

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2010-124481

(P2010-124481A)

(43) 公開日 平成22年6月3日(2010.6.3)

(51) Int.Cl.		F I				テーマコード (参考)
H04W 12/04	(2009.01)	H04Q 7/00	182			5J104
H04W 36/08	(2009.01)	H04Q 7/00	306			5K067
H04L 9/08	(2006.01)	H04L 9/00	601B			

審査請求 未請求 請求項の数 3 O L (全 15 頁)

(21) 出願番号	特願2010-2185 (P2010-2185)	(71) 出願人	392026693
(22) 出願日	平成22年1月7日 (2010.1.7)		株式会社エヌ・ティ・ティ・ドコモ
(62) 分割の表示	特願2008-169669 (P2008-169669) の分割	(74) 代理人	100083806
原出願日	平成20年6月27日 (2008.6.27)		弁理士 三好 秀和
		(74) 代理人	100100712
			弁理士 岩▲崎▼ 幸邦
		(74) 代理人	100095500
			弁理士 伊藤 正和
		(74) 代理人	100101247
			弁理士 高橋 俊一
		(74) 代理人	100117064
			弁理士 伊藤 市太郎

最終頁に続く

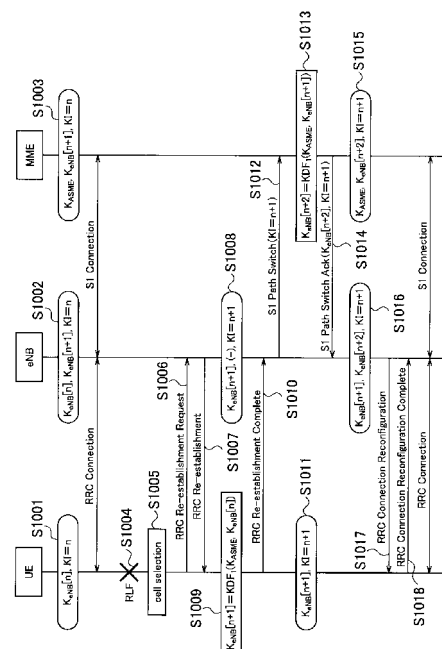
(54) 【発明の名称】 移動通信方法

(57) 【要約】

【課題】簡素化された手順で、再接続先セルを管理する無線基地局eNB、eNB#2で用いられる第1鍵を生成する。

【解決手段】本発明に係る移動通信方法は、所定鍵を用いて移動局UEと無線基地局eNBとの間の通信を行う移動通信方法であって、移動局UEの再接続手順において、移動局UEの再接続先セルを管理する無線基地局は、移動局UEの次の再接続先セルと移動局UEとの間の通信に用いられる予定の所定鍵を生成するための第1鍵 $K_{eNB[n+1]}$ を取得する工程を有する。

【選択図】図3



【特許請求の範囲】

【請求項 1】

所定鍵を用いて移動局と無線基地局との間の通信を行う移動通信方法であって、

移動局の再接続手順において、該移動局の再接続先セルを管理する無線基地局は、該移動局の次の再接続先セルと該移動局との間の通信に用いられる予定の所定鍵を生成するための第 1 鍵を取得する工程を有することを特徴とする移動通信方法。

【請求項 2】

前記移動局の再接続手順において、前記無線基地局は、該移動局の再接続先セルと該移動局との間の通信に用いられる所定鍵を生成するための第 1 鍵を取得する工程を更に有することを特徴とする請求項 1 に記載の移動通信方法。

10

【請求項 3】

前記移動局は、前記無線基地局に対して再接続要求信号を送信した後、該無線基地局から受信した再接続応答信号に応じて、前記第 1 鍵を更新する工程を有することを特徴とする請求項 1 又は 2 に記載の移動通信方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、所定鍵を用いて移動局と無線基地局との間の通信を行う移動通信方法に関する。

【背景技術】

20

【0002】

従来、3GPPで規定されているLTE (Long Term Evolution) 方式の移動通信システムでは、所定鍵を用いて、移動局UEと無線基地局eNBとの間の通信を行うように構成されている。

【0003】

所定鍵としては、例えば、移動局UEと無線基地局eNBとの間 (Access Stratum、AS) のCプレーンプロトコルであるRRCプロトコルにおける「Ciphering」で用いられる鍵 K_{RRC_Ciph} や、同RRCプロトコルにおける「Integrity Protection」で用いられる鍵 K_{RRC_IP} や、移動局UEと無線基地局eNBとの間 (Access Stratum、AS) のUプレーンにおける「Ciphering」で用いられる鍵 K_{UP_Ciph} 等が挙げられる。なお、かかる所定鍵は、第 1 鍵 K_{eNB} を用いて生成される。

