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

特許第5096588号
(P5096588)

(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 12/08	(2009.01)	H04Q	7/00	184
H04W 80/10	(2009.01)	H04Q	7/00	605
G09C 1/00	(2006.01)	G09C	1/00	660E

請求項の数 13　(全 16 頁)

(21)出願番号	特願2010-529893 (P2010-529893)
(86)(22)出願日	平成19年10月17日 (2007.10.17)
(65)公表番号	特表2011-504665 (P2011-504665A)
(43)公表日	平成23年2月10日 (2011.2.10)
(86)国際出願番号	PCT/SE2007/000914
(87)国際公開番号	WO2009/051528
(87)国際公開日	平成21年4月23日 (2009.4.23)
審査請求日	平成22年9月17日 (2010.9.17)

(73)特許権者　598036300
テレフオンアクチーボラゲット　エル　エム　エリクソン（パブル）
スウェーデン国　ストックホルム　エス－１６４　８３
(74)代理人　100095957
弁理士　亀谷　美明
(74)代理人　100096389
弁理士　金本　哲男
(74)代理人　100101557
弁理士　萩原　康司
(74)代理人　100128587
弁理士　松本　一騎

最終頁に続く

(54)【発明の名称】セキュリティ設定を決定するための方法及び構成

(57)【特許請求の範囲】

【請求項１】

複数のアクセスポイント（２０３）及び少なくとも１つのゲートウェイデバイス（２０４）を含む移動体通信ネットワークにおける方法であって、

・ネットワークコンポーネントによって、専用ベアラ信号のトランスポートレベルセキュリティのために必要とされるセキュリティの設定を決定するステップと、

・通信を確立するために配置されるノードに前記決定を通信するステップと、

・前記複数のアクセスポイント（２０３）の１つによって、前記複数のアクセスポイントの１つと前記ゲートウェイデバイス（２０４）との間で必要なセキュアプロトコル（２０５）を構成し又は選択するステップと、

を備え、

・前記決定は、使用中の前記ネットワークの配置及び／又はネットワークオペレータポリシーのうちの１つ又は複数に基づいている、

方法。

【請求項２】

前記ネットワークコンポーネントは、プロキシコールセッション制御機能（Ｐ－ＣＳＣＦ）、問い合わせコールセッション制御機能（Ｉ－ＣＳＣＦ）若しくはサービングコールセッション制御機能（Ｓ－ＣＳＣＦ）、若しくはアプリケーションサーバ（ＡＳ）のうちの１つ又は複数であるアプリケーションレベルのコンポーネントである、請求項１に記載の方法。

【請求項３】
前記ネットワークコンポーネントは、前記セキュリティのニーズをＰＣＲＦに送信する、請求項１に記載の方法。
【請求項４】
セキュリティを必要とするセッションは、前記アクセスポイントと前記ゲートウェイデバイスとの間の暗号化と共に前記セキュアプロトコルを用いる、請求項１に記載の方法。
【請求項５】
セキュリティの必要性が小さいセッションは、メッセージ認証及びヌル暗号化と共にセキュリティプロトコルを使用する、請求項１に記載の方法。
【請求項６】
セッションの保護が必要であるか否かを前記ネットワークコンポーネントが判断する場合に、以下の情報、即ち、暗号化がアクティブ化されたか否か、暗号化レベル、メッセージ認証がアクティブ化されたか否か、及びメッセージ認証レベル、が使用される、請求項２に記載の方法。
【請求項７】
前記ネットワークコンポーネントは、ＰＣＲＦ（ポリシー制御及び課金ルール機能）である、請求項１に記載の方法。
【請求項８】
ＰＣＲＦは、Ｒｅ－Ａｕｔｈ－Ｒｅｑｕｅｓｔ（ＲＡＲ）メッセージにおけるセキュリティ情報をＳＡＥ－ＧＷに送信し、前記ＳＡＥ－ＧＷは、前記情報を移動性管理エンティティ（ＭＭＥ）に転送し、及び、前記ＭＭＥは、最終的に、前記アクセスポイントとゲートウェイデバイスとの間に確立すべきベアラのための追加的な情報と共にリクエストされたセキュリティ設定について前記アクセスポイントに通知する、請求項７に記載の方法。
【請求項９】
前記アクセスポイントは、リクエストされた前記セキュリティ設定及び確立すべきベアラ信号のために必要なトランスポートアドレス情報と、前記ゲートウェイデバイスのＩＰアドレスのアドレス情報と、任意的に、ベアラについてのユーザデータグラムプロトコル（ＵＤＰ）ポートと、に関する情報を含み、前記アクセスポイントは、当該情報に基づいて、新たなＩＰｓｅｃ関連性記述、即ちＩＰＳｅｃセキュリティアソシエーション（ＳＡ）が確立される必要があるか否か、又は既存のＩＰｓｅｃ　ＳＡが未修正のまま使用可能であるか若しくは更新される必要があるか、をチェックする、請求項７に記載の方法。
【請求項１０】
前記ゲートウェイデバイスにより、トラフィックセレクタを使用してトラフィックを異なるＩＰｓｅｃ　ＳＡにマッピングすることによって、ダウンリンク内の前記トラフィックを異なるＩＰｓｅｃ　ＳＡにマッピングするステップ、をさらに備える、請求項９に記載の方法。
【請求項１１】
セキュリティ設定に関する決定は、現在のネットワークの配置又は使用中のアクセスポイントのタイプに基づいてなされ、前記セキュリティ設定は、異なるタイプのアクセスポイント間で移動するユーザ機器（ＵＥ）（２２０）に基づいて更新される、請求項１に記載の方法。
【請求項１２】
移動局及び通信ネットワークに対して信号を送受信するように適合されている基盤デバイス（２０３）であって、前記デバイスは、メモリと、処理構成と、専用ベアラ信号を受信／送信するための受信機／送信機構成とを備え、
・前記受信機は、前記専用ベアラ信号のトランスポートレベルセキュリティのために決定されるセキュリティ設定を受信するようにさらに構成され、前記決定は、使用中のネットワークの配置、及び、専用ベアラ信号について必要とされるネットワークオペレータポリシーのうちの１つ又は複数に基づいて、前記ネットワーク内のネットワークコンポーネントによってなされることと、

