(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2016-506204
(P2016-506204A)
(43)公表日　平成28年2月25日(2016.2.25)

(51)Int.Cl.		F I			テーマコード（参考）
H04W 12/04	(2009.01)	H04W	12/04		5K067
H04W 72/04	(2009.01)	H04W	72/04	111	

審査請求 未請求　予備審査請求 未請求　（全 22 頁）

(21)出願番号	特願2015-551800 (P2015-551800)
(86)(22)出願日	平成26年1月6日 (2014.1.6)
(85)翻訳文提出日	平成27年8月20日 (2015.8.20)
(86)国際出願番号	PCT/US2014/010273
(87)国際公開番号	WO2014/109968
(87)国際公開日	平成26年7月17日 (2014.7.17)
(31)優先権主張番号	61/750,732
(32)優先日	平成25年1月9日 (2013.1.9)
(33)優先権主張国	米国 (US)

(71)出願人　392026693
株式会社ＮＴＴドコモ
東京都千代田区永田町二丁目１１番１号
(74)代理人　100121083
弁理士　青木　宏義
(74)代理人　100138391
弁理士　天田　昌行
(74)代理人　100158528
弁理士　守屋　芳隆
(74)代理人　100137903
弁理士　菅野　亨
(72)発明者　ジョン　ムー　リョン
アメリカ合衆国　９４３０４　カリフォルニア州　パロ　アルト　ヒルビュー　アベニュー　３２４０

最終頁に続く

(54)【発明の名称】無線基地局間（ｉｎｔｅｒ－ｅＮＢ）キャリアアグリゲーションによる保護された無線アクセス

(57)【要約】
ユーザ装置との通信を保護するプライマリ無線基地局を含む無線基地局間（ｉｎｔｅｒ－ｅＮＢ）キャリアアグリゲーションによる無線アクセスを保護するシステムに関する。プライマリ無線基地局は、基本鍵を生成し、対応する一組の無線ベアラによる通信を保護するために用いる一組の導出鍵を導出する。無線基地局間キャリアアグリゲーションによる無線アクセスを保護するシステムは、セカンダリ無線基地局を含む。セカンダリ無線基地局は、受信した一組の導出鍵の少なくとも一つであって、ＳｅＮＢで使われている一組の無線ベアラの内の一つに対応する導出鍵を用いて、ＵＥとの通信を保護する。

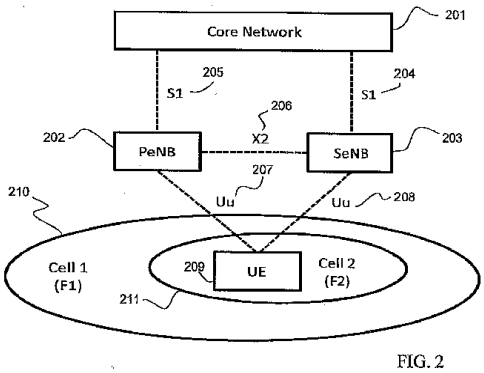


FIG. 2

【特許請求の範囲】
【請求項１】
無線基地局間（ｉｎｔｅｒ－ｅＮＢ）キャリアアグリゲーションによる無線アクセスを保護するシステムであって、
基本鍵を生成し、対応する一組の無線ベアラによる通信を保護するために使われる一組の導出鍵を導出することにより、ユーザ装置（ＵＥ）との通信を保護するプライマリ無線基地局（ＰｅＮＢ）と、
受信した一組の導出鍵の少なくとも一つであって、セカンダリ無線基地局（ＳｅＮＢ）により使われている一組の無線ベアラの内の一つに対応する導出鍵を使って前記ＵＥとの通信を保護するＳｅＮＢと、
を含むシステム。
【請求項２】
請求項１記載の、無線基地局間（ｉｎｔｅｒ－ｅＮＢ）キャリアアグリゲーションによる無線アクセスを保護するシステムであって、導出鍵をＰｅＮＢからＳｅＮＢに送るために用いられる、前記ＰｅＮＢと前記ＳｅＮＢとの間の保護されたインターフェイスをさらに含むシステム。
【請求項３】
請求項１記載の、無線基地局間（ｉｎｔｅｒ－ｅＮＢ）キャリアアグリゲーションによる無線アクセスを保護するシステムであって、
ＰｅＮＢにより管理されている複数の無線基地局をさらに含み、前記複数の無線基地局のそれぞれは、受信した一組の導出鍵の少なくとも一つであって、前記無線基地局のそれぞれにより使われている一組の無線ベアラの内の一つに対応する導出鍵を使ってＵＥとの通信を保護するシステム。
【請求項４】
無線基地局間（ｉｎｔｅｒ－ｅＮＢ）キャリアアグリゲーションによる保護された無線アクセス方法であって、
ユーザ装置（ＵＥ）と通信するプライマリ無線基地局（ＰｅＮＢ）を選択し、
前記ＰｅＮＢにおいて、基本鍵を生成し、それぞれが一組の無線ベアラの内の一つに対応する一組の導出鍵を前記基本鍵から導出し、
前記ＵＥと通信するセカンダリ無線基地局（ＳｅＮＢ）を選択し、
前記ＳｅＮＢにおいて、前記一組の導出鍵からの少なくとも一つであって、前記ＳｅＮＢが使う無線ベアラに対応する導出鍵を、前記ＰｅＮＢから受信する、方法。
【請求項５】
請求項４記載の、無線基地局間（ｉｎｔｅｒ－ｅＮＢ）キャリアアグリゲーションによる無線アクセスを保護するプライマリ無線基地局（ＰｅＮＢ）の使用方法であって、さらに、
前記ベアラが前記ＳｅＮＢにより管理されているいずれかのセルで通信に用いられていないかどうかを判定し、
基本鍵を更新し、前記更新された基本鍵に基づいて一組の導出鍵を再度導出する、方法。
【請求項６】
無線基地局間（ｉｎｔｅｒ－ｅＮＢ）キャリアアグリゲーションによる無線アクセスを保護するプライマリ無線基地局（ＰｅＮＢ）の使用方法であって、
前記ＰｅＮＢにより管理されているセルの中からユーザ装置（ＵＥ）に対するプライマリセル（ＰＣｅｌｌ）を決定し、
前記ＰＣｅｌｌの物理セルＩＤと下りリンク周波数に基づいて前記ＵＥの基本鍵（K_{eNB}）を得て、
前記基本鍵に基づいて前記ＵＥの導出鍵（K_{RRCenc}、K_{RRCint}及びK_{UPenc}）を導出し、
セカンダリ無線基地局（ＳｅＮＢ）により管理されているセルの中から、前記ＵＥのた

めのセカンダリセル（ＳＣｅｌｌ）であって、その下りリンク周波数が前記ＰＣｅｌｌの下りリンク周波数と異なるＳＣｅｌｌを決定し、
ベアラが前記ＳＣｅｌｌによる通信に用いられているか否かを判定し、
前記ベアラがデータベアラか又はシグナリングベアラかに応じて、前記一組の導出鍵の少なくとも一つを、前記ＰｅＮＢと前記ＳｅＮＢとの間の保護された接続を介して、前記ＳｅＮＢへ送る、使用方法。
【請求項７】
請求項６記載の、無線基地局間（ｉｎｔｅｒ－ｅＮＢ）キャリアアグリゲーションによる無線アクセスを保護するプライマリ無線基地局（ＰｅＮＢ）の使用方法であって、さらに、前記ＰｅＮＢにおいて無線基地局内（ｉｎｔｒａ－ｅＮＢ）ハンドオーバを実施することにより、新しいＰＣｅｌｌを決定する、使用方法。
【請求項８】
無線基地局間（ｉｎｔｅｒ－ｅＮＢ）キャリアアグリゲーションによる無線アクセスを保護するセカンダリ無線基地局（ＳｅＮＢ）の使用方法であって、
前記セカンダリ無線基地局（ＳｅＮＢ）により管理されているセルの中から、ユーザ装置（ＵＥ）のためのＳＣｅｌｌであって、その下りリンク周波数がＰＣｅｌｌの下りリンク周波数と異なるＳＣｅｌｌを決定し、
ベアラが前記ＳＣｅｌｌによる通信に用いられているか否かを判定し、
前記ベアラがデータベアラか又はシグナリングベアラかに応じて、一組の導出鍵の少なくとも一つを、前記ＰｅＮＢと前記ＳｅＮＢとの間の保護された接続を介して、前記ＰｅＮＢから受信し、
前記一組の導出鍵の少なくとも一つにより前記ベアラを保護する、使用方法。
【請求項９】
請求項８記載の、無線基地局間（ｉｎｔｅｒ－ｅＮＢ）キャリアアグリゲーションによる無線アクセスを保護するセカンダリ無線基地局（ＳｅＮＢ）の使用方法であって、さらに、
前記ベアラが前記ＳｅＮＢにより管理されているいずれかのセルにおいて通信に使われていないかどうかを判定し、
前記ベアラのための導出鍵を削除する、使用方法。
【請求項１０】
請求項８記載の、無線基地局間（ｉｎｔｅｒ－ｅＮＢ）キャリアアグリゲーションによる無線アクセスを保護するセカンダリ無線基地局（ＳｅＮＢ）の使用方法であって、前記ＳＣｅｌｌは前記ＰｅＮＢ又は前記ＳｅＮＢのいずれかによって選択される、使用方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、２０１３年１月９日出願の米国仮出願第６１７５０７３２号の優先権を主張し、その内容を参照によりここに組み込むものとする。
【０００２】
本開示の一つ又は複数の実施形態は、３ＧＰＰのＬＴＥ（Ｌｏｎｇ　Ｔｅｒｍ　Ｅｖｏｌｕｔｉｏｎ）のような無線ネットワークシステムにおける無線基地局間（ｉｎｔｅｒ－ｅＮＢ）キャリアアグリゲーションによる保護された無線アクセスに関するものである。一つ又は複数の実施形態における設計では、ある無線基地局（ｅＮＢ）との通信にユーザー端末（ＵＥ）の一組のベアラが用いられるのに対し、そのＵＥの他の一組のベアラが他のｅＮＢとの通信に用いられる。特に、本開示の一つ又は複数の実施形態では、無線基地局間（ｉｎｔｅｒ－ｅＮＢ）キャリアアグリゲーションによる無線ネットワークの安全性を改善するために用いられる。
【背景技術】
【０００３】
ＬＴＥ又はＬＴＥアドバンスネットワークにおいて、安全性に関する基本構成はユーザ

