットワークの動作と基地局の動作の間での労働分散がLTEのものとは異なり、さらには存在しない可能性があるということも理解すべきである。

【0090】

ここで、通信デバイス200の部分的に切断された概略的な図を示す図2を参照しながら、考えられる移動体通信デバイスについて説明する。このような通信デバイスは多くの場合、ユーザー機器(UE)または端末と呼ばれる。適切な移動体通信デバイスは、無線信号を送信し受信することのできるあらゆるデバイスによって提供されることができる。非限定的な例としては、移動局(MS)または移動体デバイス、例えば携帯電話または「スマート・ホン」として知られているもの、無線インターフェースまたは他の無線インターフェース設備(例えばUSB dongle)を備えるコンピュータ、無線通信能力を備えたパーソナル・データ・アシスタント(PDA)またはタブレット(ラップトップ・コンピュータ、タッチスクリーン・コンピュータ)、またはこれらの任意の組合せなどが含まれる。ユーザー・デバイス(UE)のいくつかの他の例は、ゲーム・コンソール、ノート型パソコン、マルチメディア・デバイスおよび無線モデムを用いるデバイス(アラームまたは測定デバイスなど)である。移動体通信デバイスは、例えば、音声、電子メール(Eメール)、テキスト・メッセージ、マルチメディアなどの通信を搬送するためのデータ通信を提供することができる。こうしてユーザーは、自らの通信デバイスを介して多くのサービスのオフターおよび提供を受けることができる。これらのサービスの非限定的例としては、双方向または多方向呼出し、データ通信またはマルチメディア・サービスまたは単にインターネットなどのデータ通信ネットワークシステムへのアクセスが含まれる。ユーザーは同様に、ブロードキャストまたはマルチキャスト・データの提供を受けることもできる。コンテンツの非限定的例には、ダウンロード、テレビおよびラジオ番組、ビデオ、広告、さまざまな警報および他の情報が含まれる。

【0091】

移動体デバイス200は、受信のための適切な装置を介してエアまたは無線インターフェース207上で信号を受信でき、無線信号を伝送するための適切な装置を介して信号を伝送することができる。図2中、送受信機装置は、ブロック206によって概略的に示されている。送受信機装置206は、例えば、無線部品および付随するアンテナ配列を用いて提供することができる。アンテナ配列は、移動体デバイスの内部または外部に配置することができる。

【0092】

移動体デバイスには典型的に、少なくとも1つのデータ処理エンティティ201、少なくとも1つのメモリ202および、アクセス・システムおよび他の通信デバイスへのアクセスおよび通信の制御を含めた、この移動体デバイスが実施するように設計されているタスクのソフトウェアおよびハードウェアにより支援された実行において使用するための他の考えられるコンポーネント203が備えられている。データ処理、記憶および他の関連する制御用の装置は、適切な回路板上および／またはチップセット内に備えることができる。この特徴は、参照番号204によって示されている。ユーザーは、キーパッド205、音声コマンド、タッチ・センシティブ・スクリーンまたはパッド、それらの組合せなどの好適なユーザー・インターフェースを用いて、移動体デバイスの動作を制御することができる。ディスプレイ208、スピーカーおよびマイクロホンも備えることができる。さらに、移動体通信デバイスは、他のデバイスに対するおよび／または例えばハンドフリー機器などの外部付属備品を接続するための適切なコネクタ(有線または無線)を含むことができる。

【0093】

通信デバイス102、104、105は、さまざまなアクセス技術、例えば符号分割多元接続（CDMA）、または広帯域CDMA（WCDMA（登録商標））に基づいて通信システムにアクセスできる。他の非限定的例には、時分割多元接続（TDMA）、周波数分割多元接続（FDMA）およびそのさまざまなスキーム、例えばインターリーブ周波数分割多元接続（IFDMA）、シングル・キャリア周波数分割多元接続（SC-FDMA）および直交周波数分割多元接続（OFDMA）、空間分割多元接続（SDMA）などが含まれる。

【0094】

無線通信システムの一例は、第3世代パートナーシップ・プロジェクト（3GPP）によって標準化されたアーキテクチャである。最新の3GPPに基づく開発は、多くの場合、ユニバーサル移動体通信システム（UMTS）無線アクセス技術のロング・ターム・エボリューション（LTE）と呼ばれる。3GPP仕様のさまざまな開発段階は、リリースと呼ばれている。LTEの最新の開発は、多くの場合、LTEアドバンスド（LTE-A）と呼ばれている。LTEは、進化型ユニバーサル地上無線アクセス・ネットワーク（E-UTRAN）として知られる移動体アーキテクチャを用いる。このようなシステムの基地局は、進化型または強化型のノードBs（eNBs）として知られ、通信デバイスに向かうユーザー・プレーン・無線リンク制御／メディア・アクセス制御／物理層プロトコル（RLC／MAC／PHY）および制御プレーン無線リソース制御（RRC）プロトコル終端などのE-UTRANフィーチャを提供する。無線アクセス・システムの他の例としては、無線ローカル・エリア・ネットワーク（WLAN）および／またはWiMax（Worldwide interoperability for microwave access）などの技術に基づくシステムの基地局によって提供されるものが含まれる。

【0095】

3GPPは、LTEおよび3Gなどの移動体無線アクセス技術を標準化したが、一方WLAN移動体無線アクセスは、IEEE標準802.11に基づいている。UEは、少なくとも1つの3GPP RATならびにWLAN無線インターフェースを備えることができる。WLANアクセス・ポイントはユーザー展開され得、アンライセンス・スペクトル内で動作し、一方3GPP基地局およびUEは事業者が所有でき、ライセンス・スペクトルを使用することができる。近年、事業者はWLAN APも展開し始め、WLANおよび3GPPネットワーク間に提供される能力の間のより良い協調を探求している。3GPPは、LTE-Uとして知られているイニシアチブであるライセンス・スペクトルを使用できるが、LTEのための正式なライセンス補助アクセス（LAA）には、WLANによっても使用されるアンライセンス・スペクトルの使用が関与している。

【0096】

WLANレグは、アンライセンスLTEの使用と同様に、UEとアクセス・ネットワークの間の二次的無線ベアラとしてセットアップすることができる。進化型パケット・システム（EPS）自体はWLANを認識していない場合がある。WLANは、あたかも元来LTEレグを介して送出されたかのようにUEとeNBの間でLTEユーザー・プレーン・パケットを搬送することができる（例えば課金の削減を目的として、EPSに対してWLAN標示を提供することができる）。UEは、エンドアプリケーションに対する送出の前に2つのインターフェースからのダウンリンク・ペイロードを組合せることができる。UEは同様に、アプリケーションが認識することなくいずれかのインターフェースを介してアップリンク・データを送出することもできる。eNB S1インターフェースは、ネットワーク側でアンカー・ポイントとして作用できる。このプロセスは、タイト・インターワーキングとして知られている可能性がある。

【0097】

RANなる用語は、無線リソース制御（RRC）機能性が存在する任意の3GPP無線アクセス・ネットワーク・エンティティを表わすために使用される。LTEにおいて、これは、eNBノードであることができ、一方WCDMAでは、それはRANノード（No

ニズムは、認証および認証のためのEAP-SIM/AKA/AKA-Primeの使用を含み、したがって、ホームHSSサーバー内で発生する。これは、高速アクセスを達成しWLANをRAN内部に保つためには望ましくない可能性がある。十分にセキュアかつロバストであることを仮定して、他の認証メカニズム、例えば証明書に基づくEAP-TLSまたは保護されたユーザー名とパスワード（十分に複雑である必要がある）に基づくEAP-PEAPを使用することができる。

【0103】

1つの代替的ソリューションでは、WLANを用いてWLAN無線上でWPA2セキュリティをセットアップするために使用されるべき永久的／一時的／一回限りのWPA2事前共有鍵（PSK）セキュリティ鍵またはペアワイズ・マスタ鍵（PMK）などの、UE 10に対する3GPP無線上での交換が導入される。UEは、RANに対してそのメディア・アクセス制御（MAC）アドレスを提供し、RANはWLANと使用すべきPSKまたはPMKについてネゴシエートする。

【0104】

PSK/PMK交換の結果、UEおよびWLANは両方共、802.11仕様書中に規定されているペアワイズ・マスタ鍵・セキュリティ・アソシエーション（PMKSA）をセットアップすることができる。PMKSAコンテキストは通常、EPA認証の成功の結果として、またはPSKから作成される。主要なコンポーネントは、MACアドレスおよびPMKである。

