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

特許第5096584号
(P5096584)

(45)発行日　平成24年12月12日(2012.12.12)　(24)登録日　平成24年9月28日(2012.9.28)

(51)Int.Cl.		F I		
H04W 12/04	(2009.01)	H04Q	7/00	182
H04W 84/10	(2009.01)	H04Q	7/00	628
H04W 12/06	(2009.01)	H04Q	7/00	183
H04L 9/08	(2006.01)	H04L	9/00	601B
		H04L	9/00	601E

請求項の数 16　(全 18 頁)

(21)出願番号	特願2010-527950 (P2010-527950)
(86)(22)出願日	平成20年9月25日 (2008.9.25)
(65)公表番号	特表2011-501899 (P2011-501899A)
(43)公表日	平成23年1月13日 (2011.1.13)
(86)国際出願番号	PCT/US2008/011099
(87)国際公開番号	WO2009/045310
(87)国際公開日	平成21年4月9日 (2009.4.9)
審査請求日	平成22年5月26日 (2010.5.26)
(31)優先権主張番号	60/997,639
(32)優先日	平成19年10月4日 (2007.10.4)
(33)優先権主張国	米国(US)
(31)優先権主張番号	12/019,903
(32)優先日	平成20年1月25日 (2008.1.25)
(33)優先権主張国	米国(US)

(73)特許権者　596092698
アルカテル－ルーセント　ユーエスエー　インコーポレーテッド
アメリカ合衆国　０７９７４　ニュージャーシィ，マレイ　ヒル，マウンテン　アヴェニュー　６００－７００
(74)代理人　100094112
弁理士　岡部　讓
(74)代理人　100085176
弁理士　加藤　伸晃
(74)代理人　100104352
弁理士　朝日　伸光
(74)代理人　100128657
弁理士　三山　勝巳

最終頁に続く

(54)【発明の名称】符号分割多重アクセスによって動作するフェムトセルに接続される移動体装置を認証するための方法

(57)【特許請求の範囲】

【請求項１】

安全なネットワークと通信するフェムトセルを関与させる方法であって、

前記安全なネットワーク内の第１の安全なエンティティにおいて、移動体装置から受信したグローバル認証応答を用いて、前記移動体装置を認証するステップであって、前記グローバル認証応答は、第１のセキュリティ鍵及び第１の乱数を用いて前記移動体装置によって生成され、前記第１のセキュリティ鍵は、前記フェムトセルに知られていない、ステップと、

前記第１の安全なエンティティにおいて、前記安全なネットワーク内の第２の安全なエンティティから、グローバルチャレンジに基づいて形成された少なくとも１つの第２のセキュリティ鍵を受信するステップと、

前記フェムトセルを介して、前記第１の安全なエンティティから前記移動体装置へ、第２の乱数を含む固有のチャレンジを送信するステップと、

前記第１の安全なエンティティにおいて、前記フェムトセルから、前記第２の乱数及び前記第１のセキュリティ鍵を用いて前記移動体装置によって生成された固有のチャレンジ応答を受信するステップと、

前記第２の乱数に基づいて前記第１の安全なエンティティが前記移動体装置を認証することに応じて、前記少なくとも１つの第２のセキュリティ鍵を前記フェムトセルに提供するステップとを備える方法。

【請求項２】

請求項１の方法において、
前記グローバル認証応答を用いて前記移動体装置を認証するステップは、前記移動体装置を固有に識別する識別子と、前記第１の乱数と、前記第１の乱数及び前記移動体装置によって知られているが前記フェムトセルによっては知られていない前記第１のセキュリティ鍵に基づいて前記移動体装置によって計算される認証応答とを示す情報を含むグローバル認証応答を用いて、前記移動体装置を認証するステップを備える、方法。
【請求項３】
請求項２の方法において、
前記固有のチャレンジを送信するステップは、前記第２の乱数及び前記移動体装置に固有の認証応答を用いて前記フェムトセルによって形成された固有のチャレンジを送信するステップを備え、前記第２の安全なエンティティが前記移動体装置を固有に識別する前記識別子に基づいて前記認証応答を特定する、方法。
【請求項４】
請求項３の方法において、
前記フェムトセルが前記第２の乱数を含む前記固有のチャレンジを前記移動体装置に送信できるように、前記フェムトセルに、前記第２の乱数を提供するステップを備える、方法。
【請求項５】
請求項４の方法において、
前記第１の安全なエンティティにおいて、前記第２の乱数を提供するステップに応じて、前記第２の乱数と、前記第２の乱数に基づいて前記移動体装置によって計算される認証応答とを示す情報を受信するステップを備える、方法。
【請求項６】
請求項５の方法において、
前記第２の乱数に基づいて前記移動体装置によって計算される前記認証応答が、前記第２の安全なエンティティから受信した前記認証応答に一致する場合に、前記移動体装置を認証するステップを備える、方法。
【請求項７】
請求項１の方法において、
前記第２の安全なエンティティから少なくとも１つの第２のセキュリティ鍵を要求することは、シグナリング及びベアラトラフィックの暗号化のためのセッション鍵を要求することを含む、方法。
【請求項８】
請求項１の方法において、
前記移動体装置を認証するステップは、前記移動体装置から前記フェムトセルに送信される登録メッセージ又は前記移動体装置から前記フェムトセルに送信される発信メッセージの少なくとも１つに応じて、前記移動体装置を認証するステップを備える、方法。
【請求項９】
符号分割多重アクセス（ＣＤＭＡ）標準に従って動作するフェムトセルを関与させる方法において、前記フェムトセルはまた、インターネットプロトコル・マルチメディア・サブシステム（ＩＭＳ）ネットワークと通信するように構成され、前記方法は、
前記ＩＭＳネットワーク内の第１の安全なエンティティにおいて、移動体装置から受信したグローバル認証応答を用いて、前記移動体装置を認証するステップであって、前記グローバル認証応答は、第１の乱数及び前記フェムトセルに知られていない第１のセキュリティ鍵を用いて前記移動体装置によって生成される、ステップと、
前記第１の安全なエンティティにおいて、前記ＩＭＳネットワークに接続されたＣＤＭＡベースの認証サーバから、グローバルチャレンジに基づいて形成された少なくとも１つの暗号鍵を受信するステップ、
前記フェムトセルを介して、前記第１の安全なエンティティから前記移動体装置へ、第２の乱数を含む固有のチャレンジを送信するステップと、

前記第１の安全なエンティティにおいて、前記フェムトセルから、前記第２の乱数及び前記第１のセキュリティ鍵を用いて前記移動体装置によって生成された固有のチャレンジ応答を受信するステップと、

前記第２の乱数に基づいて前記第１の安全なエンティティが前記移動体装置を認証することに応じて、前記少なくとも１つの暗号鍵を前記フェムトセルに提供するステップとを備える方法。

【請求項１０】

請求項９の方法において、

前記移動体装置を認証するステップは、前記移動体装置を固有に識別する電子シリアル番号と、前記第１の乱数と、前記第１の乱数及び前記移動体装置によって知られているが前記フェムトセルによっては知られていない前記第１のセキュリティ鍵に基づいて前記移動体装置によって計算される認証応答とを示す情報を含むグローバル認証応答を用いて、前記移動体装置を認証するステップを備える、方法。

【請求項１１】

請求項１０の方法において、

前記第２の乱数及び前記移動体装置に固有の認証応答を示す情報を用いて前記固有のチャレンジを形成するステップを備え、前記ＣＤＭＡベースの認証サーバが、前記移動体装置を固有に識別する前記電子シリアル番号に基づいて前記認証応答を特定する、方法。

【請求項１２】

請求項１１の方法において、

前記固有のチャレンジを送信するステップは、前記フェムトセルが前記第２の乱数を含む前記固有のチャレンジを前記移動体装置に送信できるように、前記フェムトセルに、前記第２の乱数を提供するステップを備える、方法。

【請求項１３】

請求項１２の方法において、

前記移動体装置を認証するステップは、前記第１の安全なエンティティにおいて、前記第２の乱数を提供するステップに応じて、前記第２の乱数と、前記第２の乱数に基づいて前記移動体装置によって計算される認証応答とを示す情報を受信するステップを備える、方法。

【請求項１４】

請求項１３の方法において、

前記移動体装置を認証するステップは、前記第２の乱数に基づいて前記移動体装置によって計算される前記認証応答が、前記ＣＤＭＡベースの認証サーバから受信した前記認証応答に一致する場合に、前記移動体装置を認証するステップを備える、方法。

【請求項１５】

請求項９の方法において、

前記ＣＤＭＡベースの認証サーバから少なくとも１つの暗号鍵を要求することは、ＳＭＥＫＥＹ又はＰｕｂｌｉｃ　Ｌｏｎｇ　Ｃｏｄｅ　Ｍａｓｋ鍵の少なくとも１つを要求することを含む、方法。