端末（ＵＥ）が一つの無線基地局（ｅＮＢ）と接続しているという仮定をよりどころとする。とりわけ、コアネットワーク、ｅＮＢ及びＵＥの安全性に関する手順及びアーキテクチャはすべて、ＵＥが一つのｅＮＢと接続しているという仮定をよりどころとしている。

【０００４】

既存の基本構成では、既存のｅＮＢは、ＵＥが接続しているｅＮＢが変わった場合、ＵＥのK_{eNB}を他のｅＮＢと交換することができる。言い換えると、ｅＮＢ間でハンドオーバが起きると、既存のｅＮＢは新しいｅＮＢとK_{eNB}を交換することができる。ＬＴＥ又はＬＴＥアドバンスネットワークにおいて、K_{eNB}はあるＵＥとｅＮＢのペア特有の基本鍵であり、無線インターフェイスを介するＵＥとｅＮＢとの間の通信の暗号化又は安全性保証のための一組の鍵を導出するのに用いられる。このK_{eNB}から導出された一組の鍵は、K_{RRCenc}、K_{RRCint}、及びK_{upenc}を含んでもよい。

【０００５】

上述したようにＬＴＥ又はＬＴＥアドバンスネットワークにおいては、ＵＥ－ｅＮＢペアに特有の基本鍵であるK_{eNB}が定義され、それは他の鍵を導出するのに用いられる。ＵＥが接続しているｅＮＢが変わった場合には、新しいｅＮＢとＵＥのペアのための基本鍵が作られる。この新しい鍵は、以前のｅＮＢか又はコアネットワークにおけるモビリティ・マネジメント・エンティティ（ＭＭＥ）により作ることができる。次に、一組の新しい導出鍵（ｄｅｒｉｖｅｄ　ｋｅｙｓ）が、新しい基本鍵を用いて再び導出される。しかしながら、いずれにしても、基本鍵は同時には一つしか存在し得ず、導出された一組の鍵も同時には一つしか存在しえない。

【０００６】

ＬＴＥアドバンスにおいて、キャリアアグリゲーションがネットワーク容量をさらに強化し、ピークスループットを増加させるために導入された。ＬＴＥアドバンスにおけるキャリアアグリゲーションでは、キャリアは一つのｅＮＢにより管理されていることを要求されている。言い換えると、無線基地局内（ｉｎｔｒａ－ｅＮＢ）キャリアアグリゲーションである。例えば、図１には、コアネットワーク１０１、ｅＮＢ１０２及びＵＥ１０５における無線基地局内（ｉｎｔｒａ－ｅＮＢ）キャリアアグリゲーションが描かれている。図１には、キャリア周波数Ｆ１のセル１（１０３）とキャリア周波数Ｆ２のセル２（１０４）が描かれている。ここでは、Ｆ１とＦ２は異なる周波数であるが、共にｅＮＢ１０２により管理されている。もしＵＥ１５がセル１０３とセル１０４の両方の範囲内に在圏し、Ｆ１とＦ２の両方の周波数のキャリアアグリゲーションをサポートする場合には、この二つのキャリアは統合され、ＵＥ１０５はセル１０３とセル１０４の両方に接続することができる。このように、キャリア周波数Ｆ１とＦ２は異なるので、インターフェイスを導入せずに、セル１０３とセル１０４の二つのセルを介して同時に伝送することが可能となる。このように統合されたキャリアはコンポーネントキャリア（ＣＣ）呼ばれる。

【０００７】

無線基地局内（ｉｎｔｒａ－ｅＮＢ）キャリアアグリゲーションにおいては、一以上のＣＣを統合することは、単なる伝送リソースの追加と考えることができる。どのキャリアで下りリンクにおけるデータ無線ベアラ（Ｄａｔａ　Ｒａｄｉｏ　ｂｅａｒｅｒ（ＤＲＢ））のトランスポートブロック（ｔｒａｎｓｐｏｒｔ　ｂｌｏｃｋ（ＴＢ））を送るかは、基本的にｅＮＢにおけるスケジューリングで決定される。ＴＢがあるＣＣにマッピングされた後は、引き続き、そのＴＢに対して、ＨＡＲＱ、符号化、レートマッチング、変調及びリソースマッピング等の物理層における処理がそのＣＣ上でなされる。下りリンクにおいては、ＵＥが同時に（つまり一つのサブフレーム内で）複数のＣＣにおける上りリンク許可（ｕｐｌｉｎｋ　ｇｒａｎｔｓ）を受信した場合、ＵＥはＲＢのＴＢをどのＣＣに対しても自由にマッピングすることが許される。ＴＢがＣＣにマッピングされた後は、引き続きそのＴＢに対する物理層の処理がＣＣごとになされる。

【０００８】

Ｉｎｔｒａ－ｅＮＢ　ＣＡは安全性に関する基本構成には影響を与えない。ＣＡしない場合は、一つのｅＮＢだけがＵＥに接続する。基本鍵であるK_{eNB}はＵＥとそれに接続

するｅＮＢとの特定のペアで適切に定義される。ＣＡがない場合であっても、ＵＥとｅＮＢとの間の制御プレーンでの通信はK_{RRCenc}で暗号化され、K_{RRCint}で安全性保証され、ユーザプレーンでの通信はK_{UPENC}で暗号化される。これらはすべて基本鍵K_{eNB}から導出される。

【発明の概要】

【発明が解決しようとする課題】

【０００９】

ＬＴＥとＬＴＥアドバンスが成長し拡張し続けると、無線基地局間（Ｉｎｔｅｒ－ｅＮＢ）キャリアアグリゲーションの開発の必要性が増す。しかしながら、現状の安全性体系は無線基地局間キャリアアグリゲーションシステム向けの鍵生成をサポートできていない。

【課題を解決するための手段】

【００１０】

一つ又は複数の実施形態において、本発明は、無線基地局間（Ｉｎｔｅｒ－ｅＮＢ）キャリアアグリゲーションによる無線アクセスを保護するシステムに関する。そのシステムは、基本鍵を生成して、対応する一組の無線ベアラでの通信の保護に用いられる一組の導出鍵を導出することによりユーザ装置（ＵＥ）との通信を保護するプライマリ無線基地局（ＰｅＮＢ）と、受信した一組の導出鍵の少なくとも一つであって、自らが使っている一組の無線ベアラの内の一つの無線ベアラに対応する導出鍵を用いて、そのＵＥとの通信を保護するセカンダリ無線基地局（ＳｅＮＢ）とを有する。

【００１１】

一つ又は複数の実施形態において、本発明は、無線基地局間（Ｉｎｔｅｒ－ｅＮＢ）キャリアアグリゲーションによる保護された無線アクセス方法に関し、その方法は、ユーザ装置（ＵＥ）と通信するプライマリ無線基地局（ＰｅＮＢ）を選択し、ＰｅＮＢにおいて基本鍵を生成して、その基本鍵から、それぞれが一組の無線ベアラの内の一つに対応する一組の導出鍵を導出し、前記ＵＥと通信するセカンダリ無線基地局（ＳｅＮＢ）を選択し、ＳｅＮＢが使用する無線ベアラに対応する導出鍵であって、前記一組の導出鍵の内の少なくとも一つをＳｅＮＢがＰｅＮＢから受信すること、を含む。

【００１２】

一つ又は複数の実施形態において、本発明は、無線基地局間（Ｉｎｔｅｒ－ｅＮＢ）キャリアアグリゲーションによる無線アクセスを保護するプライマリ無線基地局（ＰｅＮＢ）の使用方法に関し、その方法は、ＰｅＮＢにより管理されているセルの中からユーザ装置（ＵＥ）のためのプライマリセル（ＰＣｅｌｌ）を決定し、そのＰＣｅｌｌの物理セルＩＤと下りリンク周波数に基づいて前記ＵＥの基本鍵（K_{eNB}）を取得し、その基本鍵に基づいて前記ＵＥの一組の導出鍵（K_{RRCenc}、K_{RRCint}及びK_{UPenc}）を導出し、セカンダリ無線基地局（ＳｅＮＢ）が管理するセルの中から前記ＵＥのためのセカンダリセル（ＳＣｅｌｌ）を決定し、ここで、ＳＣｅｌｌの下りリンク周波数はＰＣｅｌｌの下りリンク周波数とは異なっており、ベアラがそのＳＣｅｌｌを介して通信するかどうかを判定し、ＰｅＮＢとＳｅＮＢとの間の保護された接続を介して、そのベアラがデータベアラかシグナリングベアラかに応じて、前記一組の導出鍵の少なくとも一つをＳｅＮＢに送信すること、を含む。

【００１３】

一つ又は複数の実施形態において、本発明は、無線基地局間（Ｉｎｔｅｒ－ｅＮＢ）キャリアアグリゲーションによる無線アクセスを保護するセカンダリ無線基地局（ＳｅＮＢ）の使用方法に関し、その方法は、セカンダリセルＳｅＮＢにより管理されているセルの中からユーザ装置（ＵＥ）のためのＳＣｅｌｌを決定し、ここで、ＳＣｅｌｌの下りリンク周波数はＰＣｅｌｌの下りリンク周波数とは異なっており、ベアラがそのＳＣｅｌｌを介して通信するベアラかどうかを判定し、ＰｅＮＢとＳｅＮＢとの間の保護された接続を介して、そのベアラがデータベアラかシグナリングベアラかに応じて、ＳｅＮＢへの一組の導出鍵の少なくとも一つを受信し、前記一組の導出鍵の少なくとも一つにより前記ベア