・受信される前記セキュリティ設定に基づいて、前記デバイスとゲートウェイデバイスとの間で必要なセキュアプロトコル（ＩＰｓｅｃ）を構成する手段と、
を特徴とする、基盤デバイス（２０３）。
【請求項１３】
様々なアプリケーションについてのオペレータポリシー及び現在使用中のネットワークの配置に応じた専用ベアラ信号のトランスポートレベルセキュリティのためのセキュリティニーズリクエストの標識についての信号を受信する手段を備える通信ネットワークにおける機能要素（ＰＣＲＦ）であって、
・ネットワークノード（２０７、２０３、２０６）へのベアラ確立シグナリング内に当該標識を含めるための手段と、セキュリティレベルがアプリケーションニーズ及び前記現在使用中のネットワークに応じて選択されることと、
・セキュリティニーズリクエストに基づいて、セキュリティが必要か否か、及び適用すべきセキュリティレベル、を決定する手段を含むロジック部と、
を備えることを特徴とする、機能要素。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般的に、少なくとも２つのノード間の通信ネットワークにおけるセキュリティ方法に関する。より具体的には、本発明は、セッションのベアラを確立する場合にセキュリティ設定を決定することと、ベアラが他のノードに移動される場合に、最初に決定されたセキュリティ設定が維持されることを保証することとに関する。
【背景技術】
【０００２】
ＬＴＥ（Ｌｏｎｇ　Ｔｅｒｍ　Ｅｖｏｌｕｔｉｏｎ（ロングタームエボリューション））及びＳＡＥ（Ｓｙｓｔｅｍ　Ａｒｃｈｉｔｅｃｔｕｒｅ　Ｅｖｏｌｕｔｉｏｎ（システムアーキテクチャエボリューション））アーキテクチャが、現在、例えば３ＧＰＰ　Ｒｅｌｅａｓｅ－８に含まれる３ＧＰＰによって仕様化されている。図１ａ及び１ｂは、例えば、非ローミングシナリオ向けの３ＧＰＰ　ＴＳ２３．４０１に説明されているような３ＧＰＰのＳＡＥ／ＬＴＥの標準化対象の一部としてこれまでに合意された従来のアーキテクチャを示している。図１ａは、３ＧＰＰアクセス向けの非ローミングアーキテクチャを示しており、図１ｂは、単一のゲートウェイオプションにおける３ＧＰＰアクセス向けの非ローミングアーキテクチャを示している。
【０００３】
Ｓ１インタフェース（即ち、Ｓ１－ＭＭＥ及びＳ１－Ｕ両方のインタフェース）におけるトランスポートネットワークレベルのセキュリティは、Ｅ－ＵＴＲＡＮノードＢ（ｅＮｏｄｅＢ）と称される単一のノードタイプを含むＥｖｏｌｕｔｅｄ　ＵＴＲＡＮ（Ｅ－ＵＴＲＡＮ）と、コアネットワーク（ＣＮ）ノード、移動性管理エンティティ（ＭＭＥ）及びサービングゲートウェイとの間の多くの配置（deployment）についてのシナリオにおいて必要とされる（図１ａ及び１ｂはまたＰＤＮゲートウェイを示しており、サービングゲートウェイとＰＤＮゲートウェイの組み合わせは、これらのゲートウェイノードの双方についてこの用途で使用されている用語であるＳＡＥ－ＧＷとしても知られている）。Ｓ１インタフェース（Ｓ１－ＭＭＥ及びＳ１－Ｕの双方のインタフェース）は、安全でないＩＰネットワークを横断することもある。このような配置についてのシナリオの一例は、３ＧＰＰで現在検討中のＨｏｍｅ　ｅＮｏｄｅＢ（ＨＮＢ）の概念である。
【０００４】
Ｓ１インタフェースのセキュリティは、ネットワーク側のｅＮｏｄｅＢ（即ちＨＮＢ）とセキュリティゲートウェイ（ＳＥＧＷ）との間に確立されるＩＰｓｅｃトンネルに基づいている。ＳＥＧＷの機能性は、ＳＡＥ－ＧＷ及びＭＭＥの機能性に論理的に組み込まれてもよいが、ＩＰｓｅｃに必要とされる相当に重い処理容量ゆえに専用機器によって取り扱われることになる可能性が高い。

【０００５】
専用ＳＡＥ／ＬＴＥベアラを確立するためのシグナリングシーケンスが図３に示されている。この図は、一例として、ネットワークが開始したベアラのアクティブ化がポリシー及び課金ルール機能（Ｐｏｌｉｃｙ ａｎｄ Ｃｈａｒｇｉｎｇ Ｒｕｌｅｓ Ｆｕｎｃｔｉｏｎ）（ＰＣＲＦ）を介して適用される場合に、ベアラがＩＭＳ．ＶｏＩＰ／ＳＩＰコール／トランザクション向けに生成されることを示している。
【０００６】
Ｐ－ＣＳＣＦとＰＣＲＦ間のインタフェースは、「Ｒｘ＋」インタフェースと称され、３ＧＰＰ向けのＲｘインタフェース、例えば３ＧＰＰ ＴＳ２９．２１４のＲｅｌｅａｓｅ－７に基づいている。ＰＣＲＦとＰＤＮゲートウェイ（及びＳＡＥ－ＧＷ）との間のインタフェースは、Ｓ７インタフェースと称され、３ＧＰＰ向けのＧｘインタフェース、例えば３ＧＰＰ ＴＳ２９．２１２のＲｅｌｅａｓｅ－７に基づいている。
【発明の概要】
【発明が解決しようとする課題】
【０００７】
想定されているセキュリティアーキテクチャは、ｅＮｏｄｅＢとＳＥＧＷとの間の全ての通信がＩＰｓｅｃを使用し、かつ暗号化される必要があることを意味している。このことは、この強力なセキュリティが全ての異なるタイプのベアラに必要とされなくても、例えば、ウェブ閲覧やビデオストリーミング用のベアラがセキュリティなどを必要としなくても、ｅＮｏｄｅＢ及びＳＥＧＷに重い処理負荷をかけることになる。加えて、アプリケーション層にセキュリティを提供する用途もあり、ベアラ向けのトランスポートレベルセキュリティをこれらの場合に使用することはリソースの無駄に思われる。
【課題を解決するための手段】
【０００８】
本発明によって、ベアラレベルのセキュリティ設定の動的選択が可能になる。
【０００９】
これら及び他の利点は、少なくとも１つのアクセスポイント及び少なくとも１つのゲートウェイデバイスを含む移動体通信ネットワークで使用される方法により達成される。本方法は、ネットワークコンポーネントによって専用ベアラ信号のために必要とされるセキュリティ設定を決定するステップと、通信を確立するために必要とされるノードに決定を通信するステップと、アクセスポイントとゲートウェイデバイスとの間で必要とされるようなセキュアプロトコルをアクセスポイントによって構成し又は選択するステップとを備え、決定は、使用中のネットワークの配置及び／又はネットワークオペレータポリシーのうちの１つ又は複数に基づいている。一実施形態によると、ネットワークコンポーネントは、プロキシコールセッション制御機能（Ｐ－ＣＳＣＦ）、問い合わせコールセッション制御機能（Ｉ－ＣＳＣＦ）、サービングコールセッション制御機能（Ｓ－ＣＳＣＦ）又はＩＭＳアプリケーションサーバ（ＡＳ）のうちの１つ又は複数であるアプリケーションレベルのコンポーネントである。ネットワークコンポーネントはＰＣＲＦにセキュリティニーズを送信する。好ましくは、セキュリティを必要とするセッションは、アクセスポイントとゲートウェイデバイスとの間の暗号化と共にセキュアプロトコルを用いる。一実施形態では、セキュリティの必要性が小さいセッションは、メッセージ認証及びヌル暗号化と共にセキュリティプロトコルを使用する。
【００１０】
一般的に、いずれのノードがセキュリティの必要性を決定するのかに応じて、種々のプロトコル及びノードが変更される。セッションが保護される必要があるか否かをネットワークコンポーネントが決定する場合、以下の情報が使用される：暗号化がアクティブ化されているか否か、暗号化レベル、メッセージ認証がアクティブ化されているか否か、メッセージ認証レベル。ネットワークコンポーネントは、セッションの確立に関連するシグナリングのセッション記述プロトコル（ＳＤＰ）部分に含まれている情報に基づいてセキュリティを決定してもよい。セキュリティニーズに関する追加的な標識を含むアプリケーシ

ョンサーバ（ＡＳ）に基づいて他のネットワークコンポーネントがセキュリティを判断することも可能である。Ｓ－ＣＳＣＦは、ＡＡ－リクエスト（ＡＡＲ）メッセージの新たなパラメータにセキュリティ情報をマッピングするＰ－ＣＳＣＦに標識を転送する場合に、その標識を使用する。