【請求項１６】

請求項９の方法において、

前記移動体装置を認証するステップは、前記移動体装置から前記フェムトセルに送信される登録メッセージ又は前記移動体装置から前記フェムトセルに送信される発信メッセージの少なくとも１つに応じて受信される前記グローバル認証応答を用いて、前記移動体装置を認証するステップを備える、方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本願は米国特許出願第１１／９７２２６２号、２００８年１月１０日出願、発明の名称「Method for Authenticating Mobile Units Attached to a Femtocell that Operates A

ccording to Code Division Multiple Access」に関係する。
本発明は概略として通信システムに関し、より具体的には無線通信システムに関する。
【背景技術】
【０００２】
従来の無線通信システムは基地局のネットワークを用いて無線接続を１以上の移動体装置に提供する。ある場合では、例えば、移動体装置のユーザが音声又はデータ呼を開始したいときに、移動体装置はネットワーク内の１以上の基地局との無線通信を開始できる。或いは、ネットワークは移動体装置との無線通信リンクを開始できる。例えば、従来の階層的無線通信では、サーバはターゲット移動体装置に宛てられた音声及び／又はデータを無線ネットワークコントローラ（ＲＣＮ）のような中央要素に送信する。そして、ＲＮＣはページングメッセージをターゲット移動体装置に１以上の基地局を介して送信する。ターゲット移動体装置は、無線通信システムからのページングの受信に応じて、無線リンクを１以上の基地局に無線リンクを確立する。ＲＮＣ内の無線リソース管理機能は音声及び／又はデータを受信し、基地局のセットによって使用される無線及び時間リソースを調整して情報をターゲット移動体装置に送信する。無線リソース管理機能は基地局のセットを介してブロードキャスト送信のためのリソースを割り当て及び解放するために微調ゲイン制御を実行する。
【０００３】
ＣＤＭＡシステム等の従来の階層的システムにおける安全な通信は、ネットワーク内の移動体装置及び安全なエンティティにのみ知られている秘密情報（例えば、認証鍵）に基づいて確立される。ＨＬＲ／ＡｕＣ及び移動体装置は、例えば、ＣＡＶＥアルゴリズムを用いて認証鍵（ＡＫ）から共有秘密データ（ＳＳＤ）を引き出す。ＡＫは、移動局及びＨＬＲ／ＡｕＣのみに知られている６４ビット１次秘密鍵である。この鍵はローミングしている相手方に共有されることはない。ＡＫが用いられてＳＳＤが生成され、それはＣＡＶＥアルゴリズムを用いて算出されるものであり、ローミングしている相手方にも共有され得る１２８ビットの２次鍵である。認証中、ＨＬＲ／ＡｕＣ及び移動体装置の双方は、ＳＳＤ、電子シリアル番号（ＥＳＮ）、移動体識別番号（ＭＩＮ）、及び共有乱数（ＲＡＮＤ）等の共有入力を個別に独立して用いて認証応答を算出する。独立して算出された結果が一致した場合には、認証は承認され、移動体装置はネットワークに登録することが許可される。
【０００４】
ＡＫ又はＳＳＤはネットワークに登録される移動体装置を認証するために使用できる。例えば、基地局は乱数（ＲＡＮＤ）を周期的に生成し、ＲＡＮＤをブロードキャストすることができる。ブロードキャストされたＲＡＮＤを受信する移動体装置はＲＡＮＤ及びＡＫ又はＳＳＤを含む入力を用いて認証アルゴリズム出力（ＡＵＴＨ）を計算する。ＡＵＴＨ及び関連のＲＡＮＤ（又はＲＡＮＤの選択された部分）はペアといわれることもある。そして、移動体装置はＡＵＴＨ／ＲＡＮＤペアを基地局に送信し、それはこの情報をネットワークを介してＨＬＲ／ＡｕＣに渡す。ＨＬＲ／ＡｕＣは認証アルゴリズム、ＡＫ又はＳＳＤの記憶された値、各移動体装置に対応する他のデータ、及びＲＡＮＤを用いてＡＵＴＨの予想値を計算する。この値が移動体装置によって送信された値に一致する場合、移動体装置は認証される。基地局はＲＡＮＤの値を頻繁に変更して、ＡＵＴＨ値が新しいことを保証し、以前に生成されたＡＵＴＨ／ＲＡＮＤ結果がエアインターフェイスをモニタすることによって捕捉され、不正な移動体装置又は移動体装置エミュレータによって再現され得る可能性を減らす。少なくともある程度において、基地局は通常は無線通信プロバイダの支配下にある安全なデバイスであることから、この技術は合理的に信頼性があるものと考えられている。
【０００５】
移動体装置を試すのに固有のチャレンジ（問いかけ）が使用できる。固有のチャレンジでは、認証センターは固有乱数を生成し、それが移動体装置に送信される。移動体装置はセキュリティアルゴリズムを用いて、固有のチャレンジに対する固有の応答を算出し、そ

の固有の応答の値を示す情報を認証センターに送信する。認証センターはまた、セキュリティアルゴリズムを実行して固有の応答の予想値を生成する。認証センターが、固有の応答の予想値が移動体装置によって与えられる値と同じであると判断した場合には、移動体装置は認証される。そうでない場合、可能なセキュリティ侵害が起こっている。固有のチャレンジは通常、例えばグローバルなチャレンジを用いてシステムアクセスについて認証することができないシステムによって使用される。固有のチャレンジはまた、システムアクセス上で有効な交換が行われなかった場合のバックアップ認証手順として使用され得る。

【０００６】

従来の階層的ネットワークアーキテクチャに対する１つの代替は、分散通信ネットワーク機能を実施する基地局ルータのようなアクセスポイントのネットワークを含む分散アーキテクチャである。例えば、各基地局ルータはＲＮＣ及び／又はＰＤＳＮ機能を、１以上の移動体装置とインターネット等の外部ネットワークの間の無線リンクを管理する単一のエンティティに統合することができる。階層的ネットワークと比べて分散アーキテクチャは、ネットワークを配備するコスト及び／又は複雑さや、例えば、基地局ルータ等の追加の無線アクセスポイントを付加するコスト及び／又は複雑さを低減して既存のネットワークのカバレッジを拡張する可能性を持っている。分散ネットワークはまた、階層的ネットワークのＲＮＣ及びＰＤＳＮでのパケット待ち行列遅延が低減又は除去されるので、ユーザによって経験される遅延を（階層的ネットワークに対して）減少させることができる。

【０００７】

基地局ルータを配備するコスト及び複雑さが低減されることに少なくともある程度起因して、基地局ルータは従来の基地局に対しては現実的ではないような場所に配備できるようになる。例えば、基地局ルータは住宅又はビル内に配備されて住宅又はビルの居住者に無線接続を与えることができる。住宅内に配備された基地局ルータは通常、住宅を包含する非常に小さいエリア（例えば、フェムトセル）への無線接続を提供することが意図されているので、ホーム基地局又はフェムトセルといわれる。しかし、フェムトセル内の機能は通常、約数平方キロメートルの面積をカバーするマクロセルへの無線接続を提供することが意図された従来の基地局ルータで実施される機能と非常に似ている。フェムトセルと従来の基地局ルータの間の１つの重要な相違は、ホーム基地局ルータは、在庫から購入して素人によって簡単に設置できる安価なプラグアンドプレイデバイスとして設計されていることである。

【０００８】

フェムトセルは通常、フェムトセルと移動体装置の間の安全な通信を確立するのに使用され得る情報を記憶するための高価なセキュリティチップを含まない。さらに、フェムトセルは個人の自宅又は職場といった安全でない場所に配備されることが意図されている。結果として、フェムトセルは、移動体装置を認証するのに使用され得る秘密鍵又は他の情報を記憶するための信頼できる場所としては考えられていない。従って、移動体装置を認証するのに使用される乱数であるＲＡＮＤを生成するようにフェムトセルが構成された場合、フェムトセルは移動体装置を不正に名乗るように改造できる。例えば、違法なフェムトセルは適法な移動体装置と適法な基地局の間で送信された有効なＡＵＴＨ／ＲＡＮＤペアを途中で奪うことができる。そして、違法なフェムトセルは奪ったＡＵＴＨ／ＲＡＮＤペアを用いて適法な移動体装置を模擬する。フェムトセルがＲＡＮＤ値を生成する責任を持っているので、ネットワークは違法なフェムトセルによって送信されたＡＵＴＨ／ＲＡＮＤペアがＲＡＮＤの新たな値に対応するのか否か判断することができない。

【発明の概要】

【課題を解決するための手段】

【０００９】

本発明は上述の問題の１以上の効果に対処するように向けられている。以降に、発明の幾つかの側面の基本的理解を提供するために発明の簡略化された概要を提示する。この概要は発明の網羅的な概観ではない。発明の鍵となる若しくは重大な要素を特定し、又は発

明の範囲の輪郭付けることは意図されていない。専らの目的は、後述する更に詳細な説明の導入部として簡略化された形式で幾つかの概念を提示することである。

【００１０】

本発明の一実施例では、インターネットプロトコル・マルチメディア・サブシステム（ＩＭＳ）ネットワークとの通信においてフェムトセルを関与させる方法が提供される。一実施例では、フェムトセルは符号分割多重アクセス（ＣＤＭＡ）標準に従って動作する。その方法は、ＩＭＳネットワークにおいてフェムトセルから及び第１の安全なエンティティにおいて、グローバルなチャレンジにおいてフェムトセルによってブロードキャストされた第１の乱数を用いて移動体装置によって生成された第１の認証情報を受信することを含む。その方法はまた、安全なネットワークにおいて第２の安全なエンティティから、グローバルなチャレンジ及び移動体装置を固有にチャレンジする（問いかける）ための第２の認証情報に基づいて形成された少なくとも１つのセキュリティ鍵を受信することを含む。一実施例では、第２の安全なエンティティはＣＤＭＡベースの認証サーバである。その方法はさらに、第２の認証情報に基づいて移動体装置を認証することに応じて、セキュリティ鍵をフェムトセルに提供することを含む。