ラを保護する、ことを含む。
【００１４】
本発明のその他の様相及び利点は、下記の説明及び別紙の請求の範囲により明らかになる。
【図面の簡単な説明】
【００１５】
【図１】無線基地局内（Ｉｎｔｒａ－ｅＮＢ）キャリアアグリゲーションの例を示す図。
【図２】本開示の一つ又は複数の実施形態による無線基地局間（Ｉｎｔｅｒ－ｅＮＢ）キャリアアグリゲーションの例を示す図。
【図３】本開示の一つ又は複数の実施形態によるＰｅＮＢの処理手順の一例を示す図。
【図４】本開示の一つ又は複数の実施形態によるＰｅＮＢのブロック図の一例を示す図。
【図５】本開示の一つ又は複数の実施形態によるＳｅＮＢのブロック図の一例を示す図。
【図６】本開示の一つ又は複数の実施形態によるＳｅＮＢの処理手順の一例を示す図。
【発明を実施するための形態】
【００１６】
本発明をよりよく理解するために、本発明の実施形態において、いくつかの具体的な詳細を説明する。しかしながら、当業者ならこれらの具体的かつ詳細な説明がなくても本発明を実行できるであろう。その他、本発明をあいまいにするのを避けるため、周知の特徴は詳細には説明しないこととする。
【００１７】
本開示の一つ又は複数の実施形態は、概していうと、無線基地局間（Ｉｎｔｅｒ－ｅＮＢ）キャリアアグリゲーションを採用したネットワークにおける保護された無線アクセスのためのシステムに関する。本発明の一つ又は複数の実施形態は、追加の通信リソースの提供に特によく適合する。
【００１８】
図２に、本発明の一実施形態における無線基地局間キャリアアグリゲーションを示す。この例においては、複数の無線基地局（ｅＮＢ）がＵＥ２０９に接続している。第一のセルであるセル１（２１０）はキャリア周波数Ｆ１であり、ｅＮＢ２０２により形成されている。第二のセルであるセル２（２１１）はキャリア周波数Ｆ２であり、異なるｅＮＢ２０３により形成されている。
【００１９】
無線基地局内（Ｉｎｔｒａ－ｅＮＢ）キャリアアグリゲーションと同様に、もしＵＥが両方のセルの通信可能範囲に在圏し、キャリア周波数Ｆ１とＦ２それぞれについてアグリゲーションをサポートしている場合、キャリアは集められ、ＵＥ２０９は二つのセル２１０と２１１に接続される。利点となるのは、周波数が異なるために必要となるインターフェイスを用いずに、周波数Ｆ１とＦ２の両方を使って同時に通信できることである。このように、本実施形態に係る無線基地局間キャリアアグリゲーションは、ＬＴＥアドバンスにおける無線基地局内キャリアアグリゲーションと同様に、追加の通信リソースを提供する。しかしながら無線基地局内キャリアアグリゲーションとは異なり、無線基地局間キャリアアグリゲーションは、ＵＥ２０９とｅＮＢ２０２及びｅＮＢ２０３との間のＵｕインターフェイス２０７及び２０８の安全性に影響を与える。無線基地局内キャリアアグリゲーションには安全性に関する基本構成が存在するが、それは接続するｅＮＢが一つであることが前提なので、直接適用できない。
【００２０】
図２に記載されている本発明の一つ又は複数の実施形態では、それぞれのｅＮＢとＵＥのペアについて基本鍵K_{eNB}を生成することにより、既存の安全性に関する基本構成が拡張されている。それぞれのｅＮＢの基本鍵から、K_{RRCenc}、K_{RRCint}及びK_{UPenc}などからなる一組の鍵が導出される。この実施形態においては、コアネットワークとＵＥの両方は、複数のｅＮＢと接続できることのみならず、複数の基本鍵導出手順に適応するよう変更されている。このようにコアネットワークとＵＥを変更することに

より、それぞれのｅＮＢとＵＥとの間の通信がすべて保護される。

【００２１】

図２に記載されている本発明の他の実施形態では、既存の安全性に関する基本構成が、特定のｅＮＢ－ＵＥペアについてのみ基本鍵を生成することにより、拡張されている。本実施形態では、基本鍵は、無線基地局間（Ｉｎｔｅｒ－ｅＮＢ）キャリアアグリゲーションに関わる全てのｅＮＢの間で共有される。特定のｅＮＢ－ＵＥペアの基本鍵は、Ｘ２インターフェイス２０６を介して、接続している他のｅＮＢに配信される。本実施形態においては、基本鍵を受信したそれぞれのｅＮＢは、その基本鍵からそれぞれ同じ導出鍵のセットを独自に導出する。本発明の実施形態に係るキャリアアグリゲーションに関わる全てのｅＮＢは、セル間ハンドオーバ、無線基地局内（Ｉｎｔｒａ－ｅＮＢ）ハンドオーバ又は無線基地局間（Ｉｎｔｅｒ－ｅＮＢ）ハンドオーバのための新しい基本鍵を導出する場合に、この基本鍵を使うことができる。さらに、ユーザプレーンでのみ接続できるｅＮＢがある可能性があるが、この場合は.K_{UPenc}のみが必要であり、制御プレーンに関わる鍵であるK_{RRCenc}とK_{RRCint}は導出する必要はない。

【００２２】

図２に記載されている本発明の他の実施形態における目的は、コアネットワークとＵＥのシグナリングオーバーヘッドや複雑さを増加させることなしに、ＵＥとｅＮＢの間の無線アクセスを保護することである。さらに本実施形態の他の目的は、基本鍵と導出鍵のｅＮＢへの開示を可能な範囲で制限することである。

【００２３】

本実施形態において、あるＵＥに対して特定のｅＮＢが選択され、プライマリ無線基地局（ＰｅＮＢ）２０２として指定される。そのＰｅＮＢとＵＥのペアについて基本鍵が生成される。ＰｅＮＢはその後、生成された基本鍵を用いてその特定のＵＥと通信するための一組の導出鍵を導出する。次に、いくつかのベアラのパスが、ＰｅＮＢ以外のｅＮＢと送受信するために、切り替えられ又はセットアップされる。これら代替えのｅＮＢがセカンダリ無線基地局（ＳｅＮＢ）２０３である。このように、必要な導出鍵は、ＳｅＮＢからの送信に用いられるベアラを保護するために必要な場合にだけ、それぞれのＳｅＮＢに配信される。

【００２４】

本実施形態はいくつかの利点を導く。まず、特定のＵＥに対する基本鍵が一つのｅＮＢに対してのみ生成されるので、この場合のＰｅＮＢ２０２では、コアネットワークとＵＥのシグナリングオーバーヘッドと複雑さは、キャリアアグリゲーションがない場合や上述の無線基地局内（Ｉｎｔｒａ－ｅＮＢ）キャリアアグリゲーションの場合と同じである。二つ目に、基本鍵はＰｅＮＢのみで保持されるので、基本鍵の不必要な開示を避けられ、安全性を向上することができる。三つ目に、導出鍵の開示も、ベアラパス管理に結び付けられた鍵の配信に限られる。最後に、それぞれのｅＮＢからの通信に用いられるベアラを保護するために必要な鍵は、接続されたすべてのｅＮＢに提供されるので、どの例でもＵＥへの無線インターフェイスは保護される。

【００２５】

図３には、本発明の一つ又は複数の実施形態におけるＰｅＮＢの手順が例示されている。ＰｅＮＢには、接続しているＵＥに対する無線基地局間（Ｉｎｔｅｒ－ｅＮＢ）キャリアアグリゲーションを管理する、キャリアアグリゲーション（ＣＡ）管理ユニットがある。ＣＡ管理ユニットは、ＵＥに対するキャリアアグリゲーションを適切に開始するためのいくつかのステップを実施する。

【００２６】

まずはじめに、ステップＳ３０１において、ＰｅＮＢのＣＡ管理ユニットは、ＰｅＮＢにより管理されているセルの中からＵＥに対するプライマリセル（ＰＣｅｌｌ）を決める。ＰＣｅｌｌを決定するために考慮すべきことは、無線リソースコントロール（ＲＲＣ）ユニットからの指示により無線通信ユニットを介してＵＥにより提供される参照信号受信パワー（ＲＳＲＰ）や参照信号受信品質（ＲＳＲＱ）等の測定結果、又はＰｅＮＢの無線

通信ユニットにより測定された他のチャネル品質指標である。しかし、それに限定されない。さらに、ＣＡ管理ユニットは、それ自身又は他のｅＮＢにより管理されているセルそれぞれの、現在、過去又は予測される負荷についても考慮することができる。他のｅＮＢからの負荷情報は、バックホール通信ユニットとＸ２適用プロトコル（Ｘ２ＡＰ）ユニットによってＸ２インターフェイスを介して通信される。

【００２７】

ＰｅＮＢによるもう一つの考慮すべきことは、当業者が認識するべき他のファクタのみならず、キャリア周波数により定義される各セルの通信可能範囲、伝送パワー及びサイト間距離をも含む。好ましくは、ＰＣｅｌｌは要求されるレベルのサービスの品質（ＱｏＳ）を提供するのに十分な程度の高いチャネル品質を有しており、負荷は、ネットワークの負荷バランスを助けるのに十分なくらい軽く、通信可能範囲は、ハンドオーバの数が制限されるか又は十分に抑制されるように、ＵＥから見て十分大きいと良い。ハンドオーバの数は、ハンドオーバにより誘発されるコアネットワークシグナリングの要求される生成を考慮すれば、抑制されるのが好ましい。

【００２８】

ＵＥがｅＮＢ間ハンドオーバをする状況において、ＰＣｅｌｌ選択が現在のＰｅＮＢとは異なるｅＮＢによりなされる場合がある。例えば、元の又は以前のｅＮＢ又はＰｅＮＢが、バックホール通信ユニットとＸ２ＡＰによるＸ２インターフェイスを介してＰｅＮＢへ送られたＨＡＮＤＯＶＥＲ　ＲＥＱＵＥＳＴメッセージで伝達されたハンドオーバを実施できる場合がある。この場合、現在のＰｅＮＢのＣＡ管理ユニットは、元のｅＮＢにより選択されたものをＰＣｅｌｌとして単に採用する。さらに、必要であれば、現在のＰｅＮＢはｅＮＢ内ハンドオーバを実施することにより、後にＰＣｅｌｌを変更できる。

【００２９】

次に、ステップＳ３０２において、ＰｅＮＢのK_{eNB}管理ユニットは、ＰＣｅｌｌの物理セルＩＤと下りリンク周波数を基に導き出される基本鍵、つまりK_{eNB}を得る。例えば、一つ又は複数の実施形態において、K_{eNB}は次の式により生成することができる。

【００３０】

$$K_{eNB}=HMAC-SHA(Key, S)$$

【００３１】

上式において、Ｋｅｙは２５６ビットのネクストホップ（ＮＨ）パラメータ又は現在のK_{eNB}である。Ｓは次の式を基に導き出される。

【００３２】

Ｓ＝ＦＣ｜｜Ｐ０｜｜Ｌ０｜｜Ｐ１｜｜Ｌ１

【００３３】

Ｓを導き出すのに用いられる変数は以下の通りです。

【００３４】

ＦＣ＝０ｘ１３

【００３５】

Ｐ０＝目標物理セルＩＤ又はＰＣＩ

【００３６】

Ｌ０＝ＰＣＩの長さ（すなわち、０ｘ００、０ｘ０２など）

【００３７】

Ｐ１＝目標物理セル下りリンク周波数又はＥＡＲＦＣＮ－ＤＬ

【００３８】

Ｌ１＝ＥＡＲＦＣＮ－ＤＬの長さ（すなわち、０ｘ００、０ｘ０２）

【００３９】

Ｓを導く上記の式において、「｜｜」は連結演算子を示す。さらに、ＨＭＡＣ－ＳＨＡは、ＩＥＴＦ　ＲＦＣ　２１０４（１９９７）：“ＨＭＡＣ：Ｋｅｙｅｄ－Ｈａｓｈｉｎｇ　ｆｏｒ　Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ”と、ＩＳＯ／ＩＥＣ　１