【００１１】

本発明の第２の態様によると、ネットワークコンポーネントはＰＣＲＦ（ポリシー制御及び課金ルール機能）である。ＰＣＲＦは、Ｒｅ－Ａｕｔｈ－Ｒｅｑｕｅｓｔ（ＲＡＲ）メッセージのセキュリティ情報をＳＡＥ－ＧＷに送信し、ＳＡＥ－ＧＷは、当該情報を移動性管理エンティティ（ＭＭＥ）に転送し、ＭＭＥは、最終的に、アクセスポイントとゲートウェイデバイスとの間に確立すべきベアラに関する追加的な情報と共に、リクエストされたセキュリティ設定をアクセスポイントに通知する。アクセスポイントは、リクエストされたセキュリティ設定及び確立すべきベアラ信号のために必要なトランスポートアドレス情報と、ゲートウェイデバイスのＩＰアドレスのアドレス情報と、任意的にベアラのユーザデータグラムプロトコル（ＵＤＰ）ポートと、に関する情報を含み、この情報に基づいて、アクセスポイントは、新たなＩＰｓｅｃの関連性記述（relationship description）、即ちＩＰＳｅｃセキュリティアソシエーション（Security Association；ＳＡ）が確立される必要があるか否か、又は既存のＩＰｓｅｃ　ＳＡが未修正のまま使用可能であるか若しくは更新される必要があるかをチェックする。本方法はさらに、異なるベアラ信号に異なるトランスポートアドレス情報を使用するステップを備えてもよい。ゲートウェイデバイスはローカルＩＰネットワークアドレスを選択して、これを、ベアラ確立シグナリングの一部としてアクセスポイントにシグナリングする。ゲートウェイデバイスは、マルチホーミングに局所的に基づいている個別の論理ＩＰアドレスを有してもよく、また、リクエストされたセキュリティ設定に応じて異なるローカルＩＰアドレスを選択する論理ユニットを備える。好ましくは、ＧＰＲＳトンネリング（ＧＴＰ）プロトコルが使用されてもよい。本方法はさらに、ＧＰＲＳトンネリング（ＧＴＰ）プロトコルを変更するステップと、異なるベアラに使用され、かつエンドノード間にシグナリングされるＵＤＰポートを動的に選択するステップとを備えてもよい。アクセスポイントは、生成された無線ベアラと、使用すべきＧＴＰトンネル間のバインディングを生成するように構成されている。

【００１２】

ゲートウェイによりトラフィックセレクタを使用してトラフィックを異なるＩＰｓｅｃ　ＳＡにマッピングすることで、トラフィックがダウンリンク内で異なるＩＰｓｅｃ　ＳＡにマッピングされてもよい。ＰＣＲＦは、様々なベアラについていかなるセキュリティレベルが必要であるかを決定するために必要とされるポリシーを含んでもよい。

【００１３】

セキュリティ設定に関する決定は、異なるタイプのアクセスポイント間を移動するユーザ機器（ＵＥ）に基づいて更新されてもよい。アクセスポイントは、ハンドオーバ及びリロケーションシグナリングの一部として新たなパラメータを受信する。アクセスポイントは、インカミングのハンドオーバリクエストの標識を受信すると、当該アクセスポイントへハンドオーバされるべきアクティブなベアラの全てについて必要とされるサービングＧＷアドレス及びセキュリティ設定に関する情報をさらに受信する。

【００１４】

一実施形態において、アプリケーションレベルのコンポーネントは、セッション記述プロトコル（ＳＤＰ）におけるレベルに関する標識を含み、かつＰ－ＣＳＣＦに送信するセキュリティレベルを選択する。当該情報又はその一部は、ＳＤＰのＰ－ＣＳＣＦからＰＣＲＦへのＲｘ＋／Ｒｘインタフェース、Ｒｘ＋／ＲｘインタフェースのＤＩＡＭＥＴＥＲプロトコル、ＰＣＲＦとＳＡＥ－ＧＷ又はＳＡＥ－ＧＷのＰＤＮゲートウェイ部分間のＳ７／Ｇｘインタフェース、ＳＡＥ-ＧＷとＭＭＥ間のＳ１１インタフェース、ＭＭＥとｅＮｏｄｅＢ間のＳ１－ＭＭＥインタフェースのうちの１つ又は複数で送信される。

【００１５】

本発明はまた、移動局及び通信ネットワークに対して信号を送受信するように適合される基盤デバイスに関し、当該デバイスは、メモリと、処理構成と、専用ベアラ信号を受信／送信するための受信機／送信機構成とを備える。受信機はさらに、決定されるセキュリティ設定を受信するように構成され、当該決定は、ネットワークにおけるネットワークコンポーネントにより、使用中のネットワークの配置及び／又は専用ベアラ信号について必要とされるネットワークオペレータポリシーのうちの１つ又は複数に基づいてなされる。また、受信機はさらに、デバイスとゲートウェイデバイスとの間で必要なセキュアプロトコル（ＩＰｓｅｃ）を構成する手段を含む。

【００１６】

本発明はまた、様々なアプリケーション及び現在使用中のネットワークの配置についてのオペレータポリシーに応じたセキュリティニーズリクエストの標識についての信号を受信する手段、を備える通信ネットワークにおける機能要素（ＰＣＲＦ）に関する。機能要素は、ネットワークノードへのベアラ確立シグナリングにこの標識を含めるための手段と、アプリケーションニーズ及び／又は現在使用中のネットワークに応じてセキュリティレベルが選択されることと、セキュリティが必要とされるか否か及び適用すべきセキュリティレベルを決定する手段を含むロジック部と、を備える。アプリケーションレベルのコンポーネントは、Ｐ－ＣＳＣＦ、ＩＭＳ　ＡＳのうちの１つ又は複数であってもよく、セキュリティニーズがベアラに適用されるべきことを示すように構成される。ネットワークノードとは、ＭＭＥ、ｅＮｏｄｅＢ又はＳＡＥ－ＧＷのうちの１つ又は複数を含む。

【００１７】

本発明はまた、移動体通信ネットワークにおける使用のためのデータ構造に関し、ネットワークは少なくとも１つのアクセスポイントと、少なくとも１つのゲートウェイデバイスと、少なくとも１つのネットワークコンポーネントとを含み、ネットワークコンポーネントは、専用ベアラ信号のために必要とされるセキュリティ設定を決定するように構成され、データ構造は、暗号アクティブ化ステータス、暗号化レベル、メッセージ認証アクティブ化及び／又はメッセージ認証レベルに関する情報を含む。

【００１８】

いわゆる当業者であれば、上述したアクセスポイントが、本発明をＷＬＡＮや類似のアクセスポイントに限定するものではなく、ネットワークアクセスの構成に関連するものに過ぎないことを理解するであろう。

【図面の簡単な説明】

【００１９】

本発明は多数の図面を参照してより詳細に説明される。

【００２０】

【図１ａ】３ＧＰＰのＳＡＥ／ＬＴＥ標準化対象としてこれまでに合意された従来のアーキテクチャを示している。

【図１ｂ】３ＧＰＰのＳＡＥ／ＬＴＥ標準化対象としてこれまでに合意された従来のアーキテクチャを示している。

【図２】本発明によるネットワークである。

【図３】従来技術による信号フロー図である。

【図４】本発明による信号フロー図である。

【図５】本発明によるステップを図示するフロー図である。

【図６】本発明による基盤ノードデバイスを概略的に図示するブロック図である。

【図７】本発明によるアクセスポイントデバイスを概略的に図示するブロック図である。

【図８】本発明による機能要素を概略的に図示するブロック図である。

【発明を実施するための形態】

【００２１】

以下、本発明について、ＬＴＥ及びＳＡＥを基準にして例示される一般的な解決策を参照して説明する。しかしながら、本発明の教示が、本発明の教示を実行する能力を具備するノード及び基盤エンティティを有する任意のネットワークに適用可能であることが認識