【００１１】

発明は添付図面との関連で以降の説明を参照することによって理解され、図面では同様の参照符号は同様の要素を特定する。

発明は種々の修正及び代替の形式に影響を受けるものであるが、その具体的な実施例は図面に例示として示され、ここにその詳細が記載される。しかし、具体的な実施例のここでの説明は開示される特定の形式に発明を限定することを意図するものではなく、逆に、後記の特許請求の範囲によって規定される発明の範囲内に入る全ての変形例、均等物及び代替物を包含することを意図することが理解されるべきである。

【図面の簡単な説明】

【００１２】

【図１】図１は本発明による、無線通信システムの一実施例を概略的に示す。

【図２】図２は本発明による、移動体装置が登録するときの固有のチャレンジを提供することによって移動体装置を認証する方法の一実施例を概略的に示す。

【図３】図３は本発明による、移動体装置の登録中の固有のチャレンジに基づいて移動体装置を認証する方法の一実施例を概略的に示す。

【図４】図４は本発明による、移動体装置の発呼に応じて固有のチャレンジを提供することによって移動体装置を認証する方法の一実施例を概略的に示す。

【図５】図５は本発明による、移動体装置の登録中の固有のチャレンジに基づいて移動体装置を認証する方法の一実施例を概略的に示す。

【図６Ａ】図６Ａは本発明による、固有のチャレンジに基づいて移動体装置を認証する方法の一代替実施例を概略的に示す。

【図６Ｂ】図６Ｂは本発明による、固有のチャレンジに基づいて移動体装置を認証する方法の一代替実施例を概略的に示す。

【発明を実施するための形態】

【００１３】

発明の例示的実施例が以下に記載される。説明の簡明化のために、実際の実施における全ての構成がこの明細書に記載されているわけではない。もちろん、そのようなあらゆる現実の実施例の開発において、実施に特有の多数の決定が、システム関連及び事業関連の規制への準拠のような開発者の特定の目標を達成するためになされ、それは実施によって異なり得るものであることが分かるはずである。さらに、そのような開発の労力は複雑で時間のかかるものではあるが、それでも本開示の利益を得た当業者にとっては普通の試行といえる。

【００１４】

本発明が添付図面を参照してここに記載される。種々の構造、システム及び装置は、説明の便宜のため、及び当業者に周知の詳細事項によって本発明を分かりにくくしないよう

にするために模擬的に図示されている。それでもなお、添付図面は本発明の例示的実施例を記載し、説明するために含まれる。ここで使用される語句及び表現は、当業者によるそれらの語句及び表現の理解に従う意味を有するものと解釈されるものとする。その用語又は表現の矛盾ない使用によって示唆されることを意図する用語又は表現の特別な定義、即ち、当業者によって理解される通常の及び慣例に従う意味と異なる定義はない。用語又は表現が特別の意味、即ち、当業者によって理解されるもの以外の意味を有することを意図する限りは、そのような特別の定義は、直接的及び等価的に特別の定義をその用語又は表現に与える定義様式で明細書中に記載される。

【００１５】

図１に無線通信システム１００の一実施例を概略的に示す。図示する実施例では、無線通信システム１００は、無線接続を提供するための１以上のフェムトセル１０５を含む。フェムトセル１０５は、これに限定されないが符号分割多重アクセス（ＣＤＭＡ）規格及び／又はプロトコル、ユニバーサル移動通信サービス（ＵＭＴＳ）規格及び／又はプロトコル、移動体通信グローバルシステム（ＧＳＭ）規格及び／又はプロトコル、ＷｉＭＡＸ規格及び／又はプロトコル、ＩＥＥＥ規格及び／又はプロトコル等の規格及び／又はプロトコルに従って無線接続を提供することができる。またさらに、本開示の利益を受けた当業者であれば、本発明は無線接続を与えるためにフェムトセル１０５を用いることに限定されないことが分かるはずである。代替の実施例では、基地局、基地局ルータ、アクセスネットワーク等のようなデバイスが無線通信システム１００において無線接続を与えるために使用できる。

【００１６】

フェムトセル１０５は、フェムトセル１０５にアクセスすることが許可された１以上の移動体装置１１０を含む建造物をほぼ包含するエリアへの無線カバレッジを与えるものとする。移動体装置１１０は、移動体装置１１０とフェムトセル１０５の間のハンドシェイク・プロトコルを用いる等して、登録済み移動体装置１１０に対する国際移動体加入者識別（ＩＭＳＩ）をウェブページを介してユーザに入力させる等の種々の技術を用いてフェムトセル１０５に登録することができる。説明の実施例では、移動体装置１１０は符号分割多重アクセス（ＣＤＭＡ）ベースの無線移動体装置１１０である。しかし、本開示の利益を受けた当業者であれば、本発明はＣＤＭＡベースの移動体装置１１０に限定されないことが分かるはずである。

【００１７】

フェムトセル１０５はインターネットプロトコル・マルチメディア・サブシステム（ＩＭＳ）ネットワーク１１５（破線四角で示す）を介して無線通信システム１００へのアクセスを提供する。種々の代替実施例では、フェムトセル１０５は種々の機能要素によってＩＭＳネットワーク１１５に結合され得る。例えば、図１では、フェムトセル１０５はデジタル加入者線（ＤＳＬ）又はケーブルモデムネットワーク１２０に結合され、それはフェムトネットワークゲートウェイ１２５に結合される。運用管理及び保守（ＯＡ＆Ｍ）サーバ１３０はフェムトネットワークゲートウェイ１２５に結合され、フェムトネットワークゲートウェイ（ＦＮＧ）１２５を介してフェムトセル１０５とインターネットプロトコル（ＩＰ）ネットワーク１３５の間の通信を確立するために使用できる。例えば、ＩＰＳｅｃトンネルがフェムトセル１０５とフェムトネットワークゲートウェイ１２５の間に形成できる。しかし、本開示の利益を受けた当業者であれば、実施例は本発明をこの特定のネットワークアーキテクチャに限定するものではないことが分かるはずである。

【００１８】

ＩＭＳネットワーク１１５は、多数のタイプのハンドセットによるインターネット上の通信をサポートするセッション開始プロトコル（ＳＩＰ）ベースのネットワークである。例えば、（フェムトセル１０５に結合される移動体装置１１０等の）これらのハンドセットは、ボイス・オーバー・インターネット・プロトコル（ＶｏＩＰ）及び他の方法を用いてリアルタイムアプリケーションにおけるデータ及び音声をＩＰネットワーク１３５にわたって転送できる。ＩＭＳネットワーク１１５はホーム加入者サーバ（ＨＳＳ）１４０を

含み、それは呼を扱うＩＭＳネットワークエンティティをサポートするマスターユーザデータベースである。ＨＳＳ１４０は契約関連情報（ユーザプロファイル）を含み、認証及びユーザの認証を実行し、ユーザの物理的位置についての情報を提供することができる。ＩＭＳネットワーク１１５はまた、ＩＭＳネットワーク１１５においてＳＩＰシグナリングパケットを処理するのに使用される１以上のコールセッション制御機能（ＣＳＣＦ）エンティティ１４５を含むことができる。図１ではＣＳＣＦエンティティ１４５は単一の機能ブロックで示しているが、本開示の利益を受けた当業者であれば、ＣＳＣＦエンティティ１４５はサービングＣＳＣＦ、プロキシＣＳＣＦ、インテロゲーティングＣＳＣＦ等のような複数のエンティティを含むことができ、これらは１以上の他の機能的及び／又は物理的エンティティにおいて実施され得ることが分かるはずである。移動管理アプリケーションサーバ（ＭＭＡＳ）１５０は移動体装置１１０の移動に関する機能を調整及び管理するのに使用される。

【００１９】

フェムトセル１０５はグローバルなチャレンジ（問いかけ）をオーバーヘッドチャネルで移動体装置１１０に送することができる。一実施例では、グローバルチャレンジはフェムトセル１０５で生成されるグローバル乱数に基づく。システムアクセス毎に、移動体装置はシークレットデータ（ＳＳＤ又はＡＫ）を用いた応答を計算し、応答及び乱数の少なくとも一部を承認のためのシステムに返信する。フェムトセル１０５はグローバル乱数及び応答を用いて移動体装置１１０を認証し、移動体装置１１０とのエアインターフェイスを介して安全な（セキュア）通信リンクを確立する。しかし、フェムトセル１０５は無線通信システム１００の信用できる要素ではないことがある。例えば、フェムトセル１０５はユーザの自宅又は職場に配置されているために物理的に安全ではないことがある。結果として、サービスプロバイダは、フェムトセル１０５を改変又はハッキングしようとする許可なきユーザによってフェムトセル１０５がアクセスされ得ないことを保証することができない。またさらに、フェムトセル１０５はネットワークを介したハッキングの影響を受け易い。例えば、フェムトセル１０５のユーザは充分なファイアーウォール保護、ウイルス保護等を提供していない場合があり、これによって許可なきユーザがフェムトセル１０５にハッキングすることが可能となってしまうことになる。フェムトセル１０５はシステム１００の信用ある要素ではないので、フェムトセル１０５によって発せられるグローバルチャレンジも（これらのグローバルチャレンジに基づく認証も）疑わしいものとなる。