【0105】

PSKの場合、PMKは、UEおよびWLANにより局所的にPSKから導出される。UEおよびWLANは、同じPMKSAを使用できる場合、セキュアな通信を行うことができる。

【0106】

通常、EAP認証において、PMKは、UEおよびホーム認証サーバー（AAA/HSS）が知っているEAP認証鍵から導出される。これはスキップ可能であり、鍵をRAN内で局所的に作成することができる。

【0107】

これらのメカニズムの両方において、セキュリティ・アソシエーションを作成するのに必要とされる本質的に全ての情報は、セキュアなUE/RAN接続およびRAN/WLAN 30接続を介して、UE、RANおよびWLAN間で交換される。このようにして、UEは、WLAN内でEAP認証プロシーダを完全にスキップし、セキュリティ鍵の知識を証明するために直接802.11に規定された4ウェイ・ハンドシェイクを使用して、WLANおよびRANがオフロード・シナリオを識別できるようにすることができる。

【0108】

最初に802.11rにおいて導入され802.11-2012仕様書に内含された高速BSS（基地局サブシステム）遷移は、UEが2つのWLAN AP間でのハンドオーバーを行なっているときに後続する認証段階を回避するためのメカニズムを定義する。この方法は、単一のWLANネットワーク内でのみ適用可能である。ターゲットおよびソースWLAN APは、PMKから導出された特定のセキュリティ鍵を交換し、UEが完全 40な認証無くWLANセッションを再確立できるようにする。802.11は、これらの鍵がAP間でどのように交換されるかについて規定していない。典型的には、これは、同じWLANコントローラによって2つのAP'が管理されている場合にサポートされる。1つのオプションとして、これは、3GPPアグリゲーションをカバーするために拡張可能である。RANは、ここでソースWLAN APの役割を担い、UEを準備し、高速BSS移行のためにWLANをターゲティングすることができる。

【0109】

PMKSA交換ではなく、正規のローカルEAPに基づくまたはPSKメカニズムを使用することの主たる動機は、既存のWLAN設備との互換性にある。新しいWLAN HWさらにはSWの修正は全く必要とされない。それは、単に構成を介して、ネットワーク 50

サイドで実装され得る。ローカル A A A サーバーを導入することにより、ネットワークサイドで R A N における修正だけが必要になる。R A N は、A A A システムが典型的に有する既存の構成インターフェースを介して、A A A サーバーを構成できると考えられる。L T E チップが R A N コマンドにしたがって U E のための W L A N 設定値を構成しなければならないことから、U E には適応が必要となる。P M S K A 転送または高速 B S S 遷移に基づくメカニズムは、いくつかの状況下で、より速い接続時間を提供することができるが、W L A N チップレベルおよび U E (ソフトウェア/ハードウェア) S W / H W 実装まで深く進んで、しかも直ちに利用可能でない。

【0110】

P T I D コンセプトを進化させて、ローカル R A N 制御型認証を導入することができる。図 3 A は、W L A N 内で U E を認証する方法の一実施例を示し、ここで W L A N は二次的無線ベアラとして使用されるようになっている。この方法は、ブロック 900 において、ユーザー機器において、第 1 のネットワークからのアクセス情報の受信を制御するステップであって、前記アクセス情報は第 2 のネットワークと結び付けられており、第 1 および第 2 のネットワークが異なる無線アクセス技術を使用するステップを含む。ブロック 902 において、この方法は、第 2 のネットワークと通信状態で前記アクセス情報を使用するステップを含んでいる。

【0111】

図 3 B は、別の実施形態に係る U E の認証方法の一実施例を示す。この方法は、ステップ 1000 において、第 1 のネットワークによってユーザー機器に対して第 2 のネットワークに結び付けられたアクセス情報を提供し、ここで前記アクセス情報が第 2 のネットワークとの通信用であり、前記第 1 および第 2 のネットワークが異なる無線アクセス技術を使用することを含む。

【0112】

図 3 C は、別の実施形態に係る U E の認証方法の一実施例を示す。この方法は、第 1 のステップ 1100 において、第 2 のネットワークで、第 2 のネットワークと通信するユーザー機器を検出し、ここで前記ユーザー機器が第 1 のネットワークで認証され、第 1 および第 2 のネットワークが異なる無線アクセス技術を使用していることを含む。第 2 のステップにおいて、この方法は、第 1 のネットワークでのユーザー機器認証において使用されるアクセス情報に基づいてユーザー機器が第 2 のネットワークにアクセスできるようにすることを含む。

【0113】

無線アクセス技術は、ロング・ターム・エボリューション (L T E)、ロング・ターム・エボリューション・アドバンスド (L T E - A)、無線ローカル・エリア・ネットワーク (W L A N または W i F i)、マイクロ波アクセスのための世界的な相互運用性 (W i M A X)、B l u e t o o t h (登録商標)、パーソナル・コミュニケーションズ・サービス (P C S)、Z i g B e e (登録商標)、広帯域符号分割多元接続 (W C D M A)、超広帯域 (U W B) 技術を使用するシステム、センサー・ネットワークおよび移動体アドホック・ネットワーク (M A N E T) を含むことができる。上述の方法において、第 1 のネットワークは R A N であることができ、第 2 のネットワークは W L A N であることができる。

【0114】

本願方法の一実施形態は、第 1 のネットワークおよび/または第 2 のネットワークに U E 識別情報を提供するステップ、例えば e N B に U E 識別情報を提供するステップを含むことができる。ユーザー機器識別情報は、メディア・アクセス制御アドレス、一時的ユーザー機器アイデンティティ情報および疑似端末アイデンティティ情報のうちの少なくとも 1 つを含むことができる。一時的ユーザー機器アイデンティティ情報および疑似端末アイデンティティ情報を、第 1 のネットワークにおいて割当てし、第 2 のネットワークに対して提供するために U E に提供することができる。一時的ユーザー機器アイデンティティ情報は同様に、第 2 のネットワークから第 1 のネットワークにより要求され、第 1 のネット

10

20

30

40

50

ワークを介してU Eに提供されることもできる。

【0115】

アクセス情報は、第2のネットワーク内で、暗号化、認証および認可のために使用されるべきクレデンシャルを含むことができる。アクセス情報は、共通のアイデンティティを確立するため第1のネットワークと第2のネットワークの間で交換されるべきシークレットおよびユーザー名を含むことができる。このユーザー名には、特定の領域がアタッチされ得る。この領域は、概して、オフロードまたはアグリゲーション使用と結び付けられるかまたは局所的にそれが割当てられたR A N / W L A N内にあるかのいずれかであるものとして知られている。

【0116】

アクセス情報は、W L A N認証クレデンシャル、例えばW L A N提供シークレット、W L A N識別情報、R A N割当てされた一時的U Eアイデンティティ、例えばP T I D、W L A Nネットワーク・アイデンティティ、例えばM A CアドレスまたはS S I D、事前共有キー（P S K）、ペアワイズ・マスタ鍵（P M C）などを含むことができる。

【0117】

アクセス情報は、例えばR A N、インターフェースなどの第1のネットワーク上でU Eに送出されることができる。

【0118】

アクセス情報は、第2のネットワークでの認証プロシージャにおいて使用可能である。例えば、アクセス情報は、拡張可能認証プロトコル・プロシージャ、事前共有鍵（P S K）に基づく認証システム、高速基本サービス・セット遷移スキームおよびペアワイズ・マスタ鍵（P M K）に基づく認証システムのうちのいずれか1つにおいて使用可能である。

【0119】

一実施形態において、本願方法は、第1のネットワークによってユーザー機器に対して第2のネットワークに結び付けられたアクセス情報を提供するステップであって、前記アクセス情報が第2のネットワークとの通信用であり、前記第1および第2のネットワークが異なる無線アクセス技術を使用するステップを含む。

【0120】

一実施形態において、本願方法は、第2のネットワークにおいて、第2のネットワークと通信するユーザー機器を検出するステップであって、前記ユーザー機器が第1のネットワークで認証され、第1および第2のネットワークが異なる無線アクセス技術を使用しているステップと、第1のネットワークでのユーザー機器認証において使用されるアクセス情報に基づいてユーザー機器が第2のネットワークにアクセスできるようにするステップと、を含む。