０１１８－３：２００４：“Ｉｎｆｏｒｍａｔｉｏｎ Ｔｅｃｈｎｏｌｏｇｙ－Ｓｅｃｕｒｉｔｙ Ｔｅｃｈｎｉｑｕｅｓ－Ｈａｓｈ－Ｆｕｎｃｔｉｏｎｓ－Ｐａｒｔ ３：Ｄｅｄｉｃａｔｅｄ Ｈａｓｈ－Ｆｕｎｃｔｉｏｎｓ．”で明記された関数である。上記に従って導き出されたＫ$_{ｅＮＢ}$は、その後、メモリユニットで記憶される。

【００４０】

ＵＥのｅＮＢ間ハンドオーバの一つ又は複数の実施形態において、Ｋ$_{ｅＮＢ}$の導出は、現在のＰｅＮＢではなく他のｅＮＢでなされてもよい。例えば、Ｋ$_{ｅＮＢ}$の導出は元の又は以前のｅＮＢ又はＰｅＮＢにより実施されてもよく、その後、バックホール通信ユニットとＸ２ＡＰによるＸ２インターフェイスを介するＰｅＮＢへのＨＡＮＤＯＶＥＲ ＲＥＱＵＥＳＴメッセージで通信される実施形態もあり得る。この場合、現在のＰｅＮＢのＫ$_{ｅＮＢ}$管理ユニットは、元のｅＮＢにより導出されたものをＫ$_{ｅＮＢ}$として採用する。

【００４１】

ハンドオーバが終わると、現在のＰｅＮＢは、Ｓ１アプリケーションプロトコル（Ｓ１ＡＰ）ユニットと、バックホール通信ユニットにより、Ｓ１ ＰＡＴＨ ＳＷＩＴＣＨ ＲＥＱＵＥＳＴメッセージをＭＭＥに送る。Ｓ１ ＰＡＴＨ ＳＷＩＴＣＨ ＲＥＱＵＥＳＴメッセージを受信すると、ＭＭＥは新たに計算されたＮＨをＳ１ ＰＡＴＨ ＳＷＩＴＣＨ ＡＣＫＮＯＷＬＥＤＧＥメッセージでＰｅＮＢへ送る。その後、ＰｅＮＢはそのＮＨをメモリユニットに記憶し、他に既存の不使用ＮＨがメモリに記憶されている場合はそれを消去する。必要な場合は、ＰｅＮＢはその後セル間ハンドオーバをすることによりＫ$_{ｅＮＢ}$を変更する。一例としては、ＰｅＮＢは、新しいＮＨがＳ１ ＰＡＴＨ ＳＷＩＴＣＨ ＡＣＫＮＯＷＬＥＤＧＥメッセージで届いたら、すぐにセル間ハンドオーバを開始して新しいＮＨを使用状態にすることができる。

【００４２】

ステップＳ３０３において、ＰｅＮＢのＫ$_{ｅＮＢ}$管理ユニットはＫ$_{ｅＮＢ}$を基にＵＥのＫ$_{ＲＲＣｅｎｃ}$、Ｋ$_{ＲＲＣｉｎｔ}$及びＫ$_{ＵＰｅｎｃ}$を導出する。例えば、鍵は下記の式に従って導出できる。

【００４３】

Ｄｅｒｉｖｅｄ Ｋｅｙ＝ＨＭＡＣ－ＳＨＡ（Ｋｅｙ,Ｓ）

【００４４】

上式において、Ｋｅｙは２５６ビットのＫｅＮＢである。Ｓは下記の式を基に導出される。

【００４５】

Ｓ＝ＦＣ｜｜Ｐ０｜｜Ｌ０｜｜Ｐ１｜｜Ｌ１

【００４６】

Ｓを導出するのに用いた変数は下記のとおりです。

【００４７】

ＦＣ＝０ｘ１５

【００４８】

Ｐ０＝アルゴリズムタイプ識別子

【００４９】

Ｌ０＝ＰＣＩ アルゴリズムタイプ識別子の長さ（すなわち、０ｘ００、０ｘ０１）

【００５０】

Ｐ１＝アルゴリズムアイデンティティ

【００５１】

Ｌ１＝アルゴリズムアイデンティティの長さ（すなわち、０ｘ００、０ｘ０１）

【００５２】

アルゴリズムタイプ識別子を下記の表に示す。

アルゴリズム識別子	値
RRC－enc－alg（for K_{RRCenc}）	0x03
RRC－int－alg（for K_{RRCint}）	0x04
UP－enc－alg（for K_{UPenc}）	0x05

【００５３】
アルゴリズムアイデンティティは４ビットの識別子で、「００００」はヌル、暗号化、又はインテグリティ保護のアルゴリズムを示し、「０００１」はＳＮＯＷ ３Ｇベースのアルゴリズムであって、３ＧＰＰ ＴＳ ３５．２１５：“Ｃｏｎｆｉｄｅｎｔｉａｌｉｔｙ ａｎｄ Ｉｎｔｅｇｒｉｔｙ Ａｌｇｏｒｉｔｈｍｓ ＵＥＡ２ &ＵＩＡ２；Ｄｏｃｕｍｅｎｔ １：ＵＥＡ２ ａｎｄ ＵＩＡ２ ｓｐｅｃｉｆｉｃａｔｉｏｎｓ”に示されているＵＥＡ２と同じアルゴリズムを示し、「００１０」は、ＡＥＳベースのアルゴリズムを示す（これは、ＡＥＳ ｏｆ ＮＩＳＴ：“Ａｄｖａｎｃｅｄ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ （ＡＥＳ） （ＦＩＰＳ ＰＵＢ １９７）” ｉｎ ＣＴＲ ｍｏｄｅ ｏｆ ＮＩＳＴ Ｓｐｅｃｉａｌ Ｐｕｂｌｉｃａｔｉｏｎ ８００－３８Ａ （２００１）：“Ｒｅｃｏｍｍｅｎｄａｔｉｏｎ ｆｏｒ Ｂｌｏｃｋ Ｃｉｐｈｅｒ Ｍｏｄｅｓ ｏｆ Ｏｐｅｒａｔｉｏｎ”をベースにしたものである）。導出されると、鍵はメモリユニットで記憶される。利点となるのは、ＨＭＡＣ－ＳＨＡのおかけで、K_{RRCenc}、K_{RRCint}又はK_{UPenc}からK_{eNB}を予測することが計算上不可能になることである。
【００５４】
ステップＳ３０４において、ＰｅＮＢとＳｅＮＢのＣＡ管理ユニットは、ＳｅＮＢにより管理されているセルの中からＵＥに対するＳＣｅｌｌを決定する。ＳＣｅｌｌの下りリンク周波数は、ＰＣｅｌｌの下りリンク周波数とは異なる。ＳＣｅｌｌを決定するに当たっては、ＰｅＮＢのＲＲＣユニットからの指示に従ってＰｅＮＢの無線通信ユニットを介してＵＥにより供給されるＲＳＲＰやＲＳＲＱのような測定結果や、ＳｅＮＢの無線通信ユニットにより測定されたその他のチャネル品質指標が、その他当業者なら認識するであろう他のファクタと同様に考慮される。ただし、これらに限定されるわけではない。さらにＰｅＮＢとＳｅＮＢのＣＡ管理ユニットは、ＳｅＮＢ又は他のｅＮＢにより管理されているセルそれぞれの現在、過去及び予想される負荷を考慮してもよい。
【００５５】
ＳＣｅｌｌ選びの最終決定は、ＰｅＮＢ又はＳｅＮＢのいずれのＣＡ管理ユニットでなされてもよい。ＳＣｅｌｌ選択しない方のｅＮＢのＣＡ管理ユニットの役目は、ＳＣｅｌｌ選択をするｅＮＢに対して、測定結果、負荷情報及び通信可能範囲を任意に供給することと、ｅＮＢにより選択されたＳＣｅｌｌを採用することに限られる。選択されたＳＣｅｌｌは、その後、ＰｅＮＢとＳｅＮＢとの間で、それぞれのｅＮＢのバックホール通信ユニットとＸ２ＡＰユニットを介して伝えられる。
【００５６】
ステップ３０５において、ＰｅＮＢとＳｅＮＢのベアラパス管理ユニットは、ＳＣｅｌｌ上で通信されるベアラを決定する。ベアラ決定に際しては、ベアラのＱｏＳ要求条件とトラヒック特性及び、ＰＣｅｌｌとＳＣｅｌｌの負荷と通信可能範囲を考慮する。しかしこれらに限定されるわけではない。
【００５７】
ＳＣｅｌｌ選択と同様に、一つ又は複数の実施形態において、ＰｅＮＢまたはＳｅＮＢのいずれのベアラパス管理ユニットがベアラ選択してもよい。この場合、他方のｅＮＢのベアラパス管理ユニットの役目は、ベアラのＱｏＳ要求条件とトラヒック特性に関する情報を任意に供給することに限られる。さらに、他方のｅＮＢのベアラパス管理ユニットは

、ベアラ選択をしたｅＮＢにより選択されたベアラを採用した結果としての負荷と通信可能範囲を供給することもできる。

【００５８】

ベアラはデータベアラ又はシグナリングベアラのいずれかである。ベアラがデータベアラの場合、リアルタイムデータベアラと非リアルタイムデータベアラにさらに区別されてもよい。

【００５９】

当業者であれば、ベアラのパスを最適化する方法が多数あることを認識できるであろう。一つ又は複数の実施形態では、シグナリングベアラを通信可能範囲が大きなセルで用いることが制御信号を信頼性あるものにする上で利点となる。その他の一つ又は複数の実施形態として、例えばビデオのダウンロードの場合においては、データベアラを高スループットのセルで用いることが利点となる。その他の一つ又は複数の実施形態として、例えば音声通信の場合においては、データベアラを通信可能範囲が広く保証されたＱｏＳを有するセルで用いることが利点となる。当業者であれば、本発明が特定のパス最適化に限らず広く適用できることを認識できるであろう。