されるであろう。

【００２２】

概して、Ｓ１インタフェースにおける暗号化及び他のセキュリティ設定の動的制御を可能にするために必要な追加がプロトコル及びアーキテクチャになされる。

【００２３】

図２は、ネットワークにおける本発明を図示している。ネットワーク２００は、インターネット２０１及びイントラネット２０２の部分からなる。インターネット２０１（又は他のパブリックかつ安全でないネットワーク）は、安全なイントラネット２０２におけるｅＮｏｄｅＢ２０３と、ＳＡＥコアネットワーク要素（即ちＭＭＥ及びサービングゲートウェイ）との間の接続性の一部を提供するために使用されることができる。この場合、ｅＮｏｄｅＢ２０３（ｅＮＢ）はセキュリティゲートウェイ（ＳＥＧＷ）２０４を介してイントラネット２０２に接続される。ＩＰｓｅｃトンネル２０５を使用して通信は可能となり、保護される。ＳＥＧＷ２０４は、ＳＡＥ－ＧＷ２０６及びＭＭＥ２０７に対するｅＮｏｄｅＢ２０３の通信を可能にし、ＳＡＥ－ＧＷ２０６及びＭＭＥ２０７はまた相互接続されている。ＳＡＥ－ＧＷ２０６は、ＰＣＲＦ２０８との間で通信し、ＰＣＲＦ２０８は、Ｐ－ＣＳＣＦ２０９との間で通信し、Ｐ－ＣＳＣＦ２０９は、ＩＰマルチメディアサブシステム（ＩＭＳ）ＣＮ２１０との間で通信し、ＩＰマルチメディアサブシステム（ＩＭＳ）ＣＮ２１０は、ＰＣＲＦ２０８は１つ以上のＩＭＳアプリケーションサーバ（ＡＳ）２１１と通信する。

【００２４】

例えば、ボイスコール向けなどの、様々なアプリケーション及び（／又は）現在使用中のネットワークの配置（deployment）についてのオペレータ（operator；運用者）のポリシーに応じて、アプリケーションレベルのコンポーネント（例えば、ＩＭＳ　ＶｏＩＰコールの場合のＰ－ＣＳＣＦ又はＩＭＳ　ＡＳ）は、セキュリティをベアラに適用する必要があることを示す（indicate）ことができる。このことは、ＰＣＲＦ２０８にシグナリングされ、ＭＭＥ２０７、ｅＮｏｄｅＢ２０３及びＳＡＥ－ＧＷ２０６へのベアラ確立シグナリングに当該標識（indication）が含められる。このことは、セキュリティレベルが、アプリケーションのニーズ及び現在使用中のネットワークに応じて選択されることを意味している。このように、例えばウェブ閲覧セッションは、例えばｅＮｏｄｅＢとＳＡＥ－ＧＷとの間のヌル暗号化を使用することによって、処理リソースを節約することで実行可能である。もう１つの可能性は、ＰＣＲＦがオペレータポリシーと、セキュリティが特定のアプリケーションに必要であるか否かを決定するために必要とされるロジックとを含むことである。ロジック部は実質的に上記と同じである、即ちＰＣＲＦは、例えばリクエストされたベアラ、ベアラ特性、及びベアラをリクエストするアプリケーションに基づいて、セキュリティが必要とされるか否かと、適用するセキュリティレベルとを判定する手段を備える。

【００２５】

加えて、Ｐ－ＣＳＣＦは、アプリケーション機能（ＡＦ）セッションが属する特定のサービスを示す順序をＡＡ－リクエストメッセージに含めてもよい。この情報は次いで、選択され、かつ他のノードに通信されるセキュリティレベルを決定するためにＰＣＲＦによって使用可能である。加えて、ＰＣＲＦは、確立されるセッションについて記述するセッション記述プロトコル（ＳＤＰ）全体を受信してもよく、ＳＤＰの一部はセキュリティレベルの選択のために使用可能である。

【００２６】

ポリシー及び課金制御（ＰＣＣ）ルール機能（ＰＣＲＦ）の決定は、以下のうちの１つ以上に基づいてもよい：

－Ｒｘ＋／Ｒｘリファレンスポイントを介してＡＦから取得されたセッション及びメディア関連情報；

－Ｓ７／Ｇｘリファレンスポイント上でポリシー及び課金施行機能（ＰＣＥＦ）から取得されたベアラ及び加入者関連情報。ＳＡＥ－ＧＷは、上記の例示的ネットワークシナリオ

でＰＣＥＦとして機能する；
－ＰＣＲＦが、構成により、又は（ＳＰＲからの）Ｓｐリファレンスポイントを介して知り得る加入者及びサービス関連データ；
－ＰＣＲＦにおける事前構成済みの情報。
【００２７】
これらのルール（又はサブセット）はまた、セキュリティレベルを選択する場合に使用されることができる。
【００２８】
より詳細には、図５に示されている、実質的に本発明の主なステップは以下のとおりである：
・５０１：アプリケーションレベルノード若しくはＰＣＲＦノードのうちのいずれか１つ又は複数が、専用ベアラについて必要とされるセキュリティ設定を識別する。この決定は、現在使用中のネットワークと、様々なアプリケーション向けのネットワークオペレータポリシーに基づいている、
・５０２：上記決定は、必要なノードの全てへ通信される、
・５０３：最終的に、ｅＮｏｄｅＢとＳＥＧＷとの間での必要に応じてｅＮｏｄｅＢはこの情報を受信し、ＩＰｓｅｃセキュリティアソシエーション（ＳＡ）を構成する。
【００２９】
セキュリティを必要とするセッションは、ｅＮｏｄｅＢとＳＥＧＷとの間の暗号化と共にＩＰｓｅｃを使用する。セキュリティの必要性が小さいセッションは、例えば、メッセージ認証及び「ヌル暗号化」と共にＩＰｓｅｃを使用することができる。このことは、実質的にｅＮｏｄｅＢ及びＳＥＧＷの双方における処理要件を削減することになる。
【００３０】
別の代替案は、ＩＰｓｅｃトンネル外ではセキュリティを必要としないデータを送信することであるが、最も可能性の高いケースはおそらく、メッセージ認証と共に「ヌル暗号化」を使用することであろう。
【００３１】
このことは、（少なくとも）２つの異なるＩＰｓｅｃトンネル（又はＩＫＥ　ＳＡ向けの２つの異なるＩＰｓｅｃ　ＳＡ）が、一方は暗号化あり、もう一方は暗号化なしで、ｅＮｏｄｅＢとＳＥＧＷとの間で確立される必要があることを意味している。ＩＰｓｅｃ　ＳＡの数は、例えば異なる暗号化レベルや異なるメッセージ認証レベルを有する必要がある場合には、２より大きくなり得る。主要なポイントは、ｅＮｏｄｅＢとＳＥＧＷとの間で必要なＩＰｓｅｃ　ＳＡの数は、ｅＮｏｄｅＢとＳＥＧＷとの間でトランスポートされた異なるベアラに必要な異なるセキュリティ設定の数に基づいている点である。
【００３２】
ＩＰｓｅｃ　ＳＡの確立を取り扱う自動的な方法について以下に概説する。
【００３３】
本発明は、ｅＮｏｄｅＢとＳＥＧＷとの間でトランスポートされる異なるベアラの、アップリンク及びダウンリンクの双方のトラフィックについて、ＩＰｓｅｃ　ＳＡの選択を制御してｅＮｏｄｅＢとＳＥＧＷとの間で使用するための方法、手順、プロトコル及びノード修正（node　modifications）を提供する。
【００３４】
セキュリティが必要であるか否かをいずれのノードが決定するかに応じて、種々のプロトコル及びノードが修正される必要がある。例えば、アプリケーションレベルのコンポーネントがセキュリティレベルを選択すると、これに関する標識はＳＤＰに含まれた上でＰ－ＣＳＣＦに渡され、Ｐ－ＣＳＣＦは例えばＳＤＰの情報をＲｘ＋／ＲｘインタフェースでＰＣＲＦに渡す。他の可能性は、Ｒｘ＋／Ｒｘインタフェースで、ＤＩＡＭＥＴＥＲプロトコル自体にいくつかの情報を含めることである。別の例は、Ｓ７／Ｇｘインタフェース及びこのインタフェースで使用されているプロトコル向けの類似のアプローチである。
【００３５】