【0121】

この方法は、第1のネットワークにより、第2のネットワークからのアクセス情報の要求を制御するステップを含むことができる。代替的にまたは付加的に、この方法は、第1のネットワークにより、前記アクセス情報を割当てるステップと、第2のネットワークに対して前記アクセス情報を提供するステップと、を含むことができる。

【0122】

例えば、E A P - T T L S（トンネル型トランスポート層セキュリティ）、E A P - P E A P（保護型拡張可能認証プロトコル）または、例えばプレーン・テキスト・ユーザー名、サーバー証明書およびディフィー・ヘルマン交換を用いる公開鍵暗号法に基づいてW L A NでセキュアなチャネルをU Eがセットアップできるようにする他の任意の好適なE A P方法を使用して、W L A Nセキュリティを確立することができる。一つの実施例において、ひとたびセキュアなチャネルが確立されたならば、ユーザー名およびシークレットとのM S - C H A P V 2（マイクロソフト・チャレンジャーハンドシェイク認証プロトコル）交換をセキュアなチャネル内で実行して、ユーザーのアイデンティティを証明することができる。すなわち、オペレータのA A Aマシン類に達することなく、第2のネットワークまたはW L A N内で局所的に、E A P認証を実行することができる。

10

20

30

40

50

【0123】

アクセス情報は、レガシーWLAN 802.1x認証のための好適なEAPクレデンシャルを含むことができる。これらのクレデンシャルは、RANノードによって管理されることができる。クレデンシャルは、UEに対してと同時にWLANオフロード／アグリゲーションのためにWLANに対しても提供されることができる。最も単純な形態では、UEによりWLANに提供されるクレデンシャルを認証するAAAサーバーが存在する。RANは、このAAAサーバーにより使用されたクレデンシャルを維持する。クレデンシャルは、user@realmの形のユーザー名およびパスワードを含むことができる。UEは、例えば、EAP-TTLS/MSC hap V2認証メカニズムを用いて認証することができる。領域コンポーネントは、AAAサーバーを位置特定するために使用されることが考えられる。RANは、これらのクレデンシャルを管理できることから、RANは、実際、WLAN内でUEの寿命を制御することができる。RANは同様に、AAAの役割を担い、WLANの使用全体を局所的に管理することもできる。これは、WLANネットワークエンティティのための何らかの新規の開発を必要とせず、現在のWLANネットワークと互換性があると考えられる。クレデンシャルは、WLANに対してUEを識別する。

10

【0124】

事前共有キー（PSK）に基づく認証メカニズムでは、RANは、ユーザーのためにPSKキーを管理する。PSKは、PSK認証のためのサポートをブロードキャストするWLANネットワーク内で使用され得る。RANは、各々の認可されたUEについて専用PSKを割当て、それをUE MACアドレスと結び付けることができる。RANは、認可された[UE__MAC、PSK]タブルをWLANに標示でき、同様にそれが有する可能性のあるWLANオフロード／アグリゲーションポリシーにしたがってWLAN内のこのタブルの寿命を管理することもできる。

20

【0125】

共有PSKも同様に使用可能である。この場合、最終的に全てのデバイスは、潜在的に最終的にPSKを学習することができ、UE MACアドレスだけに基づいて認可を行なうことができる。このモードは、すでにいくつかのWLANネットワークによってサポートされている。RANは、WLANノード内（WLAN AP／WLANコントローラ／AAAサーバーのうちの1つ）でこれらのMACアドレスを管理する必要がある場合がある。WLANネットワークは、唯一つの共有PSKをサポートでき、このメカニズムは、ユーザーの特定のPSK値を必要とする可能性がある。

30

【0126】

ペアワイズ・マスタ鍵（PMK）に基づく認証も使用することができる。これは、EAP認証のためのサポートを標示するWLANネットワーク内で利用可能である。通常、PMKは、交換されたデータから、またはSIMカードなどのローカル鍵生成ソースからのEAP認証の成功後に、UEおよびAAAサーバー内で局所的に生成され、UEおよびAAAサーバーは両方共、同じ鍵を生成することができる。AAAサーバーは、UEとのセキュアな通信をセットアップするため、WLANネットワークに対して（アップリンク）ULおよび（ダウンリンク）DL鍵を提供する。ひとたびUEがPMKを学習したならば、UEは、WLANネットワークにこの鍵を使用する意思があるかぎり、このPMKを用いて同じAPとの後続するWLAN接続を確立することができる。PSKは、PMKの1つの形態である。RANが、UEおよびWLANネットワークのためにこれらのPMK鍵を管理し、UEおよびWLANネットワークに対し鍵を提供する場合には、UEは、EAP認証プロシーダをスキップし、APとのいわゆる4ウェイ・ハンドシェークを実行することにより、キーのオーナーシップを確認することができる。ハンドシェークは、両方向でPMK由来のキーを使用し、両方のエンドポイントは、ピアが正しいキーを有することを確認することができる。PMKキーは、UEおよびWLANの両方共がEAP認証の成功後に作成するペアワイズ・マスタ鍵セキュリティ・アソシエーション（PMKSA）内に記憶可能である。PMKSAは、この場合RAN入力に基づいて作成され得る。

40

【0127】

50

図3の方法などの方法は、RANおよびWLANがRANドメイン内部でWLAN認証を保ち、ホームAAAまたはHSSサーバーを関与させないようにすることを可能にする。RANは、WLANの使用に対する全面的な制御を再開することができる。

【0128】

所望される場合には、任意の公開WLANアクセスのために、同じWLANネットワークを使用することができる。オフロード・トラヒックは、(ユーザー・アイデンティティ内の領域に基づいて) WLAN内で容易に識別され、相応してハンドリングされることができる。

【0129】

WLANレグは二次的ベアラであり、既存のLTEベアラの次に作成され得ることから、WLANからのクレデンシャルを要求するために、UEとRANの間でLTE(無線リソース制御)RRCシグナリングを使用することができる。RANとUEの間では、RRCプロトコルが使用される。コロケートされた場合には、WLAN/3GPP無線コントローラは単一のエンティティであることができるため、クレデンシャルを提供するために、RRCシグナリングを使用することができる。一般的なケースでは、WLANとLTEは、好適なプロトコルを介して通信できるが、RRCはUEに対し値を送出することができると考えられる。

【0130】

1つのオプションとして、UEは、アクティブ・モードにない(および進行中のデータ伝送を有する)場合でさえ、第1のネットワークから、第2のネットワークと結び付けられたアクセス情報、例えば3GPP RANからのWLANクレデンシャルを受信することができる。例えば、3GPP/WLANインターワーキング・メッセージング(3GPPリリース12へと規格化されたもの)の一部として、UEは、(例えば認証を最適化しコア・ネットワーク・シグナリングを削減するために)方法にしたがって使用されるべきWLANクレデンシャルを受信することができる。

【0131】

以上で説明され図3の流れ図中に示された方法などの方法は、ベアラ確立、例えばLTEベアラ確立中に行なうことができる。

【0132】

この例では、LTEベアラの確立中に、UEはLTEデフォルト・ベアラを確立することができる。このベアラ・セットアップは、WLANアグリゲーションベアラをセットアップするためのeNBからの標示を含むことができ、および/またはUEはeNBから同じことを行なう許可を要求することができる。UEは、プロシージャの一部として、WLAN識別子、例えばWLAN MACアドレスをeNBに対し提供することができる。代替的には、WLANアグリゲーションをセットアップするための別個の専用シグナリングが存在し得る。eNBは、WLANと通信し、WLANオフロードのための一時的クレデンシャル(例えばユーザー名+シークレット)の形でアクセス情報を要求することができる。一代替案として、eNBは、アクセス情報、例えばクレデンシャルを作成するかまたは割当てし、WLANに対してアクセス情報を提供することができる(これには、例えばSIMの無いデバイス用にWLANが作成したクレデンシャルとの衝突を回避するために例えば3GPPレンジなどの使用が必要となる可能性がある)。代替的には、クレデンシャルは、RANおよびWLANにとってアクセス可能であり(例えばユーザー名内の領域を介して)作成されたクレデンシャルによって識別され得る外部ネットワーク要素の中で作成可能である。例えば、LDAPおよびAAAサーバーは、協働してクレデンシャルまたはHSSを作成することができると考えられる。