【００２０】

対照的に、ＩＭＳネットワーク１１５内のエンティティは信用ある又は安全なエンティティである。例えば、ＭＭＡＳ１５０はサービスプロバイダの支配下にある建造物内に配置されるので物理的に安全といえる。結果として、サービスプロバイダは、フェムトセル１０５を改造又はハッキングしようとする許可なきユーザによってＭＭＡＳ１５０がアクセスされ得ないことを保証することができる。さらに、ＭＭＡＳ１５０はファイアーウォール保護、ウイルス保護等を用いてハッキングから保護され、これによってＭＭＡＳ１５０への許可なきアクセスを防止できる。１以上の鍵をフェムトセル１０５又は移動体装置１１０に生成及び提供するのに使用されるホームロケーションレジスタ／認証センター（ＨＬＲ／ＡｕＣ）１６０等のネットワーク内の他のエンティティも、それらはサービスプロバイダの支配下にあるので比較的信用があり及び／又は安全であると考えられる。

【００２１】

従って、ＩＭＳネットワーク１１５内の（又はそれに安全に結合された）信用ある及び／又は安全なエンティティは、疑わしいグローバルチャレンジに続いて発せられ得る固有のチャレンジを用いて移動体装置１１０を認証するのに使用できる。一実施例では、移動体装置１１０は、グローバル認証応答をＩＭＳネットワーク１１５に転送することによってフェムトセル１０５によって発せられた（潜在的に疑わしい）グローバルチャレンジに応答することができ、それによってグローバル認証応答を承認し、ＨＬＲ／ＡｕＣ１６０と協働してセッション鍵のようなセキュリティ情報を生成することができる。その後、Ｉ

ＭＳネットワーク１１５はフェムトセル１０５を介して固有のチャレンジを移動体装置１１０に対して作成及び送信することができる。固有のチャレンジを受信すると、移動体装置１１０が認証は承認のためにＩＭＳネットワーク１１５に転送される固有の認証応答を生成する。移動体装置１１０が信用ある及び／又は安全なエンティティによって認証されると、ＩＭＳネットワーク１１５は呼処理サービス又はホームロケーションレジスタ／認証センター（ＨＬＲ／ＡｕＣ）１６０で生成された１以上の鍵等のセキュリティ情報をフェムトセル１０５に提供することができる。

【００２２】

図２に、移動体装置がネットワークに登録するときの固有のチャレンジを提供することによって移動体装置を認証する方法２００の一実施例を概略的に示す。図示する実施例では、無線接続を移動体装置に提供するためにフェムトセル又は基地局ルータ（ＢＳＲ）が使用される。フェムトセルはサービングＣＳＣＦ（Ｓ－ＣＳＣＦ）、プロキシＣＳＣＦ（Ｐ－ＣＳＣＦ）、インテロゲーティングＣＳＣＦ（Ｉ－ＣＳＣＦ）、ホーム加入者サーバ（ＨＳＳ）、及び移動管理アプリケーションサーバ（ＭＭＡＳ）を含むＩＭＳネットワークに通信可能に結合されている。ＩＭＳネットワークはまた、ホームロケーションレジスタ／認証センター（ＨＬＲ／ＡｕＣ）と通信状態にある。本開示の利益を受けた当業者であれば、図２に示す要素は例示であり、本発明を制限することを意図するものではない。代替の実施例では、より多くの又はより少ない機能を実行する、より多い又はより少ない要素が含まれてもよい。

【００２３】

図示する実施例では、矢印２０５で示すように、フェムトセルはグローバル乱数（ＲＡＮＤ）を作成し、オーバーヘッドメッセージトレインにおけるこの乱数（ＲＡＮＤ）をブロードキャストする。移動体装置はグローバル乱数並びに移動体装置及びＨＬＲ／ＡｕＣのみに知られているＳＳＤ鍵のような鍵を用いてグローバル認証応答（ＡＵＴＨＲ）を計算する。その後移動体装置は、矢印２１０で示すように、登録メッセージをフェムトセルに送信できる。移動体装置によって送信される登録メッセージはグローバル乱数、グローバル認証応答、移動体装置識別子、及び電子加入者番号を含むＳＩＰ登録メッセージであればよい。矢印２１５、２２０で示すように、フェムトセルは登録メッセージをＰ－ＣＳＣＦに転送し、その後登録メッセージをＩ－ＣＳＣＦに転送することができる。矢印２２５に示すように、Ｉ－ＣＳＣＦは移動体装置に対する適切なＳ－ＣＳＣＦを特定するために尋問メッセージをホーム加入者サーバに送信することができる。矢印２３０で示すように、ホーム加入者サーバは、選択されたＳ－ＣＳＣＦを示す情報で応答する。その後、矢印２４０で示すように、登録メッセージは選択されたＳ－ＣＳＣＦに転送される。

【００２４】

Ｓ－ＣＳＣＦは、矢印２４５で示すように、ＩＭＳ認証が移動体装置について実行される必要があるか否かを尋ねるためのメッセージをホーム加入者サーバに送信する。例えば、Ｓ－ＣＳＣＦは（２４５において）移動体認証要求（ＭＡＲ）をホーム加入者サーバに送信する。その後、矢印２５０で示すように、ホーム加入者サーバはＩＭＳ認証が移動体装置について実行される必要があるか否かを示す情報を返信する。ホーム加入者サーバからのメッセージが移動体装置を認証することが必要でないことを示す場合には、ＩＭＳ認証は（２５５で）スキップできる。ホーム加入者サーバからのメッセージが移動体装置を認証することが必要でであることを示す場合には、ＩＭＳ認証は（２５５で）フェムトセルでユーザエージェントとともに実行される。いずれの場合でも、矢印２６０で示すように、Ｓ－ＣＳＣＦは移動体装置のサービスプロファイルへの要求をホーム加入者サーバに送信し、矢印２６５で示すように、ホーム加入者サーバは移動体装置に対するサービスプロファイルをＳ－ＣＳＣＦに返信する。ＩＭＳ認証ステップがスキップされた場合には、Ｓ－ＣＳＣＦはフェムトセルに登録が完了したことを（例えば、２００－ＯＫメッセージを送信する等して）伝え、太い矢印２７０で示すように、フェムトセルはアクノリッジメントメッセージで応答することができる。

【００２５】

一実施例では、フェムトセルは（２７５で）そのＩＭＳ登録ステータスを、例えば、ＳＵＢＳＣＲＩＢＥメッセージをＳ－ＣＳＣＦを送信することによって契約し、それは（２００－ＯＫメッセージ等の）契約を確認するメッセージを返信することができる。移動体装置のＣＤＭＡ認証が後でチャレンジ／応答シーケンスで失敗した場合には、移動管理アプリケーションサーバは、例えば、２００－ＯＫメッセージの代わりに４ｘｘ失敗メッセージを供給することによって、Ｓ－ＣＳＣＦにＩＭＳ登録が失敗したことを通知することができる。移動管理アプリケーションサーバは登録メッセージをＳ－ＣＳＣＦにおいて記憶されたユーザプロファイルにおける初期フィルタ基準に基づいて第三者登録メッセージとして受信するので、登録失敗メッセージはＳ－ＣＳＣＦに移動体装置を登録解除させることができる。移動体装置の登録解除は以前に完了したＩＭＳ登録がトーンダウンされるであろうことを意味することができる。フェムトセルにおけるユーザエージェントは、契約されたフェムトセルがそのＩＭＳ登録ステータスにおいて変化するので、登録がトーンダウンされるときに通知を受信すべきである。従って、フェムトセルにおけるユーザエージェントは、消去（クリーンアップ）される必要があるものは何でも消去する立場にある。一実施例では、ユーザエージェントは自滅することができる。

【００２６】

矢印２８０で示すように、Ｓ－ＣＳＣＦは登録メッセージを移動管理アプリケーションサーバに送信することができる。一実施例では、Ｓ－ＣＳＣＦは（２８０で）移動体装置識別子、電子シリアル番号、認証応答、及びグローバル乱数を示す情報を含むＳＩＰ第三者登録メッセージを送信する。登録メッセージを受信するのに応じて、移動管理アプリケーションサーバは（２８５で）ＨＬＲ／ＡｕＣによって提供された固有のチャレンジ／応答ペアを用いて移動体装置を認証する。その後、矢印２９０で示すように、認証手続の結果は２００－ＯＫ登録メッセージ等のメッセージでＳ－ＣＳＣＦに送信される。

【００２７】

図３に、移動体装置の登録中に固有のチャレンジに基づいて移動体を認証する方法３００の一実施例を概略的に図示する。方法３００の一部又は全部は図２に示すステップ２８５の一部として実施され得る。図示する実施例では、矢印３０５で示すように、Ｓ－ＣＳＣＦはＳＩＰ第三者登録メッセージ等の登録メッセージを移動管理アプリケーションサーバに送信する。登録メッセージの受信に応じて、移動管理アプリケーションサーバは移動体装置を認証するのに使用され得る固有のチャレンジ／応答ペアを要求する。例えば、移動管理アプリケーションサーバはビジターロケーションレジスタ（ＶＬＲ）のように機能し、矢印３１０で示すように、固有のチャレンジ／応答ペアについての認証要求をＨＬＲ／ＡｕＣに送信することができる。その後、ＨＬＲ／ＡｕＣは、固有乱数（ＲＡＮＤＵ）及び固有認証応答（ＡＵＴＨＵ）等の要求された固有のチャレンジ／応答ペアを返信することができる。