次に図４を参照し、アプリケーションレベルのコンポーネント（例えば、ＩＭＳ　ＣＮ又はＩＭＳ　ＡＳにおけるＳ－ＣＳＣＦ）がセッションの保護が必要か否かを決定し、及び例えばＳＤＰ内でＰ－ＣＳＣＦ（図４に示されている後者）に送信されたことを示す（indicate）ことを想定すると、シーケンスにおいてハイライトされている、以下のメッセージ及び対応するノードロジックが拡張（enhance）される必要がある。図示されている「新たなパラメータ」は、示されているメッセージ及びプロトコルにおいて必要な追加である。これは、ｅＮｏｄｅＢとＳＥＧＷとの間で使用されるセキュリティに関連する様々な構成レベルを含むことができ、また、例えば以下の情報を含むことができる：

ａ　暗号化がアクティブ化されたか否か、

ｂ　暗号化レベル、

ｃ　メッセージ認証がアクティブ化されたか否か、

ｄ　メッセージ認証レベル。

【００３６】

アプリケーションレベルのコンポーネント（例えば、Ｓ－ＣＳＣＦ又はＡＳ）は、確立される（又は修正される）セッションのセッション記述プロトコル（ＳＤＰ）に含まれている情報に基づいて、当該セッションおよび関連ベアラのうちの１つ以上のためにセキュリティが必要であると決定することができる。また、当該決定は、例えばＳＤＰにおいてセキュリティが必要とされることと追加的な標識上に含むＡＳに基づいてもよく、そして、Ｓ－ＣＳＣＦはＰ－ＣＳＣＦに当該標識を転送する際に当該標識を使用する。Ｐ－ＣＳＣＦは、Ｒｘ＋／Ｒｘインタフェース上でＰＣＲＦに送信されるＡＡリクエスト（ＡＡＲ）メッセージにおける新たなパラメータに、上記セキュリティ情報をマッピングする。ＰＣＲＦは、Ｒｅ－Ａｕｔｈ－Ｒｅｑｕｅｓｔ（ＲＡＲ）メッセージ内のセキュリティ情報をＳ７／Ｇｘインタフェース上でＳＡＥ－ＧＷに送信し、ＳＡＥ－ＧＷは次いでＳ１１インタフェース上で当該情報をＭＭＥに転送し、最終的にＭＭＥは、ｅＮｏｄｅＢとサービングＧＷ（即ち、ｅＮｏｄｅＢに対して可視的なＳＡＥ－ＧＷの一部）との間で確立すべきベアラに関する他の情報の全てと共に、リクエストされたセキュリティ設定について（Ｓ１－ＭＭＥインタフェースで）ｅＮｏｄｅＢに通知する。

【００３７】

この段階で、ｅＮｏｄｅＢは、確立すべきベアラに対する、リクエストされたセキュリティ設定と、必要とされるトランスポートアドレス情報とを知っている。トランスポートアドレス情報は、サービングＧＷのＩＰアドレスと、任意的にベアラのサービングＧＷＵＤＰポートからなる。この情報に基づいて、ｅＮｏｄｅＢは、新たなＩＰｓｅｃ　ＳＡが確立される必要があるか否か、又は既存のＩＰｓｅｃ　ＳＡが未修正のまま使用可能であるか若しくは既存のＩＰｓｅｃ　ＳＡが更新される必要があるか否か、をチェック可能である。ここでの主な問題は、確立されたベアラが、双方向に、即ちｅＮｏｄｅＢによるアップリンクと、ＳＥＧＷによるダウンリンクにおいて、正確なＩＰｓｅｃ　ＳＡにマッピングされることを保証することである。アップリンク方向は、ここでは、ＵＥからネットワークへの方向、即ちこの場合は、ｅＮｏｄｅＢからＳＥＧＷへの方向を意味しており、ダウンリンク方向はこれと反対方向を意味している。ＳＥＧＷは、関連するシグナリングがＳＥＧＷを介して透過的に送信されたとしても、ベアラ確立の一部ではない。ｅＮｏｄｅＢは、ｅＮｏｄｅＢ及びＳＥＧＷの双方におけるＩＰｓｅｃ　ＳＡについてのトラフィックセレクタ（ＴＳ）が、確立されたベアラについてサービングＧＷのトランスポートアドレス情報をマッチングすることを保証する必要がある。

【００３８】

ＴＳｅｓは、（ＴＳｉ（Ｔｒａｆｆｉｃ　Ｓｅｌｅｃｔｏｒ　ｉｎｉｔｉａｔｏｒ）（トラフィックセレクタイニシエータ）と称される）アップリンクと、（ＴＳｒ（Ｔｒａｆｆｉｃ　Ｓｅｌｅｃｔｏｒ　ｒｅｓｐｏｎｄｅｒ）（トラフィックセレクタレスポンダ）と称される）ダウンリンクにおいて別個に定義される。ＴＳｅはＩＰｓｅｃ　ＳＡごとに定義され、ＩＰトラフィック及びＩＰプロトコルメッセージが異なるＩＰｓｅｃ　ＳＡにどのようにマッピングされるかを決定するために効果的に使用される。ＴＳｅｓに含まれ

ている情報は、ＩＰアドレス（レンジ）、ＴＣＰ／ＵＤＰポート（レンジ）及びプロトコル情報である。このことは、異なるセキュリティ設定を必要とする異なるベアラが異なるトランスポートアドレス情報を使用しなければならないことを意味している。これが必要とされるのは、ＳＥＧＷがダウンリンクにおいて正確なセキュリティ設定によって正確なＩＰｓｅｃ　ＳＡにトラフィックをマッピングできるようにするためである。

【００３９】

異なるベアラに異なるトランスポートアドレス情報を使用するという上述したニーズは、ＩＰアドレス又はＵＤＰポートのいずれかが、ベアラごとに異なるものである必要があることを意味している。ＳＡＥの場合、ネットワークにより開始されるベアラアクティブ化手順が使用されるという可能性が非常に高く、またローカルＩＰネットワークアドレスを選択して、これを、ベアラ確立シグナリングの一部としてｅＮｏｄｅＢにシグナリングするのはサービングＧＷである。このことは、サービングＧＷは、局所的に例えばマルチホーミングに基づいた個別の論理ＩＰアドレスを有し、かつリクエストされたセキュリティ設定に応じて異なるローカルＩＰアドレスを選択するためのロジックを有する必要があることを意味している。この代替案は、ある程度ＬＴＥ／ＳＡＥアーキテクチャで再使用されることになる既存のＧＰＲＳトンネリングプロトコル（ＧＴＰ）によって可能となるであろう。