【0133】

UEに対しクレデンシャルを提供することができる。UEは、UEに提供されたクレデンシャルを用いてWLANでの適切なEAP認証を実行することができる。EAP認証は、例えば、EAP-TTLS/MSCHAPV2パッケージ・ソフトであることができる。WLANは、領域を認識し、WLANで局所的にUEを認証する。UEは、WLAN接

10

20

30

40

50

続のためにDHCPを用いてIPを要求することができる。WLANは、LTEベアラに要求を結び付け、LTEベアラ上で使用されるものと同じIPアドレスを提供するかまたは、何らかのトンネリングメカニズムがWLANレグ上で使用される場合にはWLANレグに対してLTEベアラを内部的に結び付けることができる。eNBは、同じS1エンドポイントでWLANおよびLTEレグの両方を使用できる場合がある。

【0134】

代替的には、eNBは、進行中である通信の間にUEをMLANへ移動させる決定を下すことができ、こうして、この方法は、ベアラ確立の外で実施することができる。図4は、第1のネットワーク、LTE-Aおよび第2のネットワーク、WLANとUEとの接続のための第1のネットワーク内のメッセージの流れを示す。UEがLTEで進行中の通信を有するかまたはLTE通信のための無線リソースを確立した場合、UEはLTE認証され得る。

10

【0135】

上述された方法と組合せて使用可能な認証プロシージャの一例は、以下のステップを含む。UEがeNBに接続する。任意には、eNBはUEに対して監視すべきWLANネットワークを標示することができる。同様に、UEは、監視されたWLANネットワークからの信号品質レポートを標示することができる。eNBがローカルWLANノードとのWLANアグリゲーションをセットアップすることを決定した場合、eNBは、ユーザーのためのMSChapV2クレデンシャル（ユーザー名、パスワード）を準備し、それらをローカルAAAサーバーにインストールする。ユーザー名は、user@realmの形態のものである。AAAサーバーは、WLANのためのユーザー名の領域部分によって識別可能である。eNBは、UEに対するアグリゲーションを指令し、割振られたクレデンシャルおよびWLANネットワーク・アイデンティティ（一例としてMACアドレス、SSID（BSSサービスID））をUEに提供する。UEはWLANネットワークと結びつき、EAP-TTLS/MSChapV2を用いて認証する。WLANネットワークは、EAP認証メッセージを、ユーザー名の領域部分により識別されたAAAサーバーに伝播させる。このAAAサーバーはユーザー認証のためにeNBが管理するユーザークレデンシャルを使用することから、eNBは、認証プロセスを制御しアクセスを認可することができる。AAAは、UEとのEAP認証を完了し、WLANネットワークに対してPMKを提供する。UEは、同じPMKを局所的に導出する。eNBとのUE通信は、ここで、潜在的にeNBおよびWLANレグの両方を介してキャリア・オーバーされる。eNBはAAAサーバー内でユーザーを管理することから、いつでもユーザーをWLANから除去しUEをeNBに強制的に戻すことができる。

20

30

【0136】

1つのオプションとして、RANは、直接またはMMEを介して、EAM-SIM/AKA/AKA'認証の一部として使用されるべきWLANネットワークに対するチャレンジと期待レスポンスを提供する。例えば、HSSには、UEが3G/LTEネットワーク内で認証された時点で多数のチャレンジ・レスポンス対を提供することが求められる。こうして、3G/LTEネットワークは、未使用のチャレンジおよびレスポンスを有する。3G/LTEは、WLANネットワークが特定のユーザー/UEのために正しいクレデンシャルを使用できるようにするUE/ユーザー・アイデンティティと共に、HSSを関与させることなく選択されたUEのために、(U)SIMに基づく認証をWLANネットワークが実行できるようにする1セットをWLANネットワークに提供することができる。

40

【0137】

一実施形態においては、RANがWLANを使用する（LTE+WLANまたはUEをWLANに移動させる）ことを決定した場合、RANは、WLANに対し、WLAN内のセキュアな接続確立を可能にするUE用のシークレットを提供するよう要求することができる。RANは、WLANにユーザー/UEアイデンティティを共有させることができる。Wi-FiネットワークにアクセスするときにUEが自らを識別する例示的アイデンティティは、RAN割当てされた一時的アイデンティティ（例えばPTID）またはMA

50

Cアドレスである。

【0138】

RANは、例えばRAN割当てされた一時的ユーザー／UEアイデンティティ、例えばPTID、WLAN（提供）シークレット、WLANアクセスにおいて使用されるべきIPアドレス、QoS関連情報、例えばWLAN上の既存の接続を継続する場合にWi-Fiアクセス内で使用されるべきディフサーブ・コード・ポイント（DSCP）マーキングなどのWLANアクセス関連情報をUEに対し通信することができる。UEは、WLANに接続することができる。

【0139】

UEは、例えば、アクセス・ネットワーク・クエリ・プロトコル（ANQP）のクエリ、WLAN管理プロシージャまたはアクセス・ポイント（AP）プローブなどをトリガーすることができる。UEからAPへのメッセージは、一時的RAN割当てユーザー／UEアイデンティティを内含するように拡張可能である。

【0140】

UEに対するWLAN AP応答の後（応答が期待されている場合）、WLAN APは、UEに対してNon-Valueを送信することによりUEとのセキュアな接続の樹立を開始することができる。この時点で、WLAN APは、すでにユーザー・シークレットとユーザー／UE一時的アイデンティティを結び付けている。

【0141】

UEおよびWLAN APは、シークレットを用いて、802.11iにしたがってセキュアな接続をセットアップするためにメッセージを交換することができる。有効な一時的アイデンティティおよびシークレットを有するUEのみが、セキュアな無線接続を正しくセットアップすることができる。シークレットおよび一時的アイデンティティは例えばRRCメッセージ内で転送されたことから、別のUEがそれを行なう可能性は、全く存在しないか、極めて低いものである。

【0142】

WLANでのeNBアグリゲーションのための認証プロシージャの一例は、以下のステップを含むことができる。UEはeNBに接続し、独自のMACアドレスを提供する。任意には、eNBはUEに対して、監視すべきWLANネットワークを標示することができる。同様に、UEは、監視されたWLANネットワークからの信号品質レポートを標示することができる。eNBがローカルWLANノードとのWLANアグリゲーションをセットアップすることを決定した場合、eNBは、UE MACと共にWLANのためのPMK（UL／DL）を準備する。WLANは、このUL PMKを用いてUEアクセスを受入れるように準備される。DLでは、DL PMKが使用される。eNBは、UEに対するアグリゲーションを指令し、PMKおよびWLANネットワーク・アイデンティティ（一例としてMACアドレス、SSID）をUEに提供する。UEは、WLANネットワークと結びつき、提供されたPMKを用いてセキュアな接続をセットアップする。WLANは、MACアドレスに基づいてUEを識別することができ、セッションに正しいPMKを適用することができる。EAP認証は、スキップされ得る。ここでeNBとのUE通信は、潜在的に、eNBおよびWLANレグの両方を介してキャリア・オーバーされる。eNBはPMKを管理することから、いつでもWLANからPMKを削除し、UEをeNBに強制的に戻すことができる。

【0143】

この場合、UEはここで、通常の認証またはいずれかのEAPメッセージを実行することなく、WLANにアクセスすることができる。接続確立は、RANおよびWLANメッセージングのみを使用し、802.11iメッセージに加えてわずかなメッセージしか必要としない。Wi-Fiネットワーク機能は、RANがLTEおよびWi-Fiレグを同じユーザー／UEに結び付けることができるようにするため、ユーザー／UE一時的アイデンティティを使用することができる。

【0144】

10

20

30

40

50

RANが（インターネット・プロトコル）IPアドレスをUEに提供する場合、UEはDHCPプロシーダをスキップし、割振られたIPアドレスの使用を開始することができる。

【0145】

RANがクオリティ・オブ・サービス（QoS）、DSCPマーキング（または類似するQoS）ディテールをUEに提供する場合には、UEは、例えばWLAN内のトラヒック優先順位付け／QoSメカニズムを可能にするため、相応してアップリンク・パケットを開始するものとする。