【００６０】

ステップＳ３０５で決められたベアラはＰｅＮＢとＳｅＮＢそれぞれのバックホール通信ユニットとＸ２ＡＰユニットを介して、ＰｅＮＢとＳｅＮＢとの間で交換される。ＰｅＮＢとＳｅＮＢは、ＳｅＮＢにより伝送される、タイプ、制御プレーン又はユーザープレーンをメモリユニットで記憶できる。

【００６１】

ステップＳ３０６において、ＰｅＮＢの導出鍵配信ユニットは、ベアラがデータベアラかシグナリングベアラかによって、K_{UPenc}又は、K_{RRCenc}及びK_{RRCint}をＳｅＮＢへ送る。ベアラがデータベアラの場合、K_{UPenc}が送られる。ベアラがシグナリングベアラの場合、K_{RRCenc}及びK_{RRCint}が送られる。ＰｅＮＢの導出鍵配信ユニットにより送られた導出鍵は、Ｘ２ＡＰユニットを使ったＸ２インターフェイスと各ｅＮＢのバックホール通信ユニットを介して、ＳｅＮＢの導出鍵配信ユニットにより受信される。

【００６２】

一つ又は複数の実施形態において、ＰｅＮＢとＳｅＮＢとの間の通信チャネルは、物理的に保護された接続を用いて保護されている。一つ又は複数の他の実施形態においては、ＰｅＮＢとＳｅＮＢとの間の通信チャネルは、３ＧＰＰ ＴＳ ３３．２１０：“３ｒｄ Ｇｅｎｅｒａｔｉｏｎ Ｐａｒｔｎｅｒｓｈｉｐ Ｐｒｏｊｅｃｔ；Ｔｅｃｈｎｉｃａｌ Ｓｐｅｃｉｆｉｃａｔｉｏｎ Ｇｒｏｕｐ Ｓｅｒｖｉｃｅｓ ａｎｄ Ｓｙｓｔｅｍ Ａｓｐｅｃｔｓ；Ｎｅｔｗｏｒｋ Ｄｏｍａｉｎ Ｓｅｃｕｒｉｔｙ； ＩＰ ｎｅｔｗｏｒｋ ｌａｙｅｒ ｓｅｃｕｒｉｔｙ”で特定されているネットワーク・ドメイン・セキュリティ（ＮＤＳ）を使って保護されている。すべての実施形態において、ＳｅＮＢは、ベアラでの通信を保護するために必要な一つ又は複数の鍵を受信する。

【００６３】

導出鍵の配信は、ベアラパス管理と結び付けられている。ＳｅＮＢに接続されているベアラにとって必要な場合にだけＳｅＮＢへ導出鍵を送ることで、導出鍵の不必要な開示を避けていることは、当業者であれば認識できるであろう。さらに、導出鍵だけがＳｅＮＢへ送られるので、K_{UPenc}、K_{RRCenc}又はK_{RRCint}から基本鍵K_{eNB}を予測するのは、計算上実行不可能である。従って、基本鍵の不必要な開示も避けられる。

【００６４】

一つ又は複数の実施形態において、もしベアラに対する一つ又は複数の導出鍵がすでにＳｅＮＢに送られている場合には、ステップＳ３０６は省略することができる。例えば、もしＰｅＮＢのメモリユニットにおいて、ＳｅＮＢにより通信で用いられる他のベアラのタイプがユーザープレーンであることがわかった場合には、K_{UPenc}を再び送る必要

はない。なぜならそれは他のベアラのためにすでにＳｅＮＢに送られているからである。
【００６５】
ステップＳ３０７において、ＰｅＮＢとＳｅＮＢのベアラパス管理ユニットは、ベアラが、ＳｅＮＢにより管理されているセル上で通信に用いられていないかを判定する。この例においては、そのベアラはＰｅＮＢまたは他のＳｅＮＢにより通信に用いられているとする。それからＰｅＮＢ又はＳｅＮＢはメモリユニットを確認して、ＳｅＮＢにより通信に用いられている同じタイプのベアラが他にないかを判定する。もし無ければ、ＳｅＮＢは、ベアラのそのタイプに対する導出鍵はもう不要となる。
【００６６】
ステップ３０８において、ＰｅＮＢのK_{eNB}管理ユニットは、例えばセル内ハンドオーバを実施することにより基本鍵を更新する。この場合、新しいK_{eNB}は、現在のK_{eNB}の導出に用いられたものと同じＳを用い、現在のK_{eNB}かＮＨのいずれかをＫｅｙとして用いて、ＨＭＡＣ－ＳＨＡ（Ｋｅｙ，Ｓ）から導出される。その後、新しい導出鍵は新しいK_{eNB}から得られる。この例の利点としては、現在の導出鍵から新しい基本鍵K_{eNB}を予測することは計算上不可能なことであり、そのことによって、新しい導出鍵を予測することも計算上不可能であることである。
【００６７】
一つ又は複数の実施形態において、基本鍵を更新すること及び、導出鍵を導出し直して配信し直すことは、ＰｅＮＢの処理パワーを消費し、ネットワークオーバーヘッドを招く。一つの可能な解決案としては、ＳｅＮＢが所定のタイプのベアラを有していない場合だけステップＳ３０８を実施することである。例えば、ステップＳ３０７において、ＰｅＮＢとＳｅＮＢのベアラパス管理ユニットは、ベアラがＳｅＮＢにより管理されているどのセルでも通信に用いられていないかどうかを判定する。より詳細に言うと、そのベアラが現在、ＰｅＮＢ又は他のＳｅＮＢによって通信に用いられているかどうかである。その後、ＰｅＮＢ又はＳｅＮＢはメモリユニットを確認してそのＳｅＮＢで通信に用いられているものと同じタイプの他のベアラがあるか否かを判定する。もしそのＳｅＮＢで通信に用いられているベアラがない場合は、ＳｅＮＢはそのタイプのベアラに対する導出鍵は必要ない。
【００６８】
本発明の一つ又は複数の実施形態において、「生成する」という言葉の意味は、「創造する」こと、元のｅＮＢ（例えばｅＮＢ＿１）から「受信する」こと、及び基本鍵を「採用する」ことを含む。
【００６９】
図４は、本開示の一つまたは複数の実施形態におけるＰｅＮＢのブロック図である。本実施形態においてＰｅＮＢ４０１は、無線通信ユニット４０２、ベアラパス管理ユニット４０３、導出鍵配信ユニット４０４、K_{eNB}管理ユニット４０５、ＣＡ管理ユニット４０６、バックホール通信ユニット４０７、メモリユニット４０８、Ｓ１ＡＰユニット４０９、Ｘ２ＡＰユニット４１０及びＲＲＣユニット４１１を含む。
【００７０】
無線通信ユニット４０２は無線ネットワークを介して通信する。例えば、無線通信ユニットは一つ又は複数のＵＥと通信できる。一つ又は複数の実施形態において、無線通信ユニット４０２は、ＲＲＣユニット４１１によって誘発されて、ＵＥから供給されるＲＳＲＰ又はＲＳＲＱ等の測定値を収集しても良い。当業者であれば、無線通信ユニット４０２がＵＥ、ＰｅＮＢ又はＳｅＮＢによって測定された他のチャネル品質指標を収集できることを、認識できるであろう。
【００７１】
ベアラパス管理ユニット４０３は、それぞれのセル内で通信に用いられるベアラを決定する。ベアラパス管理ユニット４０３は適切なベアラを選択する上で、ＱｏＲ要求値やベアラのトラヒック特性を含む（しかし、これらに限定されない）いくつかの変数を考慮する。さらに、ベアラパス管理ユニットはそれぞれのセルの負荷と通信可能範囲を考慮して

もよい。ベアラパス管理ユニット４０３は、基準が合わない場合には、あるベアラを特定のセルにおいて通信に用いないと判定してもよい。

【００７２】

導出鍵配信ユニット４０４は導出鍵を配信する。導出鍵配信ユニット４０４は、ベアラがデータベアラか又はシグナリングベアラかを判定する。ベアラがデータベアラの場合、導出鍵配信ユニット４０４はK_{UPenc}鍵のみを送る。ベアラがシグナリングベアラの場合は、導出鍵配信ユニットはK_{RRCenc}鍵とK_{RRCint}鍵を送る。一つ又は複数の実施形態において、導出鍵配信ユニットは、Ｘ２ＡＰユニット４１０を用いることによりＸｓインターフェイスを介して、ｅＮＢから他のｅＮＢへ鍵を送る。一つ又は複数の実施形態において、導出鍵の配信は、ベアラパス管理ユニット４０３によって実施されるベアラパス選択とも関係づけられる。

【００７３】

ＰｅＮＢのK_{eNB}管理ユニット４０５は、ＰＣｅｌｌの物理セルＩＤと下りリンク周波数に基づいて、基本鍵K_{eNB}を導出する。一つ又は複数の実施形態において、図３のステップ３０２でさらに述べられているように、K_{eNB}管理ユニット４０５は下記の式に基づいてK_{eNB}を導出する。

【００７４】

ＫｅＮＢ＝ＨＭＡＣ－ＳＨＡ（Ｋｅｙ，Ｓ）

【００７５】

一つ又は複数の実施形態では、K_{eNB}管理ユニット４０５は、例えばｅＮＢ間ハンドオーバの場合には、他のｅＮＢのK_{eNB}を単に採用することができる。この場合には、新しいＰｅＮＢのK_{eNB}管理ユニット４０５が、前のＰｅＮＢにより導出されたK_{eNB}を、バックホール通信ユニット４０７を介してＸ２インターフェイスにより得て、採用する。

【００７６】

ＣＡ管理ユニット４０６は、ｅＮＢのためのセルを選択する。ＣＡ管理ユニット４０６は、セル選択において、ＲＳＲＰやＲＳＲＱを含む（しかし、これらに限定されない）いくつかのファクタを考慮する。当業者であれば、ＣＡ管理ユニット４０６が他のタイプのチャネル品質指標も考慮できることを認識できるであろう。

【００７７】

概して、ＰｅＮＢのＣＡ管理ユニット４０６は、ＰｅＮＢにより管理されているセルの中からＵＥに対するＰＣｅｌｌを決定する。一つ又は複数の実施形態において、複数のｅＮＢのＣＡ管理ユニット４０６がセルの選択に協力することもできる。ひとつの実施形態においては、ＰｅＮＢとＳｅＮＢのＣＡ管理ユニット４０６が共にＳＣｅｌｌを選択することができる。この場合、ＰｅＮＢ又はＳｅＮＢのいずれのＣＡ管理ユニット４０６がセルの最終選択をしてもよい。この場合の選択をしないＣＡ管理ユニット４０６の役目は、例えば負荷情報や通信可能範囲の情報などの測定結果を、ＳＣｅｌｌ選択の役目を担ったｅＮＢに対して送ることに限られる。