【００４０】

ＧＴＰプロトコルの変更を意味するもう１つのオプションは、異なるベアラに使用されるＵＤＰポートもまた動的に選択され、エンドポイント（即ち、サービングＧＷ及びｅＮｏｄｅＢ）間でシグナリングされることである。現在、ＧＴＰプロトコルは、１つの固定的なＵＤＰポートを使用するように仕様化されている。この場合、サービングＧＷは、リクエストされたセキュリティ設定に応じて異なるローカルＵＤＰポートを選択するためのロジックを有することになる。

【００４１】

したがって、上記機構を使用して、ｅＮｏｄｅＢは、ＩＰｓｅｃ　ＳＡのＴＳｅがｅＮｏｄｅＢ及びＳＥＧＷの双方で正確に更新されることを保証していた。次のステップは、トラフィックもまたこれらのＩＰｓｅｃ　ＳＡに正確にマッピングされることを保証することである。ｅＮｏｄｅＢはまた、生成された無線ベアラと、使用されるＧＴＰトンネル間のバインディングを生成する。ＧＴＰトンネル情報は、使用されるＩＰアドレス（及びＵＤＰポート）を含むため、ｅＮｏｄｅＢが、特定の無線ベアラを使用してＵＥからトラフィックを受信する場合、これをＧＴＰトンネルにマッピングすることができる。トラフィックがＩＰアドレス及びＵＤＰポート情報によってカプセル化される場合、ｅＮｏｄｅＢにおけるＩＰｓｅｃの実装は、正確なＩＰｓｅｃ　ＳＡを発見するトラフィックセレクタを使用して、ＳＥＧＷに対してトラフィックを送信する。

【００４２】

ダウンリンクでの異なるＩＰｓｅｃ　ＳＡへのトラフィックのマッピングはＳＥＧＷによって実行される。この場合、ＳＥＧＷは、確立されたＧＴＰトンネルに関する情報を全く有しておらず、ｅＮｏｄｅＢに対してダウンリンクトラフィックを異なるＩＰｓｅｃ　ＳＡにマッピングするために（ｅＮｏｄｅＢによって更新されるような）トラフィックセレクタを使用する。これは標準的な機能であるが、異なるＵＤＰポートが異なるベアラに使用される場合にのみ容易に適用される。そうでなければ、ｅＮｏｄｅＢは、（少なくとも）２つの異なるＩＰアドレスを有することも必要であろう。

【００４３】

例えば、決定を行うポイントがＩＭＳ　ＣＮ（例えば、Ｉ－ＣＳＣＦ又はＳ－ＣＳＣＦ）であると判断される場合には、これらのノードにロジックが追加される必要があり、また送信されるＳＤＰは、ＩＭＳ　ＣＮにおけるノードによって修正される必要がある、即ち決定を行うポイントに応じて、異なるプロトコル及びノードのロジックが更新される必要がある。

【００４４】

上記のように、さらなる追加的なアプローチは、Ｒｘ＋／Ｒｘインタフェースを未修正のままに維持し、上述したように、異なるベアラのために必要とされるセキュリティレベルを判断するために必要なポリシーをＰＣＲＦに含有させることである。

【００４５】

セキュリティ設定に関する決定はその時点のネットワークの配置及び（／又は）使用中のｅＮｏｄｅＢのタイプに基づいてもよいため、セキュリティ設定はまた、異なるタイプのｅＮｏｄｅＢ間を（即ち、ソースｅＮｏｄｅＢからターゲットｅＮｏｄｅＢへ）移動するＵＥ２２０を理由として、更新されることもある。このことは、ターゲットｅＮｏｄｅＢが、ハンドオーバ及びリロケーションシグナリングの一部としても上記の新たなパラメータを受信する必要があることから、同一の論理がこれらの場合にも適用可能であることを意味している。これを実行することによって、本発明は、上記以外の多数のケース、即ち初期のベアラ確立のケースもカバーすることができる。ターゲットｅＮｏｄｅＢは、インカミングのハンドオーバリクエストの標識を受信する場合、このｅＮｏｄｅＢへハンドオーバされるアクティブベアラの全てについて必要とされるサービングＧＷアドレス及びセキュリティ設定に関する情報をも受信する。ターゲットｅＮｏｄｅＢは次いで、上記のように、即ち、新たなＩＰｓｅｃ　ＳＡが確立される必要がある場合、又は既存のＩＰｓｅｃ　ＳＡが未修正のまま使用可能な場合、若しくは既存のＩＰｓｅｃ　ＳＡが更新される必要がある場合に、同じステップを実行することができる。

【００４６】

図６は、本発明に係る基盤ノードの概略的なブロック図を示しており、処理ユニット６０１は通信データ及び通信制御情報を取り扱う。基盤ノード６００はさらに、揮発性メモリ（例えばＲＡＭ）６０２及び／又は不揮発性メモリ（例えば、ハードディスクやフラッシュメモリ）６０３と、インタフェースユニット６０４とを備える。基盤ノード６００はさらに、ダウンストリーム通信ユニット６０５及びアップストリーム通信ユニット６０６を備えてもよく、各々はそれぞれの接続インタフェース（図示せず）を具備している。基盤ノードにおける全ユニットは、直接、又は処理ユニット６０１を介して間接的に相互に通信可能である。ネットワークに付随する移動体ユニット及び他のネットワーク要素に対する通信を取り扱うためのソフトウェアが少なくとも部分的にこのノードで実行され、ノードに記憶されてもよい。しかしながら、このソフトウェアはまた、ノードの開始時や、例えばサービスインターバル中の後段において動的にロードされてもよい。ソフトウェアは、コンピュータプログラム製品として実現され、着脱可能でコンピュータ読み取り可能な媒体、例えば、ディスケット、ＣＤ（コンパクトディスク）、ＤＶＤ（ディジタルビデオディスク）、フラッシュ又は類似のリムーバブルメモリ媒体（例えば、コンパクトフラッシュ、ＳＤセキュアディジタル、メモリスティック、ミニＳＤ、ＭＭＣマルチメディアカード、スマートメディア、トランスフラッシュ、ＸＤ）、ＨＤ－ＤＶＤ（高品位ＤＶＤ）やブルーレイＤＶＤ、ＵＳＢ（ユニバーサルシリアルバス）ベースのリムーバブルメモリメディア、磁気テープメディア、光学記憶メディア、光磁気メディア、バブルメモリに配信及び／又は記憶され、あるいはネットワーク（例えば、イーサネット、ＡＴＭ、ＩＳＤＮ、ＰＳＴＮ、Ｘ．２５、インターネット、ローカルエリアネットワーク（ＬＡＮ）、又は基盤ノードにデータパケットをトランスポート可能な類似のネットワーク）を介する伝搬信号として配信可能である。