【0146】

ホーム・オペレータAAA／HSSネットワークに対するアクセスは全く行なわれない。全てのWLAN関連AAAアクションは、WLAN／RAN内部にとどまることができる。正規の3GPP WLANで行なわれるように、ホームネットワークに向かう何らかのAAA関連シグナリングを行なう必要は全くない。こうして、より速いWLAN接続セットアップを可能にし、特に統合型LTE／WLANノードにおいて環境を単純化することができる。WLANを使用する決定は、RANノード内で局所的に行なわれる。

【0147】

代替的には、または付加的には、認証は、WLAN／RANインターフェースを用いてRAN内で行なうことができる。この実施例では、ローカルAAAインターフェースは使用されない。RANとの通信は、認証および認可を含め、このWLAN／RANインターフェースを介して起こることになる。RANがこのインターフェースを介してデータをセットアップすることができる場合、アクションは、WLANに対しても内部的なものであり得る。

【0148】

LTEベアラ・セットアップは、セキュアであり、同じセキュリティをWLANベアラ・セットアップについても再使用できる。

【0149】

全てのデータは、EPSを介して送信できる。EPSは、別個のWLAN課金が存在しないように、課金に対処することができる。

【0150】

WLANベアラは、LTEネットワーク（または他の3GPPネットワーク）の一部であることができる。これは、RANサイトからの追加の外部インターフェース（例えばAAA）無く、RANに局所的である。

【0151】

3GPPは、WLAN無線上の多数のベアラについて、3GPPリリース12内でWLC Pプロトコルを規定した。LTE／WLANアグリゲーションは、多数のLTEベアラがWLAN上でアグリゲートされなければならない場合、WLC Pプロトコルを利用することができる。

【0152】

図3または4の流れ図の各ブロックおよびそれらの任意の組合せをハードウェア、ソフトウェア、ファームウェア、1つ以上のプロセッサおよび／または回路などのさまざまな手段およびそれらの組合せによって実装することができる、ということを理解すべきである。

【0153】

図1～4を用いて以上で説明した実施形態は、ノード、ホストまたはサーバーなどの装置上、または図5に示されている制御機能を提供するユニット、モジュールなどの中、あるいは図2のものなどの移動体デバイス上（または移動体デバイス内のユニット、モジュールなどの中）で実装可能である。図5は、このような装置の一例を示す。一部の実施形態において、基地局は、制御機能を実施するための別個のユニットまたはモジュールを含む。他の実施形態においては、制御機能を、無線ネットワークコントローラまたはスペクトルコントローラなどの別のネットワーク要素により提供することができる。システムの

10

20

30

40

50

サービス・エリア内における通信についての制御を提供するように、装置 300 を配置することができる。装置 300 は、少なくとも 1 つのメモリ 301、少なくとも 1 つのデータ処理ユニット 302、303 および入出力インターフェース 304 を含む。インターフェースを介して、制御装置を、基地局の受信機および送信機に結合することができる。受信機および／または送信機を、無線フロント・エンドまたは遠隔無線ヘッドとして実装することができる。

【0154】

例えば、制御機能を提供するために適切なソフトウェア・コードを実行するように、装置 300 の一実施例を構成することができる。制御機能は、第 1 のネットワークからのアクセス情報のユーザー機器における受信を制御するステップにおいて、前記アクセス情報が第 2 のネットワークと結び付けられているステップのうちの少なくとも 1 つを含むことができる。

10

【0155】

制御機能の提供を目的として、適切なソフトウェア・コードを実行するように装置 300 の一実施例を構成することができる。制御機能は、異なる無線アクセス技術を使用する第 1 および第 2 のネットワークを含み、第 2 のネットワークと通信状態で前記アクセス情報を使用するステップと、第 1 のネットワークにより第 2 のネットワークに結び付けられたアクセス情報をユーザー機器に提供するステップであって、前記アクセス情報が第 2 のネットワークとの通信用であり、前記第 1 および第 2 のネットワークが異なる無線アクセス技術を使用するステップと、を含むことができる。

20

【0156】

装置 300 の一実施例は、制御機能を提供するために適切なソフトウェアを実行するように構成され得る。制御機能は、第 2 のネットワークにおいて、第 2 のネットワークと通信するユーザー機器を検出するステップであって、前記ユーザー機器が第 1 のネットワークで認証され、第 1 および第 2 のネットワークが異なる無線アクセス技術を使用しているステップと、第 1 のネットワークでのユーザー機器認証において使用されるアクセス情報に基づいてユーザー機器が第 2 のネットワークにアクセスできるようにするステップと、を含むことができる。

【0157】

図 6 に示されている装置 600 の一実施例は、ユーザー機器において、第 1 のネットワークからのアクセス情報の受信を制御するための手段 610 であって、前記アクセス情報は第 2 のネットワークと結び付けられており、第 1 および第 2 のネットワークが異なる無線アクセス技術を使用するための手段 610 と、第 2 のネットワークと通信状態で前記アクセス情報を使用するための手段 620 と、を含む。

30

【0158】

図 7 に示されている装置 700 の一実施例は、第 1 のネットワークによってユーザー機器に対して第 2 のネットワークに結び付けられたアクセス情報を提供するための手段 710 であって、前記アクセス情報が第 2 のネットワークとの通信用であり、前記第 1 および第 2 のネットワークが異なる無線アクセス技術を使用する手段 710 を含む。

【0159】

図 8 に示されている装置 800 の一実施形態は、第 2 のネットワークにおいて、第 2 のネットワークと通信するユーザー機器を検出するための手段 810 であって、前記ユーザー機器が第 1 のネットワークで認証され、第 1 および第 2 のネットワークが異なる無線アクセス技術を使用している手段 810 と、第 1 のネットワークでのユーザー機器認証において使用されるアクセス情報に基づいてユーザー機器が第 2 のネットワークにアクセスできるようにするための手段 820 と、を含む。

40

【0160】

本願装置は、伝送および／または受信においてまたはそのために使用される無線部品または無線ヘッドなどの他のユニットまたはモジュールなどを含むかまたはそれらに結合されることができる、ということを理解すべきである。装置は、1 つのエンティティとして

50

説明されてきたが、1つ以上の物理的または論理的エンティティ内で異なるモジュールおよびメモリを実装することができる。

【0161】

実施形態はLTEに関連して説明されてきたが、5Gなどの他の任意の通信システムまたは無線アクセス技術に対して類似の原理を適用できるということが指摘される。実施形態は概して、ライセンスまたはアンライセンス・スペクトルを用いるアクセス・システムのために応用可能である。RAN割振りされた情報を使用して、データ・パケットがどのように処理されるかに関わらずUE WLANアクセスを最適化することができる（ただし、一例としてLTE/WLANインテグレーション/アグリゲーションが使用される）。実施形態に係るWLAN認証は、第1のネットワークと第2のネットワークの間のキャリア・アグリゲーション/デュアル・コネクティビティを使用することなく行なうことができる。したがって、無線ネットワーク、技術および標準のためのいくつかの例示的アーキテクチャを参照して、一例としていくつかの例示の実施形態について以上で説明してきたが、本明細書中に例示され説明されたもの以外の任意の好適な通信システム形態に対して実施形態を適用することができる。

10

【0162】

本明細書において、以上では、例示の実施形態が記載されているものの、本発明の範囲から逸脱することなく開示された解決法に対して行なうことのできる複数の変更および修正が存在することも指摘される。

【0163】

一般に、さまざまな実施形態を、ハードウェアまたは専用回路、ソフトウェア、論理またはそれらの任意の組合せの形で実装することができる。本発明の一部の態様は、ハードウェアで実装でき、一方、他の態様は、コントローラ、マイクロプロセッサまたは他の計算デバイスにより実行され得るファームウェアまたはソフトウェアで実装可能であるが、本発明はこれに限定されない。本発明のさまざまな態様を、ブロック図、流れ図として、または他のいくつかの図的表現を用いて例示および説明することができるものの、本明細書中に説明されているブロック、装置、システム、技術または方法が、非限定的な例として、ハードウェア、ソフトウェア、ファームウェア、専用回路または論理、汎用ハードウェアまたはコントローラまたは他の計算デバイスまたはそれらのいくつかの組合せの形で実装可能であることは、十分に理解される。