【００２８】

移動管理アプリケーションサーバは提供された固有チャレンジ／応答ペアを用いて移動体装置にチャレンジする（問いかける）ことができる。図示する実施例では、矢印３２０、３２５で示すように、移動管理アプリケーションサーバはＳＩＰメッセージ等のメッセージをＳ－ＣＳＣＦに転送し、それはそのメッセージをフェムトセルに転送する。そのメッセージは移動体装置に対してＨＬＲ／ＡｕＣによって生成された固有乱数によって表された固有のチャレンジを含む。その後、矢印３３０で示すように、フェムトセルは受信固有チャレンジ乱数を用いて固有チャレンジメッセージを形成し、それを移動体装置に送信する。固有のチャレンジを受信すると、移動体装置は供給された固有乱数及び移動体装置に知られているセキュリティ鍵を用いて固有認証応答（ＡＵＴＨＵ）を生成する。矢印３３５で示すように、移動体装置は固有乱数及び計算された認証応答（ＲＡＮＤＵ／ＡＵＴＨＵ）を含むチャレンジ応答メッセージをフェムトセルに返信する。その後、矢印３４０、３４５で示すように、フェムトセルは計算された認証応答（ＡＵＴＨＵ）をＳ－ＣＳＣＦに送信し、それはこの応答を移動管理アプリケーションサーバに送る。例えば、計算された認証応答は２００－ＯＫ応答メッセージで送信され得る。

【００２９】
移動管理アプリケーションサーバは（３５０において）移動体装置及びＨＬＲ／ＡｕＣによって提供された認証応答値を用いて移動体装置を認証する。一実施例では、移動管理アプリケーションサーバは移動体装置及びＨＬＲ／ＡｕＣによって提供された認証応答値を（３５０において）比較し、これらの２値が一致した場合に（３５０において）移動体装置を認証する。移動体装置の認証が（３５０において）成功した場合には、矢印３５５で示すように、移動体管理アプリケーションサーバ送信はＨＬＲ／ＡｕＣへの登録通知を送信する。矢印３６０で示すように、ＨＬＲ／ＡｕＣは登録通知の受信に応じて確認応答を送信することができる。一実施例では、確認応答３６０は移動体装置に関連付けられたビジター・ロケーション・レジスタのプロファイルを含み得る。

【００３０】
移動体装置の認証が（３５０で）成功し（３５５、３６０で）登録された場合には、矢印３６５で示すように、移動管理アプリケーションサーバは登録確認メッセージをＳ－ＣＳＣＦに送信することができる。例えば、移動管理アプリケーションサーバは（３６５において）、移動体装置の登録及び認証が成功したことを示す２００－ＯＫメッセージを送信することができる。一実施例では、Ｓ－ＣＳＣＦは、移動体装置の登録が成功した場合に、他の何らかのアプリケーションサーバが通知されることになっているか否かを判断するために規則のリストを用いるタスクを実行するように進む。しかし、本開示の利益を受けた当業者であれば、他のアプリケーションサーバに通知するか否かを判断することはインテリジェントネットワーク「トリガ」の一例に過ぎず、Ｓ－ＣＳＣＦについての規則のリストはいつトリガをかけるかを判断するのに使用され得るインストラクションの例であることが分かるはずである。一実施例では、トリガはアプリケーションサーバに１以上のＳＩＰメッセージを処理する機会を与える。

【００３１】
図４に、移動体装置の発信に応じて固有のチャレンジを提供することによって移動体装置（ＵＥ）を認証する一実施例の方法４００を概略的に示す。図示する実施例では、フェムトセル又は基地局ルータ（ＢＳＲ）は移動体装置に無線接続を提供するために使用される。フェムトセルは、サービングＣＳＣＦ（Ｓ－ＣＳＣＦ）、プロキシＣＳＣＦ（Ｐ－ＣＳＣＦ）、インテロゲーティングＣＳＣＦ（Ｉ－ＣＳＣＦ）、移動管理アプリケーションサーバ（ＭＭＡＳ）を含むＩＭＳネットワークに継続的に結合される。ＩＭＳネットワークはまた、ホームロケーションレジスタ／認証センタ（ＨＬＲ／ＡｕＣ）及び他の移動体装置又は他の通信デバイス等の他のエンドユーザ（ＥＮＤ）と通信状態にある。本開示の利益を受けた当業者であれば、図４に示す要素は例示であって本発明を限定することを意図しないことが分かるはずである。代替の実施例では、より多い又はより少ない機能を実行する、より多い又はより少ない要素が含まれ得る。

【００３２】
実施例では、矢印４０５で示すように、フェムトセルはグローバル乱数（ＲＡＮＤ）を作成し、オーバーヘッドメッセージトレインにおけるこの乱数（ＲＡＮＤ）をブロードキャストする。移動体装置はグローバル乱数並びに移動体装置及び認証センタ（ＡｕＣ）のみに知られているＳＳＤ鍵のような鍵を用いてグローバル認証応答（ＡＵＴＨＲ）を計算する。矢印４１０で示すように、移動体装置がサービスを発信したい場合、移動体装置は発信メッセージをフェムトセルに送信することができる。例えば、移動体装置は（４１０で）グローバル乱数、認証応答、移動体識別子、及び電子加入者番号を含むＣＤＭＡ発信メッセージを送信する。移動体装置はまた、他のユーザエンドのダイヤル番号を送信することができる。矢印４１５、４２０で示すように、フェムトセルはインビテーションメッセージを形成し、インビテーションメッセージをＰ－ＣＳＣＦに転送すると、それはインビテーションメッセージをＩ－ＣＳＣＦに転送することができる。一実施例では、インビテーションメッセージはグローバル乱数、認証応答、移動体装置識別子、及び電子加入者番号を含むＳＩＰ　ＩＮＶＩＴＥメッセージである。Ｓ－ＣＳＣＦはその後、矢印４３０で示すように、インビテーションメッセージを移動管理アプリケーションサーバに転送す

る。

【００３３】

インビテーションメッセージを受信すると、（４３５で）移動管理アプリケーションサーバは移動体装置を認証することを試み、また、メッセージ又は音声トラフィックを暗号化するために使用され得るＳＭＥＫＥＹ及び／又はＰＬＣＭ等の１以上のセキュリティ鍵を作成することができる。一実施例では、移動体装置を認証し、ＣＤＭＡ暗号鍵を作成するために使用されるステップは同時に及び／又は同期して実行され得る。しかし、本開示の利益を受けた当業者であれば、各ステップが手順を最適化することを試みるコールセットアップメッセージのフロー内に代替的に分散されることが分かるはずである。例えば、コール時の即座の使用のために、固有のチャレンジは移動管理アプリケーションサーバによってコールの前に引き出されて記憶されてもよい。（４３５で）移動体装置が認証されることに成功すると、矢印４４０で示すように、移動管理アプリケーションサーバがインビテーションメッセージをエンドユーザ（ＥＮＤ）に送信する。例えば、移動管理アプリケーションサーバは（４４０で）ＩＮＶＩＴＥメッセージをエンドユーザに送信することができる。その後、矢印４４５、４５０で示すように、１８０リンギングメッセージ等の応答メッセージが移動体管理アプリケーションサーバに返され、それはこのメッセージを移動体装置にフェムトセルを介して転送することができる。矢印４５５で示すように、可聴のリンギングメッセージも移動体装置に提供できる。矢印４６０、４６５に示すように、エンドユーザはコールを受け入れると、２００－ＯＫ応答メッセージ等のユーザがコールに応答したことを示すメッセージが移動管理アプリケーションサーバを介してフェムトセルに送信され得る。

【００３４】

図５に、移動体装置の発信中に固有のチャレンジに基づいて移動体装置を認証する一実施例の方法５００を概略的に示す。方法５００の一部又は全部は図４に示すステップ４３５の一部として実施され得る。ＳＩＰ　ＩＮＶＩＴＥメッセージ等の発信要求を受信するのに応じて、矢印５０５で示すように、移動管理アプリケーションサーバは認証要求をＨＬＲ／ＡｕＣに送信する。一実施例では、認証要求はグローバル乱数を含み、移動体装置によって計算されたグローバル認証応答、他のエンドユーザに対応するダイヤル数の一部又は全部、移動体装置識別子、電子シリアル番号、及び他の任意の情報を含む。その後、ＨＬＲ／ＡｕＣは、矢印５１０で示すように、発信されたコールに関連するＳＭＥＫＥＹ及び／又はＰＬＣＭ鍵等のセキュリティ情報を提供することができる。移動管理アプリケーションサーバはまた、矢印５１０で示すように、認証要求をＨＬＲ／ＡｕＣに送信することもできる。認証要求は発信移動体装置に対応付けられた固有チャレンジ／応答のペアについての要求を含む。その後、（５２０で）ＨＬＲ／ＡｕＣは要求されたチャレンジ／応答のペアを返し、それは固有乱数（ＲＡＮＤＵ）及び対応の固有認証応答（ＡＵＴＨＵ）であればよい。