【００４７】

図７に極めて概略的に図示されている基盤デバイス７００、例えばｅＮｏｄｅＢは、移動局及び通信ネットワークに対して信号を送受信するように適合されている。このデバイスは、プロセッサ７０１と、メモリユニット７０２と、専用ベアラ信号をそれぞれ受信／送信するための受信機及び送信機の構成、即ちインタフェース７０３及び７０４とを備える。メモリは、決定されたセキュリティ設定を受信するようにデバイスを構成するための命令セットを有する。上記のような決定は、ネットワークにおけるネットワークコンポーネントにより、使用中のネットワークの配置と、専用ベアラ信号について必要とされるネットワークオペレータポリシーのうちの１つ又は複数に基づいてなされる。プロセッサは

さらに、デバイスとゲートウェイデバイスとの間で必要とされるようなセキュアプロトコル（ＩＰｓｅｃ）を構成することを命令するように構成される。

【００４８】

機能要素８００、例えばＰＣＲＦは、図８に極めて概略的に図示されており、以下を備え得る：

・処理構成８０１、

・メモリユニット８０２、

・様々なアプリケーション及び現在使用中のネットワークの配置に対するオペレータポリシーに応じて、セキュリティ設定を示す信号を受信する受信機８０３、

・ネットワークノードへのベアラ確立シグナリングに標識を含めることによって、アプリケーションニーズ及び現在使用中のネットワークに応じてセキュリティレベルを選択する論理ユニット８０４、

・送信機部分８０５、並びに

・セキュリティニーズリクエストに基づいて、セキュリティが必要であるか否かと、適用すべきセキュリティレベルとを決定する手段を含むロジック部８０６。

【００４９】

当然ながら、ロジック部及びユニットは、処理回路を備えてもよい。

【００５０】

特殊なネットワーク基準に固有のこれらの用語は実施形態の例として付与され、同一の機能性を有するエンティティ及びアイテムに関する類似の用語は本発明から除外されるものではないことに留意すべきである。

【００５１】

（略語）

ＡＦ　アプリケーション機能（Application Function）

ＡＶＰ　属性値ペア（Attribute Value Pair CRF Charging Rules Function）

ＣＲＦ　課金ルール機能（Charging Rules Function）

ＩＰ－ＣＡＮ　ＩＰ接続性アクセスネットワーク（IP Connectivity Access Network）

ＰＣＣ　ポリシー及び課金制御（Policy and Charging Control）

ＰＣＥＦ　ポリシー及び課金施行機能（Policy and Charging Enforcement Function）

ＰＣＲＦ　ポリシー及び課金ルール機能（Policy and Charging Rule Function）

ＰＤＦ　ポリシー決定機能（Policy Decision Function）

Ｐ－ＣＳＣＦ　プロキシコールセッション制御機能（Proxy-Call Session Control Function）

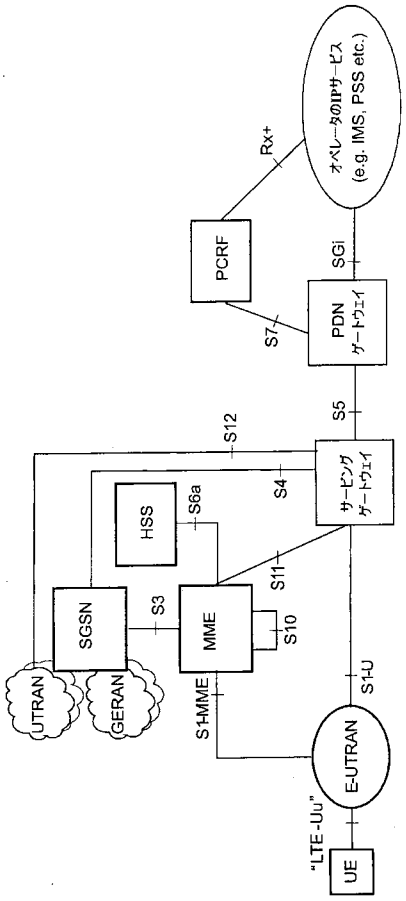
ＱｏＳ　サービス品質（Quality of Service）

ＳＤＦ　サービスデータフロー（Service Data Flow）

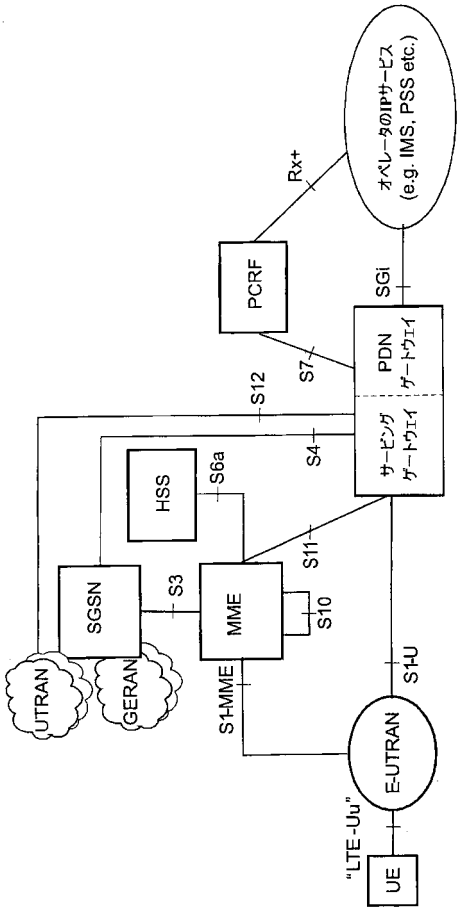
ＳＰＲ　加入者プロファイルレポジトリ（Subscriber Profile Repository）