20

30

【0164】

図1～5を用いて以上で説明した実施形態は、データ・プロセッサ、例えば基地局などのデバイスの少なくとも1つのデータ処理ユニットまたはプロセス、例えばプロセッサ・エンティティ内のeNBまたはUEによって実行可能なコンピュータ・ソフトウェアによってか、またはハードウェアによってか、あるいはソフトウェアとハードウェアの組合せによって実装され得る。ソフトウェア・ルーチン、アプレットおよび/またはマクロを含めたプログラム・プロダクトとも呼ばれるコンピュータ・ソフトウェアまたはプログラムは、任意の装置可読データ記憶装置または配布媒体中に記憶されることができ、これらは、特定のタスクを行なうためのプログラム命令を含む。装置可読データ記憶媒体または配布媒体は、非一時的媒体であることができる。コンピュータ・プログラム・プロダクトは、プログラムが実行された時点で実施形態を実施するように構成された1つ以上のコンピュータ実行可能なコンポーネントを含むことができる。1つ以上のコンピュータ実行可能なコンポーネントは、少なくとも1つのソフトウェア・コードまたはその一部分であることができる。

40

【0165】

さらにこの点に関して、図にある通りの論理フローの任意のブロックが、プログラム・ステップ、または相互接続された論理回路、ブロックおよび機能、またはプログラム・ステップおよび論理回路、ブロックおよび機能の組合せを表わすことができるという点を指摘しておくべきである。ソフトウェアは、メモリ・チップまたはプロセッサ内部に実装されたメモリ・ブロックなどの物理媒体、ハード・ディスクまたはフロッピー・ディスクな

50

どの磁気媒体、および例えばDVDおよびそのデータ変形形態であるCDなどの光学媒体上に記憶可能である。物理媒体は、非一時的媒体である。

【0166】

メモリは、局所的技術環境に好適な任意のタイプのものであることができ、任意の好適なデータ記憶技術、例えば半導体に基づくメモリー・デバイス、磁気メモリー・デバイスおよびシステム、光学メモリー・デバイスおよびシステム、固定メモリおよび着脱式メモリなどを用いて実装可能である。データ・プロセッサは局所的技術環境に好適な任意のタイプのものであることができ、非限定的な例として、汎用コンピュータ、専用コンピュータ、マイクロプロセッサ、デジタル信号プロセッサ(DSP)、特定用途向け集積回路(ASIC)、FPGA、ゲートレベル回路、マルチコア・プロセッサ・アーキテクチャに基づくプロセッサのうちの1つ以上を含むことができる。

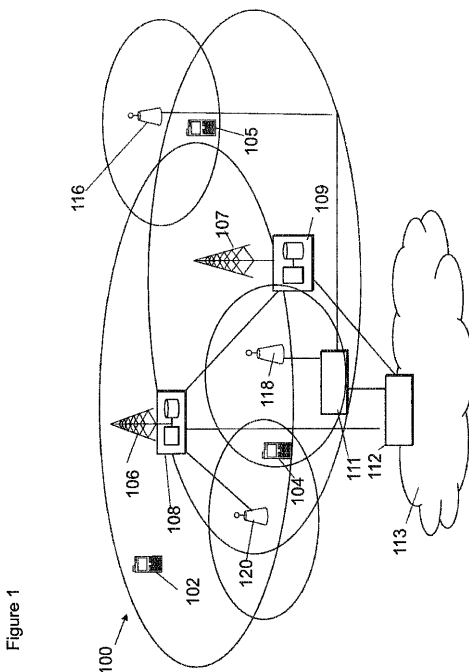
【0167】

図1～5に関連して以上で説明した実施形態は、集積回路モジュールなどのさまざまなコンポーネント内で実践することができる。集積回路の設計は、概して高度に自動化されたプロセスである。半導体基板上にいつでもエッチングし形成できる状態の半導体回路設計へと論理レベル設計を変換するために、複雑かつ強力なソフトウェア・ツールが利用可能である。

【0168】

以上の説明は、本発明の例示的实施形態の完全かつ有益な説明を非限定的な実施例として提供している。しかしながら、添付図面および添付クレームを併せて読んだ場合、以上の説明を考慮して当業者には、さまざまな修正および適応が明らかになる可能性がある。しかしながら、本発明の教示のこのようなおよび類似の修正は全て、添付クレーム内に定義される通りの本発明の範囲内になおも入るものである。実際、前述の他の実施形態のいずれかと1つ以上の実施形態との組合せを含む、さらなる実施形態が存在する。

【図1】



【図2】

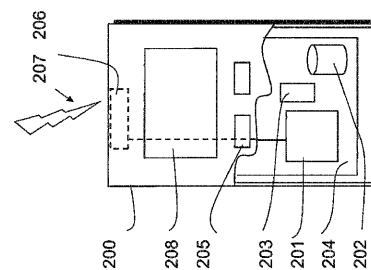
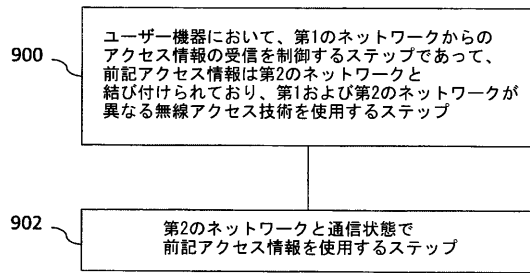


Figure 2

【図 3 A】

Figure 3A



【図 3 B】

Figure 3B

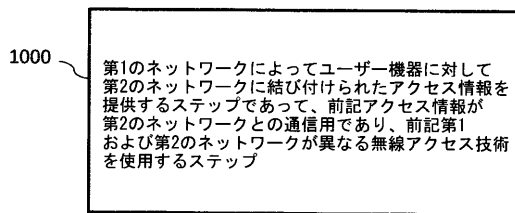
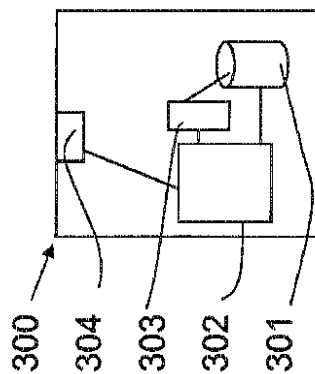
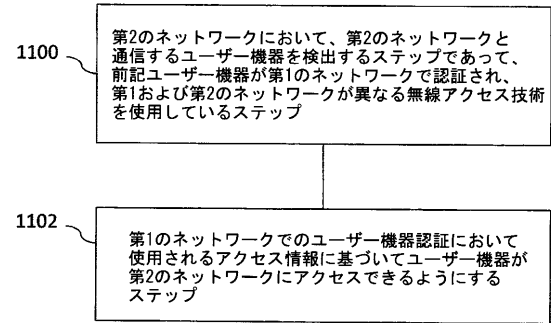


Figure 5



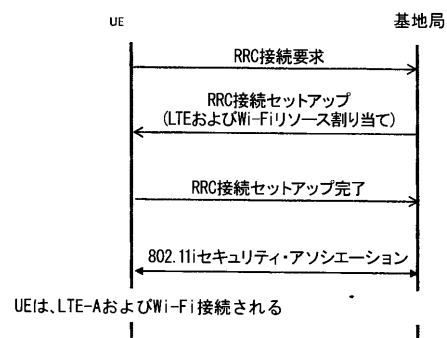
【図 3 C】

Figure 3C



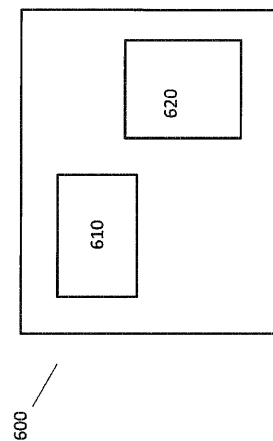
【図 4】

Figure 4



【図 6】

Figure 6



【図 7】

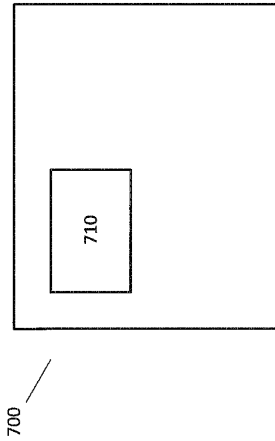


Figure 7

【図 8】

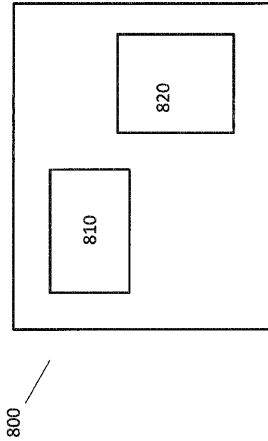


Figure 8

【手続補正書】

【提出日】平成29年6月29日(2017.6.29)