【００３５】

移動管理アプリケーションサーバはその後、矢印５２５、５３０で示すように、固有乱数を含む固有のチャレンジをＳ－ＣＳＣＦに転送し、それは固有のチャレンジをフェムトセルに転送することができる。矢印５３５で示すように、フェムトセルは固有乱数を提供して固有のチャレンジを移動体装置に発行する。固有のチャレンジに応じて、移動体装置は、提供された固有乱数及び移動体装置に記憶されたセキュリティ鍵を用いて認証応答を計算することができる。その後、矢印５４０で示すように、固有認証応答はフェムトセルに返送される。その後、矢印５４５、５５０で示すように、フェムトセルは計算された認証応答（ＡＵＴＨＵ）をＳ－ＣＳＣＦに送信し、それはこの応答を移動管理アプリケーションサーバに転送することができる。例えば、計算された認証応答及び固有乱数は２００－ＯＫ応答メッセージにおいて送信することができる。

【００３６】

移動管理アプリケーションサーバは移動体装置及び認証センタによって提供された固有認証応答値を用いて（５５５で）移動体装置を認証することができる。一実施例では、移

動管理アプリケーションサーバは移動体装置と認証センタによって提供された認証応答値を（５５５で）比較し、それらの２値が一致した場合に（５５５で）移動体装置を認証する。矢印５６０、５６５で示すように、（５５５で）移動体装置の認証が成功した場合には、移動管理アプリケーションサーバはコールに対するセキュリティ情報をフェムトセルにＳ－ＣＳＣＦを介して送信することができる。例えば、移動管理アプリケーションサーバは、移動体装置の登録及び認証が成功したことを示すとともに以前に特定されたＳＭＥＫＥＹ及び／又はＰＬＣＭ鍵を含む２００－ＯＫメッセージを（５６０、５６５で）送信することができる。この時点でフェムトセルは、コールについてのトラフィックチャネルを暗号化するのに使用できる暗号鍵を有する。フェムトセルは、矢印５７０、５７５で示すように、メッセージを移動管理アプリケーションサーバに返送することによってセキュリティ情報の受信を確認することができる。例えば、（５７０、５７５で）フェムトセルは２００－ＯＫメッセージを移動管理アプリケーションサーバに送信することができる。

【００３７】

図６Ａ及び６Ｂは、固有のチャレンジに基づいて移動体装置を認証する代替実施例の方法６００を概略的に示す。実施例では、フェムトセル又は基地局ルータ（ＢＳＲ）は移動体装置機器（ＵＥ）に無線接続を提供するために使用される。フェムトセルは、サービングＣＳＣＦ（Ｓ－ＣＳＣＦ）、プロキシＣＳＣＦ（Ｐ－ＣＳＣＦ）、インテロゲーティングＣＳＣＦ（Ｉ－ＣＳＣＦ）、移動管理アプリケーションサーバ（ＭＭＡＳ）を含むＩＭＳネットワークに継続的に結合される。ＩＭＳネットワークはまた、ホームロケーションレジスタ／認証センタ（ＨＬＲ／ＡｕＣ）及び他の移動体装置又は他の通信デバイス等の他のエンドユーザ（ＥＮＤ）と通信状態にある。本開示の利益を受けた当業者であれば、図６Ａ及び６Ｂに示す要素は例示であって本発明を限定することを意図しないことが分かるはずである。代替の実施例では、より多い又はより少ない機能を実行する、より多い又はより少ない要素が含まれ得る。

【００３８】

矢印６０１で示すように、移動管理アプリケーションサーバは認証要求を認証センタに送信する。一実施例では、認証要求は、移動体装置識別子、電子シリアル番号及び他の何らかの情報を含む。その後ＨＬＲ／ＡｕＣは、移動体装置への固有のチャレンジを後に形成するために使用され得る情報を含むメッセージで応答することができる。実施例では、（６０１での）要求及び（６０２での）応答が、移動体装置がシステムへのアクセスを要求する前に、例えば登録要求又は発信要求中に、実行される。例えば、（６０１での）要求及び（６０２での）応答が移動体装置によって以前のシステムアクセス中に実行され、固有認証情報（例えば、ＲＡＮＤＵ／ＡＵＴＨＵペア）が、移動体装置がシステムへのアクセスを要求するまでＭＭＳＡで記憶されるようにしてもよい。

【００３９】

実施例では、矢印６０３で示すように、フェムトセルはグローバル乱数（ＲＡＮＤ）を作成し、オーバーヘッドメッセージトレインにおけるこの乱数（ＲＡＮＤ）をブロードキャストする。移動体装置はグローバル乱数並びに移動体装置及び認証センタ（ＡｕＣ）のみに知られているＳＳＤ鍵のような鍵を用いてグローバル認証応答（ＡＵＴＨＲ）を計算する。矢印６０４で示すように、移動体装置がサービスを発信したい場合、移動体装置は発信メッセージをフェムトセルに送信することができる。例えば、移動体装置は、グローバル乱数、認証応答、移動体識別子、及び電子加入者番号を含むＣＤＭＡ発信メッセージを（６０４で）送信する。移動体装置はまた、他のユーザエンドのダイヤル番号を送信することができる。矢印６０５、６０６で示すように、フェムトセルはインビテーションメッセージを形成し、インビテーションメッセージをＰ－ＣＳＣＦに転送すると、それはインビテーションメッセージをＳ－ＣＳＣＦに転送することができる。一実施例では、インビテーションメッセージはグローバル乱数、認証応答、移動体装置識別子、及び電子加入者番号を含むＳＩＰ　ＩＮＶＩＴＥメッセージである。Ｓ－ＣＳＣＦはその後、矢印６０７で示すように、インビテーションメッセージを移動管理アプリケーションサーバに転送する。

【００４０】
その後、矢印６０８、６０９で示すように、移動管理アプリケーションサーバは固有乱数を含むチャレンジをＳ－ＣＳＣＦに転送し、それがチャレンジをフェムトセルに転送することができる。固有認証情報は既に計算及び記憶されているので、インビテーションメッセージの受信に応じてＭＭＳＡは、ＡｕＣからの固有チャレンジ情報をまず要求しなければならない代わりに（６０８で）固有のチャレンジを直接送信できる。矢印６１０で示すように、フェムトセルは提供された固有乱数（ＲＡＮＤＵ）を用いて固有のチャレンジを移動体装置に発行することができる。矢印６１１で示すように、移動管理アプリケーションサーバは認証要求を認証センタに送信することもできる。一実施例では、認証要求はグローバル乱数、移動体装置によって計算されたグローバル認証応答、移動体識別子、電子シリアル番号及び他の任意の情報を含むことができる。その後、矢印６１２で示すように、認証センタは発信されたコールに対応付けられるＳＭＥＫＥＹ及び／又はＰＬＣＭ鍵等のセキュリティ情報を提供することができる。（６１１での）セキュリティ情報の要求及び（６１２での）セキュリティ情報を含む応答はステップ６０８、６０９、６１０の一部又は全部と同時に実行することができる。

【００４１】
（６１０での）固有のチャレンジに応じて、移動体装置は提供された固有乱数及び移動体装置に記憶された秘密鍵を用いて認証応答を計算することができる。その後、矢印６１３で示すように、固有認証応答はフェムトセルに返送される。その後、矢印６１４、６１５で示すように、フェムトセルは計算された認証応答（ＡＵＴＨＵ）をＳ－ＣＳＣＦに送信し、これはこの応答を移動管理アプリケーションサーバに転送することができる。例えば、計算された認証応答及び固有乱数は２００－ＯＫ応答メッセージで送信することができる。

【００４２】
移動管理アプリケーションサーバは、移動体装置及び認証センタによって提供された認証応答（ＡＵＴＨＵ）値を用いて（６１６で）移動体装置を認証することができる。一実施例では、移動管理アプリケーションサーバは移動体装置と認証センタによって提供された認証応答値を（６１６で）比較し、それらの２値が一致した場合に（６１６で）移動体装置を認証する。矢印６１７、６１８で示すように、（６１６で）移動体装置の認証が成功した場合には、移動管理アプリケーションサーバはコールに対するセキュリティ情報をフェムトセルにＳ－ＣＳＣＦを介して送信することができる。例えば、移動管理アプリケーションサーバは、移動体装置の登録及び認証が成功したことを示すとともに以前に特定されたＳＭＥＫＥＹ及び／又はＰＬＣＭ鍵を含む２００－ＯＫメッセージを（６１７、６１８で）送信することができる。この時点でフェムトセルは、コールについてのトラフィックチャネルを暗号化するのに使用できる暗号鍵を有する。矢印６１９、６２０で示すように、フェムトセルはメッセージを移動管理アプリケーションサーバに返送することによってセキュリティ情報の受信を確認することができる。例えば、（６１９、６２０で）フェムトセルは２００－ＯＫメッセージを移動管理アプリケーションサーバに送信することができる。