ＵＥ　ユーザ機器（User Equipment）

【図１ａ】



【図１ｂ】



【図２】

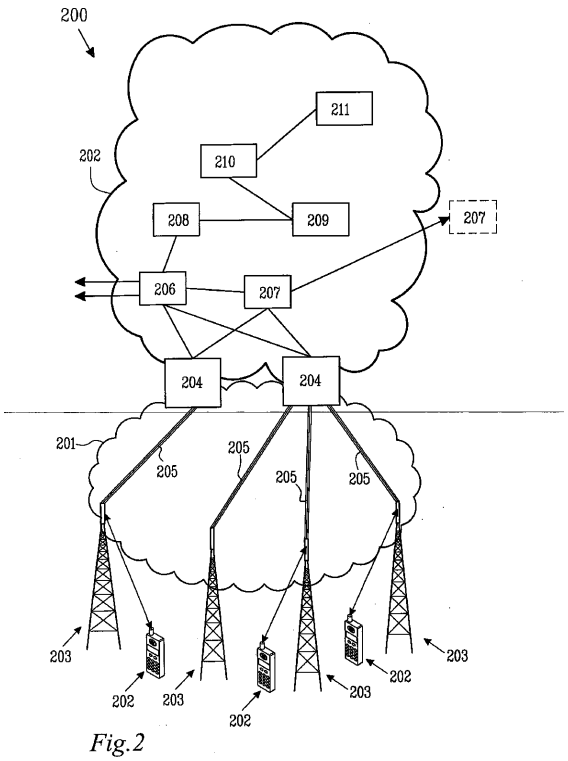
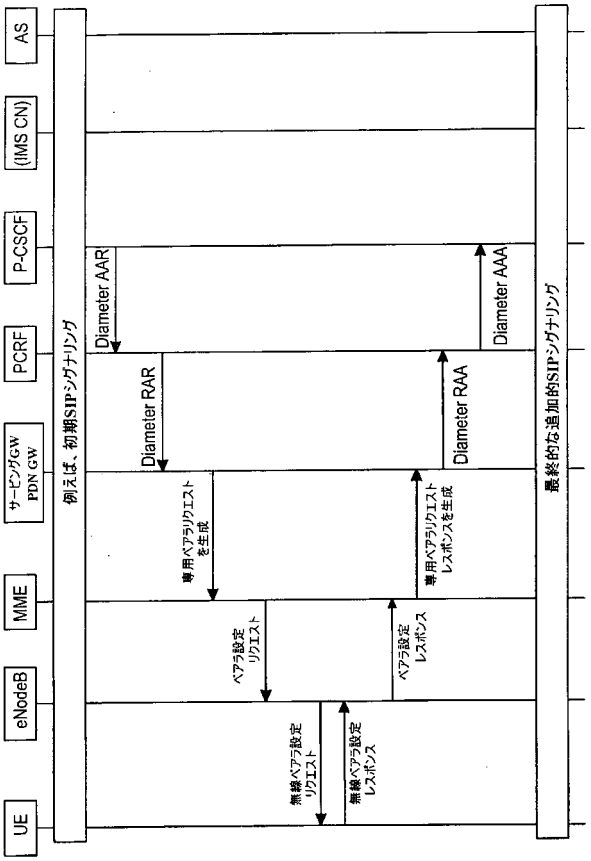
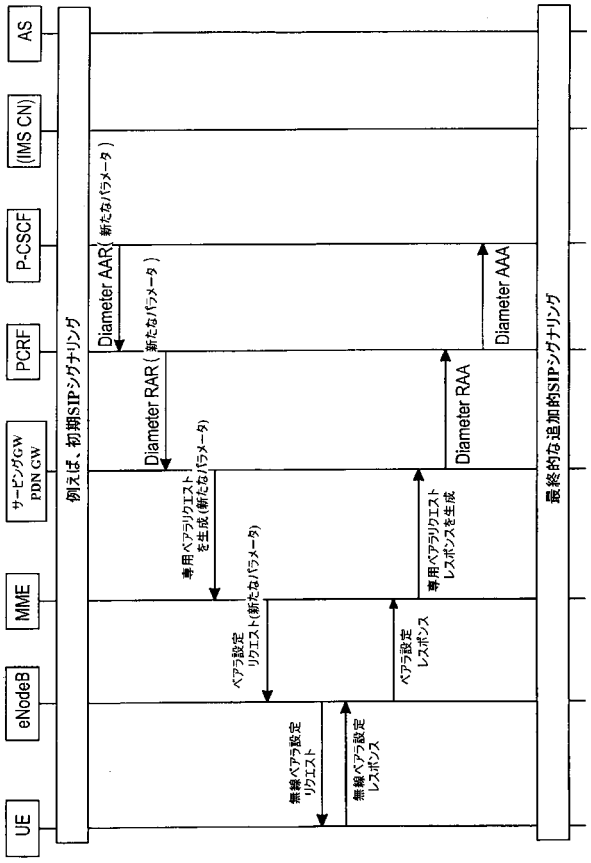


Fig.2

【図３】



【図４】



【図５】

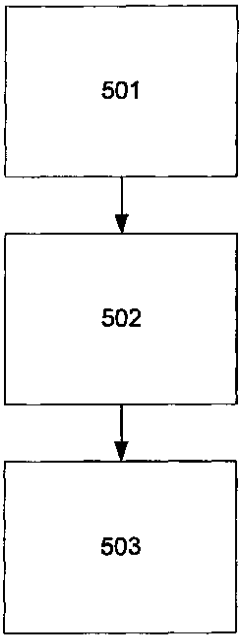


Fig. 5

【図６】

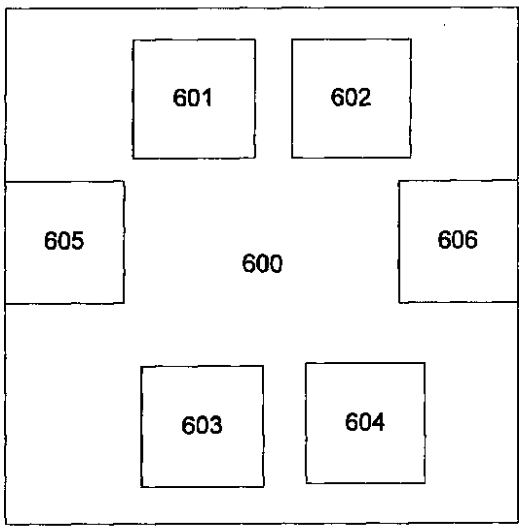


Fig. 6

【図７】

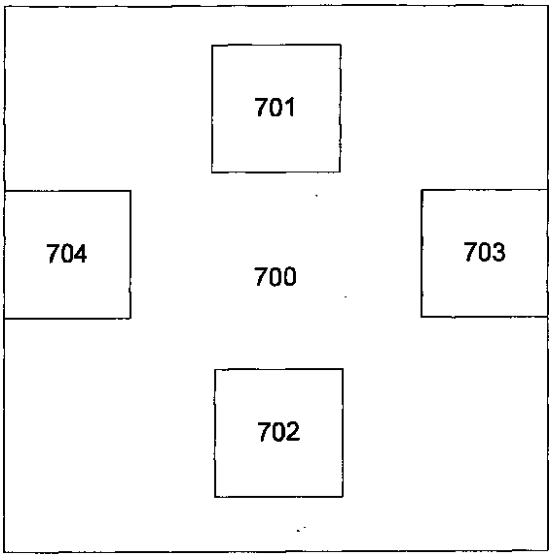


Fig. 7

【図８】

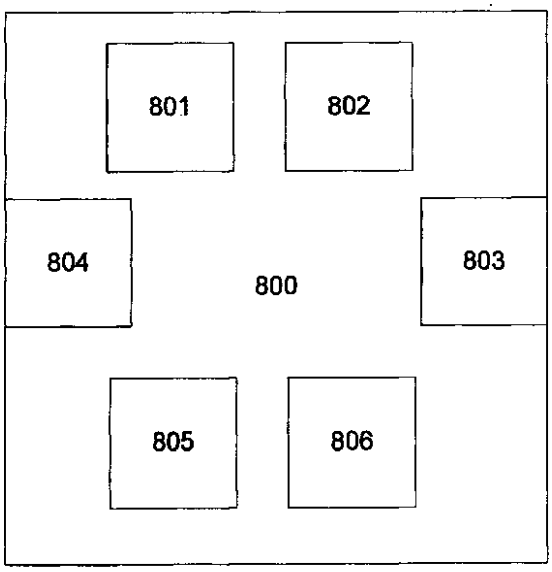


Fig. 8

フロントページの続き

(72)発明者 ナイランデル、トマス
スウェーデン王国 エス－１３９ ３４ ヴェールムデー ヘーグトルプスヴェーゲン ２８
(72)発明者 ヴィクベリ、ヤリ
スウェーデン王国 エス－１５３ ３８ イェールナ スヴァルセーテスヴェーゲン １２
(72)発明者 ジー、オスカー
スウェーデン王国 エスイー－１１８ ６７ ストックホルム マルモルガタン１３エー ４ティーアール

審査官 鈴木 重幸

(56)参考文献 国際公開第２００６／０６９５２２（WO，Ａ１）
特開２００２－０６４４８２（ＪＰ，Ａ）
特開２００７－１２９３７１（ＪＰ，Ａ）
特表２００８－５１７３８８（ＪＰ，Ａ）
国際公開第２００６／０４５３２３（WO，Ａ１）
米国特許第０７０１０６８１（ＵＳ，Ｂ１）
特表２００８－５２６１４４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04B 7/24- 7/26
H04W 4/00-99/00