【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】

ユーザー機器において、第 1 ネットワークからアクセス情報の受信を制御するステップであって、前記アクセス情報は第 2 ネットワークと結び付けられており、前記第 1 ネットワークおよび前記第 2 ネットワークが異なる無線アクセス技術を使用する、ステップと、前記第 2 ネットワークと通信状態で前記アクセス情報を使用するステップと、を含む方法。

【請求項 2】

前記第 1 ネットワークおよび前記第 2 ネットワークのうちの少なくとも 1 つに対しユーザー機器識別情報を提供するステップをさらに含む、請求項 1 に記載の方法。

【請求項 3】

ユーザー機器識別情報が、メディア・アクセス制御アドレス、一時的ユーザー機器アイデンティティ情報、および、疑似端末アイデンティティ情報のうちの少なくとも 1 つを含む、請求項 2 に記載の方法。

【請求項 4】

前記第 2 ネットワークでの認証プロシージャにおいて前記アクセス情報を使用するステップを含む、請求項 1 ないし 3 のいずれか 1 項に記載の方法。

【請求項 5】

前記認証プロシーダは、拡張可能認証プロトコル・プロシーダ、事前共有鍵ベース認証システム、高速基本サービス・セット遷移スキーム、および、ペアワイズ・マスタ鍵ベース認証システムのうちの少なくとも1つである、請求項4に記載の方法。

【請求項6】

前記アクセス情報は、無線ローカル・エリア・ネットワーク・クレデンシャル、疑似端末識別子情報、

および、

一時的ユーザー機器アイデンティティ情報のうちの少なくとも1つを含む、請求項1ないし5のいずれか1項に記載の方法。

【請求項7】

第1ネットワークによって、ユーザー機器に対して第2ネットワークに結び付けられたアクセス情報を提供するステップであって、前記アクセス情報が前記第2ネットワークとの通信用であり、前記第1ネットワークおよび前記第2ネットワークが異なる無線アクセス技術を使用する、ステップを含む方法。

【請求項8】

前記第1ネットワークにより、前記第2ネットワークからのアクセス情報の要求を制御するステップをさらに含む、請求項7に記載の方法。

【請求項9】

前記第1ネットワークにより、前記アクセス情報を割り当てるステップと、

前記第2ネットワークに対して前記アクセス情報を提供するステップと、

をさらに含む、請求項7に記載の方法。

【請求項10】

前記ユーザー機器からユーザー機器識別情報を受信するステップをさらに含む、請求項7ないし9のいずれか1項に記載の方法。

【請求項11】

第2ネットワークにおいて、前記第2ネットワークと通信するユーザー機器を検出するステップであって、前記ユーザー機器が第1ネットワークで認証され、前記第1および第2ネットワークが異なる無線アクセス技術を使用している、ステップと、

前記第1ネットワークでの前記ユーザー機器の認証において使用されるアクセス情報に基づいて前記ユーザー機器が前記第2ネットワークにアクセスできるようにするステップと、

を含む方法。

【請求項12】

前記第1ネットワークからのアクセス情報の受信を制御するステップであって、前記アクセス情報が前記第1ネットワークにより割り当てられているステップをさらに含む、請求項11に記載の方法。

【請求項13】

前記第1ネットワークからの要求に応答して、前記第1ネットワークに対しアクセス情報を提供するステップをさらに含む、請求項11に記載の方法。

【請求項14】

アクセス情報に基づいて前記ユーザー機器が前記第2ネットワークにアクセスできるようにするステップは、前記ユーザー機器での認証プロシーダにおいて前記アクセス情報を使用するステップを含む、請求項12または13に記載の方法。

【請求項15】

前記ユーザー機器からのユーザー機器識別情報の受信を制御するステップをさらに含む、請求項11ないし14のいずれか1項に記載の方法。

【請求項16】

アクセス情報に基づいて前記ユーザー機器が前記第2ネットワークにアクセスできるようにするステップは、前記ユーザー機器での認証プロシーダにおいて前記ユーザー機器識別情報を使用するステップを含む、請求項15に記載の方法。

【請求項 17】

前記第1ネットワークは無線アクセス・ネットワークであり、前記第2ネットワークは無線ローカル・エリア・ネットワークである、請求項1ないし16のいずれか1項に記載の方法。

【請求項 18】

請求項1ないし17のいずれか1項に記載の方法を実行するための手段を含む装置。

【請求項 19】

請求項1ないし17のいずれか1項に記載の方法を実行するためのソフトウェア・コード部分を備えるコンピュータ・プログラム。

【請求項 20】

少なくとも1つのプロセッサと、コンピュータ・プログラム・コードを含む少なくとも1つのメモリと、を含む装置であって、

前記少なくとも1つのメモリおよび前記コンピュータ・プログラム・コードは、前記少なくとも1つのプロセッサを用いて、前記装置に、少なくとも、ユーザー機器において第1ネットワークからのアクセス情報の受信を制御させ、ここで、前記アクセス情報は第2ネットワークに結び付けられており、前記第1ネットワークおよび前記第2ネットワークは異なる無線アクセス技術を使用しており、

前記第2ネットワークと通信状態で前記アクセス情報を使用させるように構成される、装置。

【請求項 21】

前記第1ネットワークおよび前記第2ネットワークのうちの少なくとも1つに対して、ユーザー機器識別情報を提供するように構成される、請求項20に記載の装置。

【請求項 22】

ユーザー機器識別情報が、メディア・アクセス制御アドレス、一時的ユーザー機器アイデンティティ情報、および、疑似端末アイデンティティ情報のうちの少なくとも1つを含む、請求項21に記載の装置。

【請求項 23】

前記第2ネットワークでの認証プロシージャにおいて前記アクセス情報を使用するように構成される、請求項20ないし22のいずれかに1項に記載の装置。

【請求項 24】

前記認証プロシージャは、拡張可能認証プロトコル・プロシージャ、事前共有鍵ベース認証システム、高速基本サービス・セット遷移スキーム、および、ペアワイズ・マスタ鍵ベース認証システムのうちの少なくとも1つである、請求項23に記載の装置。

【請求項 25】

前記アクセス情報は、無線ローカル・エリア・ネットワーク・クレデンシャル、疑似端末識別子情報、および、一時的ユーザー機器アイデンティティ情報のうちの少なくとも1つを含む、請求項20ないし24のいずれか1項に記載の装置。

【請求項 26】

少なくとも1つのプロセッサと、コンピュータ・プログラム・コードを含む少なくとも1つのメモリと、を備える装置であって、

前記少なくとも1つのメモリおよび前記コンピュータ・プログラム・コードは、前記少なくとも1つのプロセッサを用いて、前記装置に、少なくとも、第1ネットワークによって、ユーザー機器に対して第2ネットワークに結び付けられたアクセス情報を提供させるように構成され、

前記アクセス情報は前記第2ネットワークとの通信用であり、

前記第1および第2ネットワークは異なる無線アクセス技術を使用する、装置。

【請求項 27】

前記第1ネットワークにより、前記第2ネットワークからのアクセス情報の要求を制御するように構成される、請求項26に記載の装置。

【請求項 28】

前記第1ネットワークにより、前記アクセス情報を割当て、前記第2ネットワークに対して前記アクセス情報を提供するように構成される、請求項27に記載の装置。

【請求項 29】

前記ユーザー機器からユーザー機器識別情報を受信するように構成される、請求項26ないし28のいずれか1項に記載の装置。

【請求項 30】

少なくとも1つのプロセッサと、コンピュータ・プログラム・コードを含む少なくとも1つのメモリと、を含む装置であって、

前記少なくとも1つのメモリおよび前記コンピュータ・プログラム・コードは、前記少なくとも1つのプロセッサを用いて、前記装置に、少なくとも、

第2ネットワークにおいて、前記第2ネットワークと通信するユーザー機器を検出させ、ここで前記ユーザー機器は第1ネットワークで認証され、前記第1および第2ネットワークは異なる無線アクセス技術を使用しており、

前記第1ネットワークでの前記ユーザー機器の認証において使用されるアクセス情報に基づいて前記ユーザー機器が前記第2ネットワークにアクセスできるようにさせる、ように構成される、装置。