【００７８】

バックホール通信ユニット４０７は、他のｅＮＢや基地局と通信する。一つ又は複数の実施形態では、バックホール通信ユニット４０７は、例えば、有線インターフェイスを介して通信する。バックホール通信ユニット４０７は、例えば、セル選択、ベアラ又は鍵の伝達に用いられる。

【００７９】

メモリユニット４０８はｅＮＢにとって重要な情報を記憶する。メモリユニット４０８に記憶される情報は、基本鍵K_{eNB}、導出鍵K_{RRCinc}、K_{RRCenc}、K_{UPenc}又はベアラが含まれる（しかし、これらに限定されない）。当業者であれば、メモリユニット４０８がｅＮＢの動作のために重要な他の値の記憶にも用いられることは、認識できるであろう。

【００８０】

ＳＡＰユニット４０９は、Ｓ１プロトコルを使って、コアネットワークと通信する。一つ又は複数の実施形態では、ＰｅＮＢのＳ１ＡＰユニット４０９は、コアネットワークのＭＭＥと通信する。さらに、一つ又は複数の実施形態において、Ｓ１ＡＰユニット４０９は、バックホール通信ユニット４０７と組み合わされて一緒に動作してもよい。

【００８１】

Ｘ２ＡＰユニット４１０は、Ｘ２インターフェイスを用いて複数のｅＮＢ間の通信を促進する。一つ又は複数の実施形態において、Ｘ２ＡＰユニットは複数のｅＮＢ間における、ＱｏＳ情報、通信可能範囲情報、基本鍵、導出鍵、又はベアラを含む（しかし、これらに限定されない）データの通信に用いられる。当業者であれば、チャネル品質指標や、ｅＮＢの機能にとって重要な他のデータもＸ２ＡＰユニット４１０を使って伝達されることは認識できるであろう。

【００８２】

ＲＲＣユニット４１１は制御シグナリングのためのプロトコルを用いて通信する。そして、一つ又は複数の実施形態において、ＲＲＣユニット４１１は、制御信号の送信、受信及び解釈を担当する。ＲＲＣユニット４１１は、あるｅＮＢによって、他のｅＮＢに例えばＲＳＲＰやＲＳＲＱ等の測定結果や他のチャネル品質指標を収集する機能をするように指示するのに用いられてもよい。

【００８３】

図５は、本開示の一つ又は複数の実施形態におけるＳｅＮＢのブロック図の一例である。本実施形態において、ＳｅＮＢ５０１は無線通信ユニット５０２、ベアラパス管理ユニット５０３、導出鍵管理ユニット５０４、ＣＡ管理ユニット５０５、バックホール通信ユニット５０７、メモリユニット５０８及び、Ｘ２ＡＰユニット５０９を含む。

【００８４】

無線通信ユニット５０２は、無線ネットワークを介して通信する。例えば、無線通信ユニットは一つ又は複数のＵＥと通信できる。一つ又は複数の実施形態において、無線通信ユニット５０２はＵＥから供給されるＲＳＲＰやＲＳＲＱのような測定値を収集できる。当業者であれば、無線通信ユニット５０２が、ＵＥ、ＰｅＮＢ又はＳｅＮＢにより測定されたその他のチャネル品質指標を収集できることは認識できるであろう。

【００８５】

ベアラパス管理ユニット５０３は個々のセル内で通信に用いるベアラを決定する。ベアラパス管理ユニット５０３は適切なベアラを選択する上で、ＱｏＳ要求条件及びベアラのトラヒック特性を含む（しかし、これらに限定されない）いくつかの変数を考慮する。さらに、ベアラパス管理ユニットは各セルの負荷と通信可能範囲を考慮してもよい。ベアラパス管理ユニット５０３は、基準が合わない場合に、あるベアラを特定のセルにおいて通信に用いないことを決定してもよい。

【００８６】

導出鍵管理ユニット５０４はＰｅＮＢから供給される導出鍵を管理する。導出鍵管理ユニット５０４は、ベアラがデータベアラか又はシグナリングベアラかを決定する。ベアラがデータベアラの場合、導出鍵管理ユニット５０４はK_{UPenc}鍵を使う。ベアラがシグナリングベアラの場合、導出鍵管理ユニットはK_{RRCenc}とK_{RRCint}鍵を使う。一つ又は複数の実施形態において、導出鍵管理ユニットは、Ｘ２ＡＰユニット５０９を用いることにより、Ｘ２インターフェイスを介してＰｅＮＢから鍵を受信する。一つ又は複数の実施形態において、導出鍵の配信は、ベアラパス管理ユニット５０３によりなされるベアラパスの選択とも関係づけられる。

【００８７】

ＣＡ管理ユニット５０５はｅＮＢに対するセルを選択する。ＣＡ管理ユニット５０５はセルを選択する上で、ＲＳＲＰやＲＳＲＱを含む（しかし、これらに限定されない）いくつかの要素を考慮する。当業者であれば、ＣＡ管理ユニット５０５が他のチャネル品質指標も考慮することは認識できるであろう。

【００８８】

一般的に、ＳｅＮＢのＣＡ管理ユニット５０５が、ＳｅＮＢにより管理されているセルの中からＵＥに対するＳＣｅｌｌを決定する。一つ又は複数の実施形態において、複数のＣＡ管理ユニット５０５が協力してセル選択することもできる。ある実施形態においては、ＰｅＮＢとＳｅＮＢの両方のＣＡ管理ユニット５０５がＳＣｅｌｌを選択することができる。この場合、最終的なセル選択は、ＰｅＮＢ又はＳｅＮＢのいずれのＣＡ管理ユニット５０５によってなされてもよい。この場合に選択をしないＣＡ管理ユニット５０５の役目は、負荷情報や通信可能範囲情報などの測定結果を、ＳＣｅｌｌ選択をするｅＮＢに供給することに限られる。

【００８９】

バックホール通信ユニット５０７は、他のｅＮＢや基地局と通信する。一つ又は複数の実施形態において、バックホール通信ユニット５０７は、例えば、有線インターフェイスを介して通信してもよい。バックホール通信ユニット５０７は、例えば、セル選択、ベアラ又は鍵の伝送に用いられる。

【００９０】

メモリユニット５０８はｅＮＢにとって重要な情報を記憶する。メモリユニット５０８に記憶される情報は、導出鍵K_{RRCinc}、K_{RRCenc}、K_{UPenc}又はベアラが含まれる（しかし、これらに限定されない）。当業者であれば、メモリユニット５０８がｅＮＢの動作のために重要な他の値を記憶するのにも用いられることは、認識できるであろう。

【００９１】

Ｘ２ＡＰユニット５０９はＸ２インターフェイスを用いて複数のｅＮＢ間の通信を促進する。一つ又は複数の実施形態において、Ｘ２ＡＰユニットは複数のｅＮＢ間における、ＱｏＳ情報、通信可能範囲情報、導出鍵、又はベアラを含む（しかし、これらに限定されない）データの通信に用いられる。当業者であれば、チャネル品質指標や、ｅＮＢの機能にとって重要な他のデータもＸ２ＡＰユニット５０９を使って伝送されることは認識できるであろう。

【００９２】

図６は本発明の一つ又は複数の実施形態におけるＳｅＮＢの手順の一例を示す。ＳｅＮＢは、自身に接続されているＵＥに対する無線基地局間（ｉｎｔｅｒ－ｅＮＢ）キャリアアグリゲーションを管理するキャリアアグリゲーション（ＣＡ）管理ユニットを有する。ＣＡ管理ユニットは、いくつかの工程を実施して、ＵＥに対するキャリアアグリゲーションを適切に促進する。

【００９３】

ステップＳ６０１において、ＰｅＮＢとＳｅＮＢのＣＡ管理ユニットは、ＳｅＮＢにより管理されているセルの中からＵＥに対するＳＣｅｌｌを決定する。ＳＣｅｌｌの下りリンク周波数は、ＰＣｅｌｌの下りリンク周波数とは異なる。ＳＣｅｌｌを決定するに当たっては、ＰｅＮＢのＲＲＣユニットからの指示に従ってＰｅＮＢの無線通信ユニットを介してＵＥにより供給されるＲＳＲＰやＲＳＲＱのような測定結果や、ＳｅＮＢの無線通信ユニットにより測定されたその他のチャネル品質指標が、その他当業者なら認識するであろう他のファクタと同様に考慮される。ただし、これらに限定されるわけではない。さらにＰｅＮＢとＳｅＮＢのＣＡ管理ユニットは、ＳｅＮＢ又は他のｅＮＢにより管理されているセルそれぞれの現在、過去及び予想される負荷をも考慮してもよい。

【００９４】

ＳＣｅｌｌ選択の最終決定はＰｅＮＢ又はＳｅＮＢいずれのＣＡ管理ユニットでなされてもよい。選択しないｅＮＢのＣＡ管理ユニットの役目は、ＳＣｅｌｌ選択をするｅＮＢに対して、測定結果、負荷情報及び通信可能範囲を任意に供給することと、ｅＮＢにより選択されたＳＣｅｌｌを採用することに限られる。選択されたＳＣｅｌｌは、その後、ＰｅＮＢとＳｅＮＢとの間で、それぞれのｅＮＢのバックホール通信ユニットとＸ２ＡＰユニットを介して、通信される。

【００９５】

ステップ６０２において、ＰｅＮＢとＳｅＮＢのベアラパス管理ユニットは、ＳＣｅｌｌ上で通信されるベアラを決定する。ベアラ決定に際しては、ベアラのＱｏＳ要求条件とトラヒック特性及び、ＰＣｅｌｌとＳＣｅｌｌの負荷と通信可能範囲を考慮する。しかしこれらに限定されるわけではない。

【００９６】

ＳＣｅｌｌ選択と同様に、一つ又は複数の実施形態において、ＰｅＮＢまたはＳｅＮＢのいずれのベアラパス管理ユニットがベアラ選択してもよい。この場合、他方のｅＮＢのベアラパス管理ユニットの役目は、ベアラのＱｏＳ要求条件とトラヒック特性に関する情報を任意に供給することに限られる。さらに、他方のｅＮＢのベアラパス管理ユニットは、ベアラ選択をしたｅＮＢにより選択されたベアラを採用した結果の負荷と通信可能範囲を供給することもできる。