【００４３】
ある場合では、ＳＳＤ更新が（６０１、６０２での）認証情報の作成及び（６１６での）移動体装置の認証の間で起こっていたということもあり得る。これが起こり、かつ新たなセットのＡＵＴＨＵ／ＲＡＮＤＵデータがＨＬＲ／ＡｕＣから取得されない場合、移動体装置は、たとえ正しいＡＵＴＨＵを返したとしても認証されない。しかし、ＳＳＤ更新はフェムトセルサービングシステム（それはこの場合ではＭＭＡＳである）を介して起こる。従って、ＭＭＡＳが関与し、新たなＲＡＮＤＵ／ＡＵＴＨＵペアを取得しなければならないことを知ることになる。（例えば、ハンドセットがフェムトセルからマクロセルに移動したために）更新がマクロセルで起こる場合、更新はＨＬＲ／ＡｕＣでの登録を導き、登録解除の通知が以前のＶＬＲ（それはＭＭＡＳである）に送信されるべきである。従って、ＭＭＡＳは、その現在のペアが新たなものでないことを知るので、ハンドセットが

フェムトセルに戻って登録するとき、ＭＭＡＳは次のシステムアクセスでコール中に使用されるであろう新たなＲＡＮＤＵ／ＡＵＴＨＵを取得できる。

【００４４】

（６１６で）移動体装置の認証が成功すると、矢印６２１で示すように、移動管理アプリケーションサーバはインビテーションメッセージをエンドユーザ（ＥＮＤ）に送信することができる。例えば、移動管理アプリケーションサーバは（６２１で）ＩＮＶＩＴＥメッセージをエンドユーザに送信することができる。矢印６２２、６２３で示すように、その後１８０リンギングメッセージ等の応答メッセージが移動管理アプリケーションサーバに返され、それがこのメッセージを移動体装置にフェムトセルを介して転送することができる。その後、矢印６２４で示すように、可聴リンギングメッセージが移動体装置に送信される。６２５、６２６で示すように、エンドユーザがコールを受け入れる場合、２００－ＯＫ応答メッセージ等の、ユーザがコールに応答したことを示すメッセージがフェムトセルに移動管理アプリケーションサーバに送信される。

【００４５】

本発明の一部分及び対応の詳細な説明がソフトウェア、アルゴリズム及びコンピュータメモリ内のデータビット上の動作のシンボル的な表示の観点で開示された。これらの記載及び表示は、当業者が他の当業者に彼らの仕事の本質を効果的に伝えるものである。アルゴリズムとは、その用語がここで使用されるように、そして一般的に使用されるように、所望の結果をもたらすステップの自己整合的シーケンスとして考えられる。各ステップは物理量の物理的操作を必要とするものである。通常は、必ずしもそうではないが、これらの量は、記憶され、転送され、結合され、比較され、或いは操作されることができる光、電気又は磁気信号の形態を採る。これは、基本的に一般に使用されるために、これらの信号をビット、値、要素、シンボル、文字、項、数などとして言及するのに時として便利である。

【００４６】

なお、これらの全て及び同様の文言は適切な物理量に関連付けられるべきであり、これらの量に適用される単なる便利なラベルであると解されるべきである。具体的に否定しない限り、或いは、記載から明らかなように、「処理する」、「計算する」、「計算する」、「特定する」、「表示する」等のような文言は、コンピュータシステムのレジスタ及びメモリ内の物理的、電子的な量で表されるデータを操作して、コンピュータシステムメモリ若しくはレジスタ又は他のそのような情報記憶、伝送若しくは表示デバイス内の物理量として同様に表される他のデータに転送するコンピュータシステム又は同様の電子計算デバイスの挙動及び処理を云うものである。

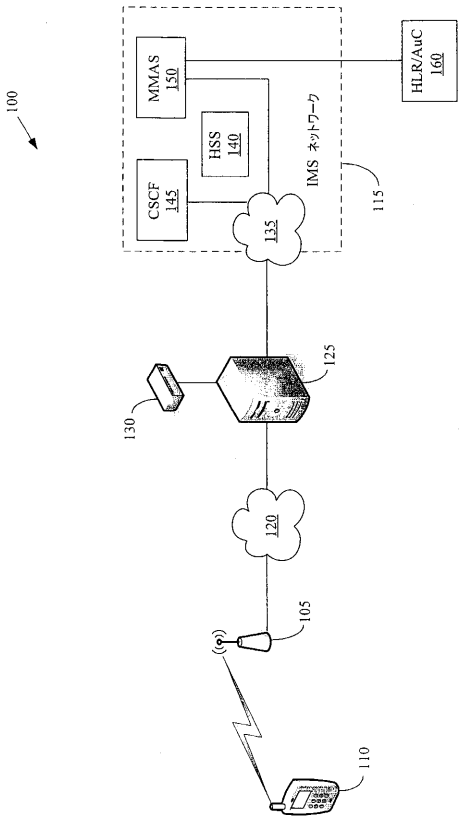
【００４７】

また、発明のソフトウェアの実施による側面は通常、プログラム記憶媒体の何らかの形態で符号化され、又はあるタイプの伝送媒体を介して実行される。プログラム記憶媒体は磁気的（例えば、フロッピー（登録商標）ディスク又はハードドライブ）又は光学的（例えば、コンパクトディスク読取り専用メモリ、又は「ＣＤ　ＲＯＭ」）であればよく、読取り専用又はランダムアクセスであればよい。同様に、伝送媒体は撚り線対、同軸ケーブル、光ファイバ、又は他の適当な周知の伝送媒体であればよい。発明はこれらのいかなる所与の実施の側面によっても限定されない。

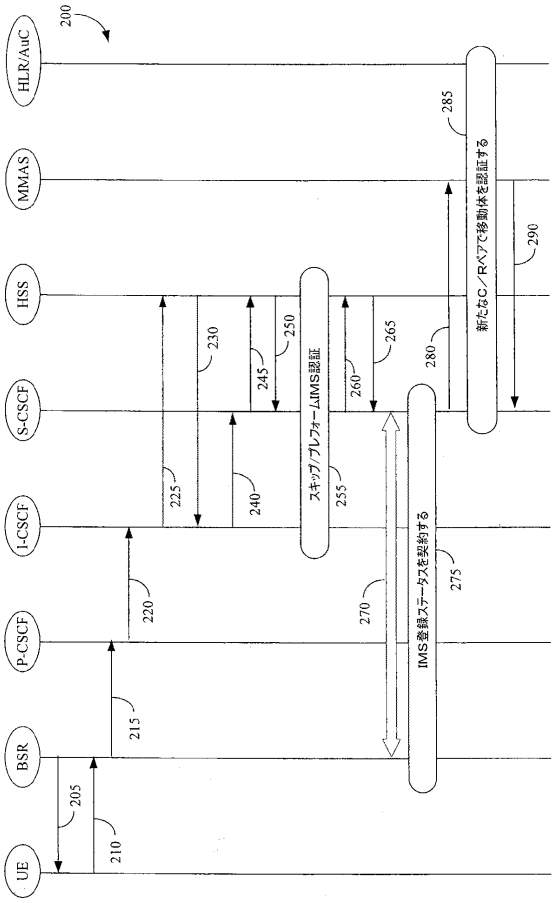
【００４８】

上記の具体的な実施例は、ここでの教示の利益を受けた当業者には明らかな、異なっていても均等な態様で修正及び実施され得るので、例示的なものにすぎない。またさらに、以下の特許請求の範囲に記載されるもの以外に、ここに開示した構成又は設計の詳細に限定は意図されていない。それゆえ、上記に開示した具体的の実施例は変更又は修正され得るものであり、全てのそのような変形例は発明の範囲内のものとしてみなされることは明らかである。従って、ここで求められる保護は以下の特許請求の範囲で示されるものである。