【請求項 31】

前記装置は、前記第1ネットワークからのアクセス情報の受信を制御するように構成され、

前記アクセス情報は前記第1ネットワークにより割当てられる、請求項30に記載の装置。

【請求項 32】

前記第1ネットワークからの要求に応答して、前記第1ネットワークに対しアクセス情報を提供するように構成される、請求項30に記載の装置。

【請求項 33】

前記ユーザー機器での認証プロシージャにおいて前記アクセス情報を使用するように構成される、請求項31または32に記載の装置。

【請求項 34】

前記ユーザー機器からユーザー機器識別情報を受信するように構成される、請求項30ないし33のいずれか1項に記載の装置。

【請求項 35】

前記ユーザー機器での認証プロシージャにおいて前記ユーザー機器識別情報を使用するように構成される、請求項34に記載の装置。

【請求項 36】

前記第1ネットワークは無線アクセス・ネットワークであり、

前記第2ネットワークは無線ローカル・エリア・ネットワークである、請求項20ないし35のいずれか1項に記載の装置。

【請求項 37】

プロセスを実行するためのプログラム・コードを備えるコンピュータ・プログラムであって、

該プロセスは、

ユーザー機器において、第1ネットワークからアクセス情報の受信を制御するステップであって、前記アクセス情報は第2ネットワークと結び付けられており、前記第1および第2ネットワークが異なる無線アクセス技術を使用する、ステップと、

前記第2ネットワークと通信状態で前記アクセス情報を使用するステップと、を含む、コンピュータ・プログラム。

【請求項 38】

前記プロセスは、前記第1ネットワークおよび前記第2ネットワークのうちの少なくと

も1つに対しユーザー機器識別情報を提供するステップをさらに含む、請求項37に記載のコンピュータ・プログラム。

【請求項39】

ユーザー機器識別情報が、メディア・アクセス制御アドレス、一時的ユーザー機器アイデンティティ情報、および、疑似端末アイデンティティ情報のうちの少なくとも1つを含む、請求項38に記載のコンピュータ・プログラム。

【請求項40】

前記プロセスは、前記第2ネットワークでの認証プロシージャにおいて前記アクセス情報を使用するステップを含む、請求項37ないし39のいずれか1項に記載のコンピュータ・プログラム。

【請求項41】

前記認証プロシージャは、拡張可能認証プロトコル・プロシージャ、事前共有鍵ベース認証システム、高速基本サービス・セット遷移スキーム、および、ペアワイズ・マスタ鍵ベース認証システムのうちの少なくとも1つである、請求項40に記載のコンピュータ・プログラム。

【請求項42】

前記アクセス情報は、無線ローカル・エリア・ネットワーク・クレデンシャル、疑似端末識別子情報、および、一時的ユーザー機器アイデンティティ情報のうちの少なくとも1つを含む、請求項37ないし41のいずれか1項に記載のコンピュータ・プログラム。

【請求項43】

プロセスを実行するためのプログラム・コードを備えるコンピュータ・プログラムであって、

該プロセスは、第1ネットワークによって、ユーザー機器に対して第2ネットワークに結び付けられたアクセス情報を提供するステップを含み、

前記アクセス情報は前記第2ネットワークとの通信用であり、

前記第1および第2ネットワークは異なる無線アクセス技術を使用する、
コンピュータ・プログラム。

【請求項44】

前記プロセスは、前記第1ネットワークにより、前記第2ネットワークからのアクセス情報の要求を制御するステップを含む、請求項43に記載のコンピュータ・プログラム。

【請求項45】

前記プロセスは、

前記第1ネットワークにより、前記アクセス情報を割り当てるステップと、

前記第2ネットワークに対して前記アクセス情報を提供するステップと、
を含む、請求項43に記載のコンピュータ・プログラム。

【請求項46】

前記プロセスは、前記ユーザー機器からユーザー機器識別情報を受信するステップを含む、請求項43ないし45のいずれか1項に記載のコンピュータ・プログラム。

【請求項47】

プロセスを実行するためのプログラム・コードを備えるコンピュータ・プログラムにあって、

該プロセスは、

第2ネットワークにおいて、前記第2ネットワークと通信するユーザー機器を検出するステップであって、前記ユーザー機器が第1ネットワークで認証され、前記第1および第2ネットワークが異なる無線アクセス技術を使用している、ステップと、

前記第1ネットワークでの前記ユーザー機器の認証において使用されるアクセス情報に基づいて前記ユーザー機器が前記第2ネットワークにアクセスできるようにするステップと、を含む、
コンピュータ・プログラム。

【請求項48】

前記プロセスは、前記第 1 ネットワークからアクセス情報の受信を制御するステップ含み、

前記アクセス情報は前記第 1 ネットワークにより割当てられている、
請求項 47 に記載のコンピュータ・プログラム。

【請求項 49】

前記プロセスは、前記第 1 ネットワークからの要求に応答して、前記第 1 ネットワークに対しアクセス情報を提供するステップを含む、請求項 47 に記載のコンピュータ・プログラム。

【請求項 50】

前記プロセスは、前記ユーザー機器での認証プロシージャにおいて前記アクセス情報を使用するステップを含む、請求項 48 または 49 に記載のコンピュータ・プログラム。

【請求項 51】

前記プロセスは、前記ユーザー機器からユーザー機器識別情報の受信を制御するステップを含む、請求項 47 ないし 50 のいずれか 1 項に記載のコンピュータ・プログラム。

【請求項 52】

前記プロセスは、前記ユーザー機器での認証プロシージャにおいて前記ユーザー機器識別情報を使用するステップを含む、請求項 51 に記載のコンピュータ・プログラム。

【請求項 53】

前記第 1 ネットワークは、無線アクセス・ネットワークであり、

前記第 2 ネットワークは無線ローカル・エリア・ネットワークである、
請求項 37 ないし 52 のいずれか 1 項に記載のコンピュータ・プログラム。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2014/074326

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04W12/06 H04W12/08 H04W36/00 H04W88/06
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2012/284785 A1 (SALKINTZIS APOSTOLIS K [GR] ET AL) 8 November 2012 (2012-11-08) figure 4 paragraph [0053] - paragraph [0069] -----	1-53
X	US 2011/222523 A1 (FU I-KANG [TW] ET AL) 15 September 2011 (2011-09-15) figure 9 paragraph [0048] - paragraph [0053] -----	1-53
X	US 2010/067434 A1 (SIU ISAAC TA-YAN [US] ET AL) 18 March 2010 (2010-03-18) figure 6 abstract paragraph [0060] - paragraph [0063] paragraph [0077] -----	1-53

☐ Further documents are listed in the continuation of Box C.☒ 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

6 July 2015

Date of mailing of the international search report

21/07/2015

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

Lamelas Polo, Yvan

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2014/074326

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2012284785 A1	08-11-2012	NONE	

US 2011222523 A1	15-09-2011	CN 102318237 A	11-01-2012
		EP 2545662 A1	16-01-2013
		JP 2013522986 A	13-06-2013
		TW 201204162 A	16-01-2012
		US 2011222523 A1	15-09-2011
		WO 2011110108 A1	15-09-2011

US 2010067434 A1	18-03-2010	CN 102160424 A	17-08-2011
		EP 2351427 A1	03-08-2011
		JP 5237456 B2	17-07-2013
		JP 2012503432 A	02-02-2012
		KR 20110073524 A	29-06-2011
		TW 201125389 A	16-07-2011
		US 2010067434 A1	18-03-2010
		WO 2010033438 A1	25-03-2010

フロントページの続き

(51)Int.Cl. F I テーマコード (参考)
H04W 72/04 (2009.01) H04W 72/04 1 1 1

(81)指定国 AP(BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, 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, 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 ヤリ ペッカ ムスタヤルビ
 フィンランド国, エフイー—0 2 7 3 0 エスプー, セイトセマス ヤルビクヤ 6

(72)発明者 ミカ フォッシェル
 フィンランド国, エフイー—0 1 1 5 0 ソデルクッラ, パロカルイエンティエ 1 1

(72)発明者 ヤンネ ペッテリ テルボネン
 フィンランド国, エフイー—0 2 6 3 0 エスプー, ランサンカッリオ 2 セー 2

Fターム(参考) 5K067 AA11 AA22 AA35 BB04 BB21 DD11 DD17 DD57 EE04 EE10
 EE16 EE24 EE56 FF02 HH22 HH24 JJ12 JJ13