【００９７】

ベアラはデータベアラ又はシグナリングベアラのいずれかである。ベアラがデータベアラの場合、リアルタイムデータベアラと非リアルタイムデータベアラにさらに区別されてもよい。

【００９８】

当業者であれば、ベアラのパスを最適化する方法が多数あることを認識できるであろう。一つ又は複数の実施形態では、シグナリングベアラを通信可能範囲が大きなセルで用いることが制御信号を信頼性あるものにする上で利点となる。その他の一つ又は複数の実施形態として、例えばビデオのダウンロードの場合においては、データベアラを高スループットのセルで用いることが利点となる。その他の一つ又は複数の実施形態として、例えば音声通信の場合においては、データベアラを通信可能範囲が広く保証されたＱｏＳを有するセルで用いることが利点となる。当業者であれば、本発明が特定のパス最適化に限らず広く適用できることを認識できるであろう。

【００９９】

ステップＳ６０２で決められたベアラはＰｅＮＢとＳｅＮＢそれぞれのバックホール通信ユニットとＸ２ＡＰユニットを介して、ＰｅＮＢとＳｅＮＢとの間で交換される。ＰｅＮＢとＳｅＮＢは、ＳｅＮＢにより伝送される、タイプ、制御プレーン又はユーザープレーンをメモリユニットで記憶できる。

【０１００】

ステップＳ６０３において、導出鍵管理ユニットは、Ｘ２ＡＰユニットとバックホール通信ユニットを使ってＸ２インターフフェイスに介してＰｅＮＢから導出鍵を受信する。ＰｅＮＢの導出鍵配信ユニットは、ベアラがデータベアラか又はシグナリングベアラかに従って、ＳｅＮＢにK_{UPenc}又はK_{RRCenc}とK_{RRCint}を送信する。ベアラがデータベアラの場合、K_{UPenc}がＳｅＮＢの導出鍵管理ユニットにより受信される。ベアラがシグナリングベアラの場合、K_{RRCenc}とK_{RRCint}がＳｅＮＢの導出鍵管理ユニットにより受信される。ステップＳ６０３において受信されたすべての導出鍵はその後ＳｅＮＢのメモリユニットに記憶される。

【０１０１】

一つ又は複数の実施形態において、ＰｅＮＢとＳｅＮＢとの間の通信チャネルは物理的に保護された接続を使って、保護されている。一つ又は複数の他の実施形態においては、ＰｅＮＢとＳｅＮＢとの間の通信チャネルは、３ＧＰＰ ＴＳ ３３．２１０：“３ｒｄ Ｇｅｎｅｒａｔｉｏｎ Ｐａｒｔｎｅｒｓｈｉｐ Ｐｒｏｊｅｃｔ；Ｔｅｃｈｎｉｃａｌ Ｓｐｅｃｉｆｉｃａｔｉｏｎ Ｇｒｏｕｐ Ｓｅｒｖｉｃｅｓ ａｎｄ Ｓｙｓｔｅｍ Ａｓｐｅｃｔｓ；Ｎｅｔｗｏｒｋ Ｄｏｍａｉｎ Ｓｅｃｕｒｉｔｙ； ＩＰ ｎｅｔｗｏｒｋ ｌａｙｅｒ ｓｅｃｕｒｉｔｙ”で特定されているネットワーク・ドメイン・セキュリティ（ＮＤＳ）を使って保護されている。すべての実施形態において、ＳｅＮＢは、ベアラでの通信を保護するために必要な一つ又は複数の鍵を受信する。

【０１０２】

導出鍵の配信は、ベアラパス管理と結び付けられる。ＳｅＮＢにより接続されているベ

アラにとって必要な場合にだけＳｅＮＢへ導出鍵を送ることで、導出鍵の不必要な開示を避けていることは、当業者であれば認識できるであろう。さらに、導出鍵だけがＳｅＮＢへ送られるので、K_{UPenc}、K_{RRCenc}又はK_{RRCint}から基本鍵K_{eNB}を予測するのは、計算上では実行不可能である。従って、基本鍵の不必要な開示も避けられる。

【０１０３】

一つ又は複数の実施形態において、もしベアラに対する一つ又は複数の導出鍵がすでにＳｅＮＢへ送られている場合には、ステップＳ６０３は省略することができる。例えば、もしＰｅＮＢのメモリユニットにおいて、ＳｅＮＢにより通信に用いられる他のベアラのタイプがユーザープレーンであることがわかった場合には、K_{UPenc}を再び送る必要はない。なぜならそれは他のベアラのためにすでにＳｅＮＢに送られているからである。

【０１０４】

ステップＳ６０４において、ベアラはＳｅＮＢからＵＥへの通信に用いられる。ベアラは、一つ又は複数の導出鍵を使って安全にＳｅＮＢとＵＥとの間の通信を担う。

【０１０５】

ステップＳ６０５において、ＰｅＮＢとＳｅＮＢのベアラパス管理ユニットは、ベアラが、ＳｅＮＢにより管理されているセル上で通信に用いられていないかを判定する。この例においては、ベアラはＰｅＮＢまたは他のＳｅＮＢにより通信に用いられているとする。ＰｅＮＢ又はＳｅＮＢはメモリユニットを確認して、ＳｅＮＢにより通信に用いられている同じタイプのベアラが他にないかを判定する。もし無ければ、ＳｅＮＢは、そのタイプのベアラに対する導出鍵はもう不要となる。

【０１０６】

ステップＳ６０６において、ＰｅＮＢのK_{eNB}管理ユニットによる基本鍵K_{eNB}の更新がされたかどうかが判定される。例えば、ＰｅＮＢはセル内ハンドオーバの際に基本鍵を更新してもよい。ステップＳ６０６において、もし、ＰｅＮＢが基本鍵を更新したとＳｅＮＢが判定した場合、個々の導出鍵はＳｅＮＢのメモリユニットから削除される。

【０１０７】

略語の説明

ＣＡ：キャリアアグリゲーション（Ｃａｒｒｉｅｒ　Ａｇｇｒｅｇａｔｉｏｎ）

ＣＣ：コンポーネントキャリア（Ｃｏｍｐｏｎｅｎｔ　Ｃａｒｒｉｅｒｓ）

ＣＮ：コアネットワーク（Ｃｏｒｅ　Ｎｅｔｗｏｒｋ）

ＤＲＢ：データ無線ベアラ（Ｄａｔａ　Ｒａｄｉｏ　Ｂｅａｒｅｒｓ）

ｅＮＢ：無線基地局（ｅＮｏｄｅＢ）

ＨＡＲＱ：ハイブリッド自動再送要求（Ｈｙｂｒｉｄ　Ａｕｔｏｍａｔｉｃ　Ｒｅｐｅａｔ　Ｒｅｑｕｅｓｔ）

ＬＴＥ：ロングタームエボリューション（Ｌｏｎｇ　Ｔｅｒｍ　Ｅｖｏｌｕｔｉｏｎ）

ＭＭＥ：モビリティマネジメントエンティティ（Ｍｏｂｉｌｅ　Ｍａｎａｇｅｍｅｎｔ　Ｅｎｔｉｔｙ）

ＮＤＳ：ネットワークドメインセキュリティ（Ｎｅｔｗｏｒｋ　Ｄｏｍａｉｎ　Ｓｅｃｕｒｉｔｙ）

ＰＣｅｌｌ：プライマリセル（Ｐｒｉｍａｒｙ　Ｃｅｌｌ）

ＰｅＮＢ：プライマリ無線基地局（Ｐｒｉｍａｒｙ　ｅＮＢ）

ＱｏＳ：クオリティオブサービス（Ｑｕａｌｉｔｙ　ｏｆ　Ｓｅｒｖｉｃｅ）

ＲＢ：リソースブロック（Ｒｅｓｏｕｒｃｅ　Ｂｌｏｃｋ）

ＲＲＣ：無線リソース制御（Ｒａｄｉｏ　Ｒｅｓｏｕｒｃｅ　Ｃｏｎｔｒｏｌ）

ＲＳＲＰ：基準信号受信電力（Ｒｅｆｅｒｅｎｃｅ　Ｓｉｇｎａｌ　Ｒｅｃｅｉｖｅｄ　Ｐｏｗｅｒ）

ＲＳＲＱ：基準信号受信品質（Ｒｅｆｅｒｅｎｃｅ　Ｓｉｇｎａｌ　Ｒｅｃｅｉｖｅｄ　Ｑｕａｌｉｔｙ）

ＳＣｅｌｌ：セカンダリセル（Ｓｅｃｏｎｄａｒｙ　Ｃｅｌｌ）

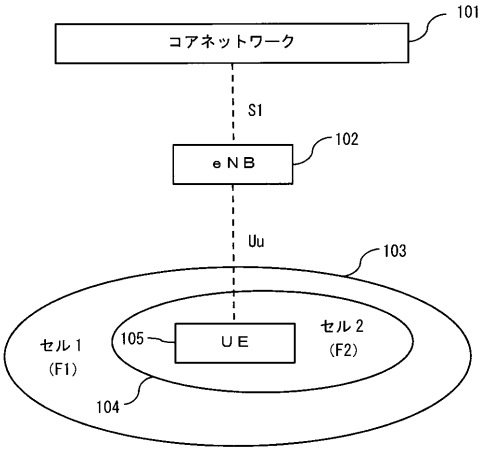
ＳｅＮＢ：セカンダリ無線基地局（Ｓｅｃｏｎｄａｒｙ　ｅＮＢ）
Ｓ１ＡＰ：Ｓ１アプリケーションプロトコル（Ｓ１　Ａｐｐｌｉｃａｔｉｏｎ　Ｐｒｏｔｏｃｏｌ）
ＴＢ：トランスポートブロック（Ｔｒａｎｓｐｏｒｔ　Ｂｌｏｃｋ）
ＵＥ：ユーザ装置（Ｕｓｅｒ　ｅｑｕｉｐｍｅｎｔ）
Ｘ２ＡＰ：Ｘ２アプリケーションプロトコル（Ｘ２　Ａｐｐｌｉｃａｔｉｏｎ　Ｐｒｏｔｏｃｏｌ）

【０１０８】
本発明は、具体的な実施形態を参照することにより上記で述べられている。しかし、当業者であれば、上記実施形態は例示的な目的でのみ述べられていることを理解するであろうし、さまざまな修正、変形、改変、変更などの例を考えつくことができる。本発明の理解を促進するために、全文を通じて具体的な値が例として用いられている。しかし、このような具体的な値は、特段の記載がなければ、ただの例示的な値であって他の値も使用できることに注意しておくべきである。