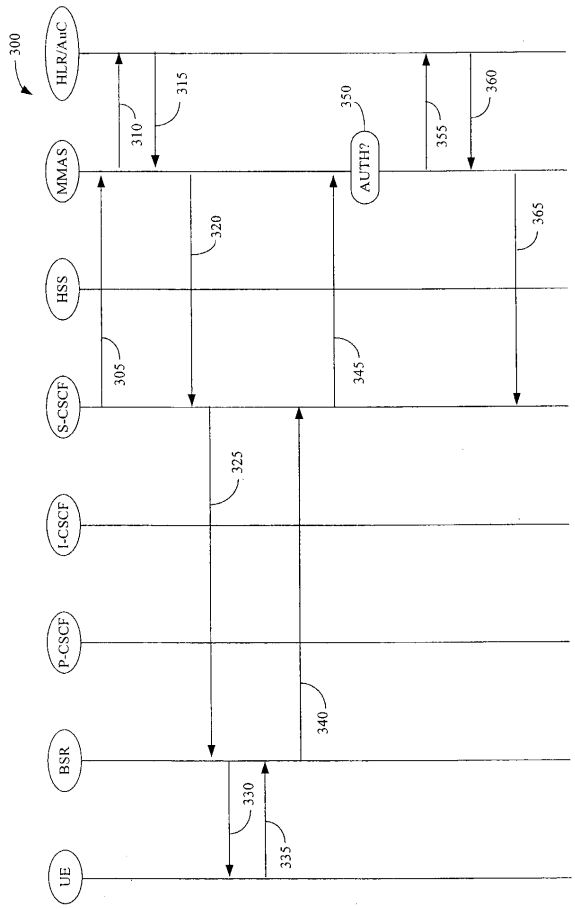
【図１】


100
MMAS 150
HSS 140
CSCF 145
IMS ネットワーク
115
HLR/AuC 160
135
125
130
120
105
110

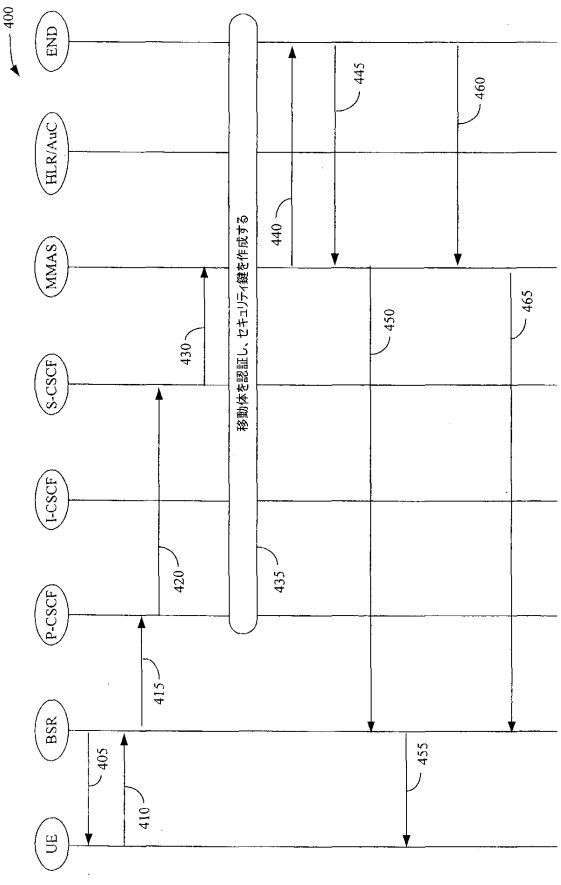
【図２】


200
HLR/AuC
MMAS
HSS
S-CSCF
I-CSCF
P-CSCF
BSR
UE
285
290
新たなC／Rペアで移動体を認証する
230
245
250
265
280
260
225
240
255
スキップ/プレフォームIMS認証
220
270
275
IMS登録ステータスを契約する
215
205
210

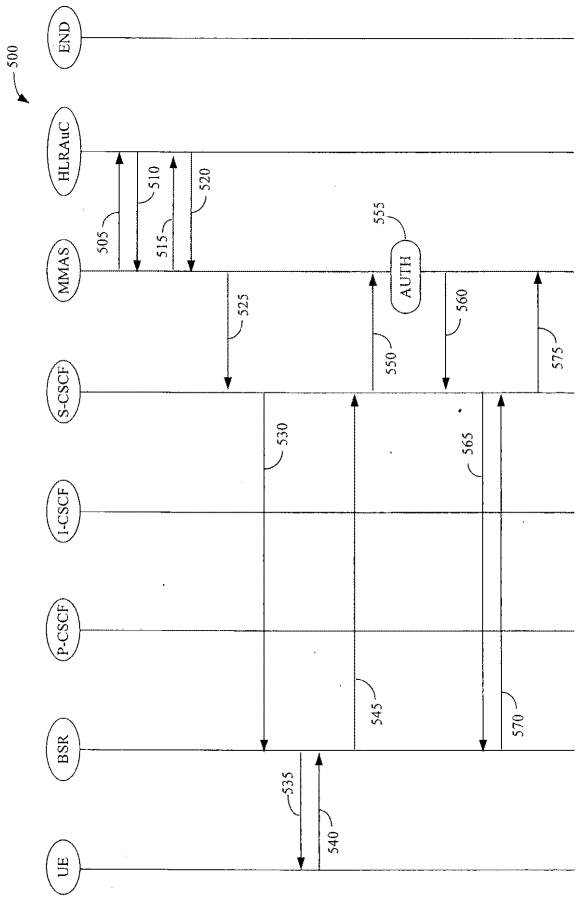
【図３】


300
HLR/AuC
MMAS
HSS
S-CSCF
I-CSCF
P-CSCF
BSR
UE
310
315
350
AUTH?
355
360
320
365
305
345
325
340
330
335

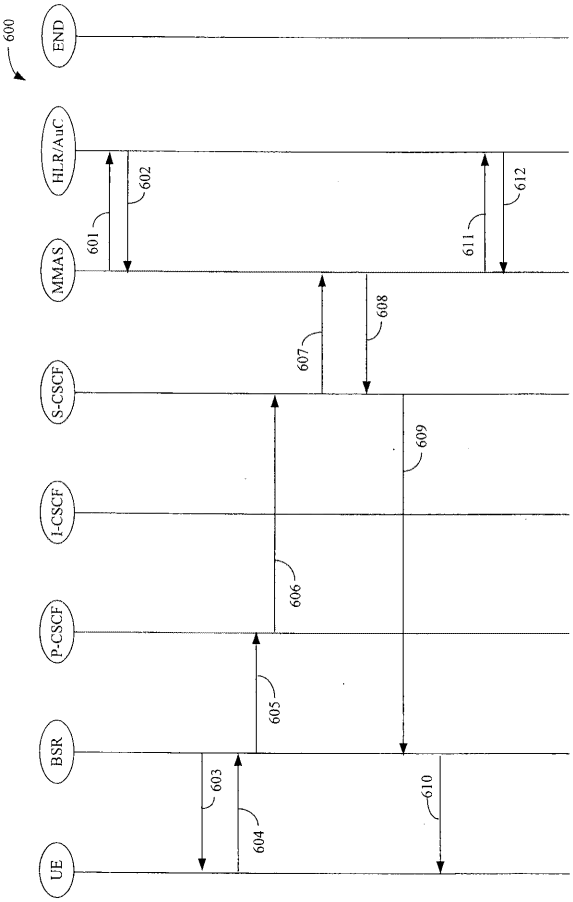
【図４】


400
END
HLR/AuC
MMAS
S-CSCF
I-CSCF
P-CSCF
BSR
UE
移動体を認証し、セキュリティ鍵を作成する
445
460
440
430
450
465
420
435
415
405
410
455

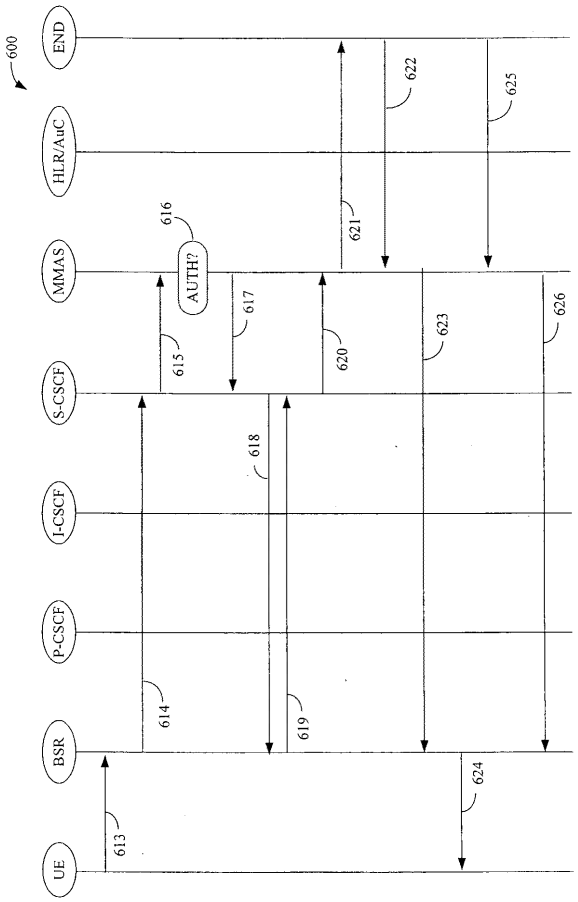
【図５】


500
END
HLRAuC
MMAS
S-CSCF
I-CSCF
P-CSCF
BSR
UE
505
510
515
520
525
530
535
540
545
550
555
AUTH
560
565
570
575

【図６Ａ】


600
END
HLR/AuC
MMAS
S-CSCF
I-CSCF
P-CSCF
BSR
UE
601
602
603
604
605
606
607
608
609
610
611
612

【図６Ｂ】


600
END
HLR/AuC
MMAS
S-CSCF
I-CSCF
P-CSCF
BSR
UE
AUTH?
613
614
615
616
617
618
619
620
621
622
623
624
625
626

フロントページの続き

(74)代理人 100160967
弁理士 ▲濱▼口 岳久
(72)発明者 モルガン，トッド，カートライト
アメリカ合衆国 ６０３０２ イリノイ，オーク パーク，サウス エルムウッド アヴェニュー １３８
(72)発明者 パテル，サーヴァー
アメリカ合衆国 ０７０４５ ニュージャーシィ，モンヴィル，ミラーズ レーン ３４
(72)発明者 トンプソン，ロビン，ジェファリー
アメリカ合衆国 ６０５１０ イリノイ，バタヴィア，ブラックホーク ドライヴ ６７９

審査官 齋藤 浩兵

(56)参考文献 国際公開第２００５／０６５１３２（WO，Ａ２）
特表２００７－５０６３９１（ＪＰ，Ａ）
国際公開第２００７／０１５０７５（WO，Ａ１）
特表２００７－５２２６９５（ＪＰ，Ａ）
特表２００９－５０４０５１（ＪＰ，Ａ）
米国特許第０６７１１４００（ＵＳ，Ｂ１）
特開２０００－０８３０１７（ＪＰ，Ａ）
特表２００１－５０３２０７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04W 12/04
H04L 9/08
H04W 12/06
H04W 84/10