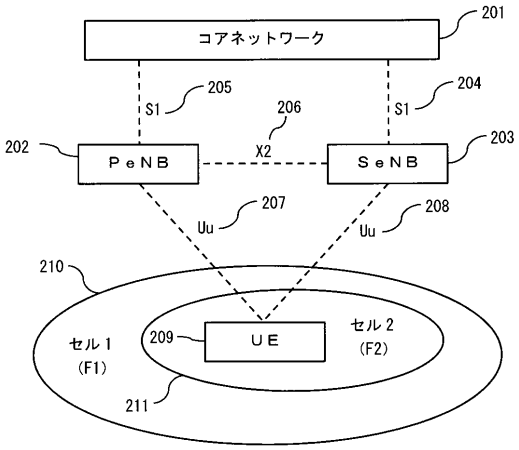
【０１０９】
本発明の実施形態における装置について、例示的な目的で、機能ブロック図を参照して説明した。しかし、この装置はハードウエア、ソフトウエア又はそれらの組み合わせにより供給されてもよい。さらに、一つ又は複数の実施形態において、本発明は、コンピュータで読み出し可能な、非一過性の適切な媒体に記憶されているコンピュータプログラムであってもよい。本発明は、上述の実施形態に限定されず、本発明の範囲及び主旨から逸脱することなく、さまざまな修正、変形、改変、変更などをすることができる。

【０１１０】
本発明を限られた数の実施形態に関連して説明したが、当業者であれば、本明細書で述べられた発明の範囲から逸脱することなく、他の実施形態を考案できることを認識できるであろう。従って発明の範囲は、添付されたクレームによってのみ限定されるべきである。

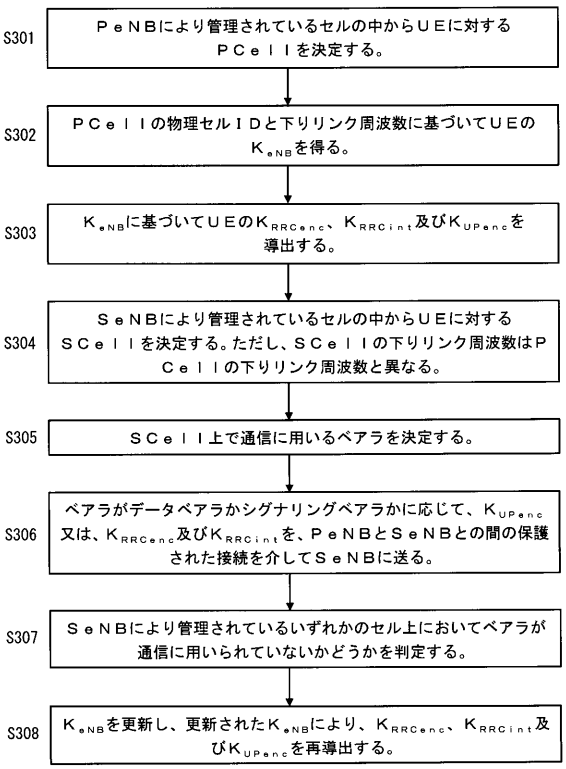
【図１】


101
コアネットワーク
S1
102
eNB
Uu
103
セル１
(F1)
105
UE
セル２
(F2)
104

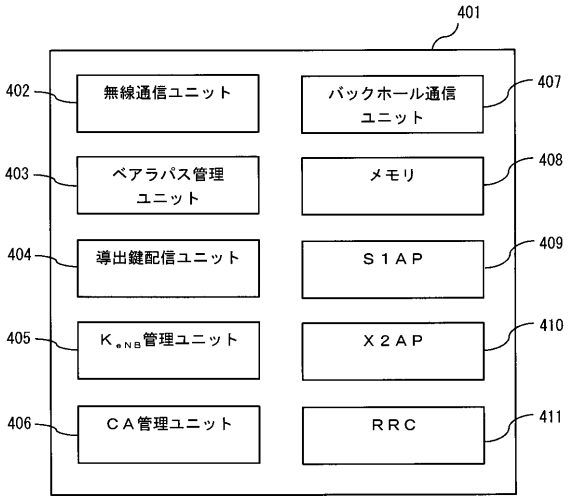
【図２】


201
コアネットワーク
S1
205
206
S1
204
202
PeNB
X2
SeNB
203
Uu
207
Uu
208
210
セル１
(F1)
209
UE
セル２
(F2)
211

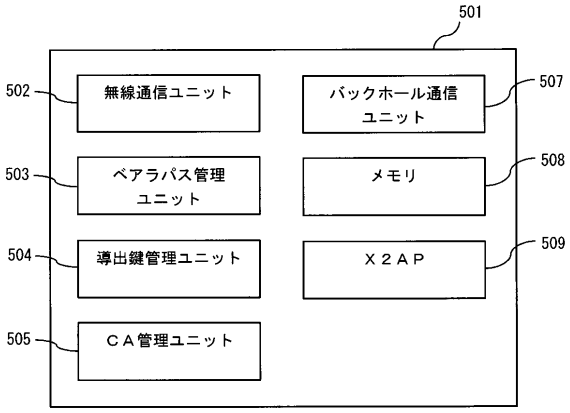
【図３】


S301
PeNBにより管理されているセルの中からUEに対するPCellを決定する。
S302
PCellの物理セルIDと下りリンク周波数に基づいてUEのK_{eNB}を得る。
S303
K_{eNB}に基づいてUEのK_{RRCenc}、K_{RRCint}及びK_{UPenc}を導出する。
S304
SeNBにより管理されているセルの中からUEに対するSCellを決定する。ただし、SCellの下りリンク周波数はPCellの下りリンク周波数と異なる。
S305
SCell上で通信に用いるベアラを決定する。
S306
ベアラがデータベアラかシグナリングベアラかに応じて、K_{UPenc}又は、K_{RRCenc}及びK_{RRCint}を、PeNBとSeNBとの間の保護された接続を介してSeNBに送る。
S307
SeNBにより管理されているいずれかのセル上においてベアラが通信に用いられていないかどうかを判定する。
S308
K_{eNB}を更新し、更新されたK_{eNB}により、K_{RRCenc}、K_{RRCint}及びK_{UPenc}を再導出する。

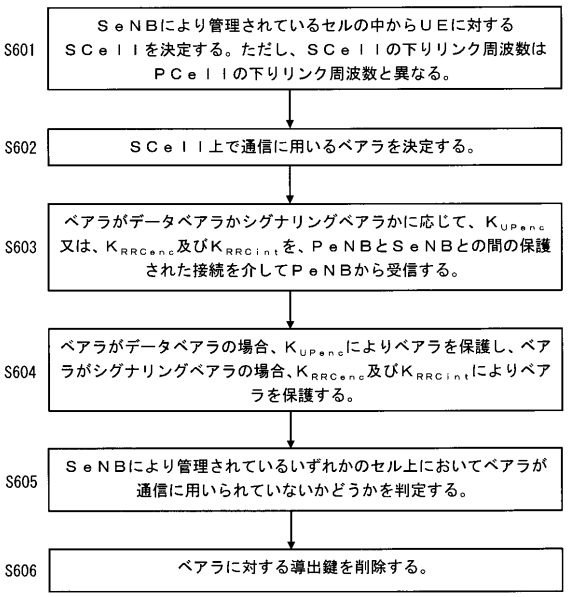
【図４】


401
402
無線通信ユニット
407
バックホール通信ユニット
403
ベアラパス管理ユニット
408
メモリ
404
導出鍵配信ユニット
409
S1AP
405
K_{eNB}管理ユニット
410
X2AP
406
CA管理ユニット
411
RRC

【図５】


501
502
無線通信ユニット
503
ベアラパス管理ユニット
504
導出鍵管理ユニット
505
ＣＡ管理ユニット
507
バックホール通信ユニット
508
メモリ
509
Ｘ２ＡＰ

【図６】


S601
ＳｅＮＢにより管理されているセルの中からＵＥに対するＳＣｅｌｌを決定する。ただし、ＳＣｅｌｌの下りリンク周波数はＰＣｅｌｌの下りリンク周波数と異なる。
S602
ＳＣｅｌｌ上で通信に用いるベアラを決定する。
S603
ベアラがデータベアラかシグナリングベアラかに応じて、K_{UPenc}又は、K_{RRCenc}及びK_{RRCint}を、ＰｅＮＢとＳｅＮＢとの間の保護された接続を介してＰｅＮＢから受信する。
S604
ベアラがデータベアラの場合、K_{UPenc}によりベアラを保護し、ベアラがシグナリングベアラの場合、K_{RRCenc}及びK_{RRCint}によりベアラを保護する。
S605
ＳｅＮＢにより管理されているいずれかのセル上においてベアラが通信に用いられていないかどうかを判定する。
S606
ベアラに対する導出鍵を削除する。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 14/10273

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06F 7/04 (2014.01)
USPC - 726/4
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)
USPC: 726/4

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC: 370/310, 338; 726/1-6, 14 (keyword limited - see terms below)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PatBase; GOOGLE; GoogleScholar; GooglePatents
Search Terms: radio, wireless, mobile, cellular, bearer, aggregate, eNB, PeNB, evolved node, transmit, carrier, inter, secure, downlink, frequency, UE, user equipment, derive, key, manage, cell, ID, identification, primary, secondary

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2010/0329452 A1 (Alanara et al.) 30 December 2010 (30.12.2010), entire document, especially; abstract, para. [0019], [0042], [0045], [0052], [0053]	1 - 10
Y	US 2013/0003975 A1 (Fukuda et al.) 03 January 2013 (03.01.2013), entire document, especially; abstract, para. [0003], [0067]	1 - 5
Y	US 2012/0250520 A1 (Chen et al.) 04 October 2012 (04.10.2012), entire document, especially; abstract, para. [0042], [0050]	6 - 10
A	US 2009/0092107 A1 (Cai et al.) 09 April 2009 (09.04.2009), entire document	1 - 10
A	US 2009/0220079 A1 (Harada et al.) 03 September 2009 (03.09.2009), entire document	1 - 10
A	US 2006/0120530 A1 (Vialen et al.) 08 June 2006 (08.06.2006), entire document	1 - 10

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

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 March 2014 (20.03.2014)	17 APR 2014
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (July 2009)

フロントページの続き

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

(72)発明者 石井 啓之
アメリカ合衆国 ９４３０４ カリフォルニア州 パロ アルト ヒルビュー アベニュー ３２４０

Ｆターム(参考) 5K067 AA33 DD17 EE02 EE10 EE24 HH24