30

【0004】

かかる所定鍵や第 1 鍵 K_{eNB} は、長時間同一のものをを用いると、セキュリティ上システムが脆弱となり、好ましくない。そこで、ハンドオーバーを行った際に、かかる所定鍵や第 1 鍵 K_{eNB} を更新する手順が、3GPPにおいて考案されている。

【0005】

ここで、図 8 を参照して、移動局UEの再接続手順において、再接続先セルを管理する無線基地局 (Target eNB) が、所定鍵の生成に用いる第 1 鍵 K_{eNB}^{**} を取得する動作について説明する。

40

【0006】

図 8 に示すように、第 1 に、再接続元セルを管理する無線基地局 (Source eNB) が、記憶している第 1 鍵 K_{eNB} と、パラメータ「Next Hop」と、ハンドオーバーの種類を示すパラメータ「Handover Type」と、ハンドオーバー先セルの識別情報示すパラメータ「Target PCI」とに基づいて、中間鍵 K_{eNB}^* を生成する。

【0007】

第 2 に、再接続元セルを管理する無線基地局 (Source eNB) が、生成した中間鍵 K_{eNB}^* を、再接続先セルを管理する無線基地局 (Target eNB) に送信する。

50

【0008】

第3に、再接続先セルを管理する無線基地局（Target eNB）が、受信した中間鍵 K_{eNB}^* と、再接続先セルによって割り当てられた「C-RNTI（Cell Radio Network Temporary ID）」とに基づいて、再接続先セルを管理する無線基地局（Target eNB）において所定鍵の生成に用いられる第1鍵 K_{eNB}^{**} を生成する。

【先行技術文献】

【非特許文献】

【0009】

【非特許文献1】3GPP TS 33.401 v8.0.0

10

【発明の概要】

【発明が解決しようとする課題】

【0010】

しかしながら、上述のように、従来の移動通信システムの再接続手順では、再接続元セルを管理する無線基地局（Source eNB）及び再接続先セルを管理する無線基地局（Target eNB）の双方で、複数のパラメータや関数を用いて、再接続先セルを管理する無線基地局（Target eNB）で用いられる第1鍵 K_{eNB}^{**} を生成しなければならないという問題点があった。

【0011】

特に、再接続元セルを管理する無線基地局（Source eNB）と再接続先セルを管理する無線基地局（Target eNB）とで、異なるパラメータを用いた K_{eNB} 変換関数（Key Derivation Function、KDF）を用いなければならない、移動局UEにおいても、これらのKDFを装備する必要がある、複雑である問題があった。

20

【0012】

また、再接続先セルのPCI（Physical Cell ID）に応じて、 K_{eNB} を更新する必要がある煩雑性があった。

【0013】

特に、PCI依存とした場合、無線基地局に「UE context」が存在するにも関わらず、移動局UEが、かかる無線基地局配下の異なるセルにて再接続を試みた場合、所定鍵が、移動局UEと無線基地局との間で一致しないために、再接続が、rejectされるケースが発生してしまう。

30

【0014】

更には、C-RNTIに応じて、 K_{eNB} を更新する必要があるため、C-RNTIの変更割当を柔軟に行うことに制約があった。

【0015】

そこで、本発明は、上述の課題に鑑みてなされたものであり、簡素化された手順で、再接続先セルを管理する無線基地局（Target eNB）で用いられる第1鍵を生成することができる移動通信方法を提供することを目的とする。

【課題を解決するための手段】

40

【0016】

本発明の第1の特徴は、所定鍵を用いて移動局と無線基地局との間の通信を行う移動通信方法であって、移動局の再接続手順において、該移動局の再接続先セルを管理する無線基地局は、該移動局の次の再接続先セルと該移動局との間の通信に用いられる予定の所定鍵を生成するための第1鍵を取得する工程を有することを要旨とする。

【0017】

本発明の第1の特徴において、前記移動局の再接続手順において、前記無線基地局は、該移動局の再接続先セルと該移動局との間の通信に用いられる所定鍵を生成するための第1鍵を取得する工程を更に有してもよい。

【0018】

50

本発明の第1の特徴において、前記移動局は、前記無線基地局に対して再接続要求信号を送信した後、該無線基地局から受信した再接続応答信号に応じて、前記第1鍵を更新する工程を有してもよい。

【発明の効果】

【0019】

以上説明したように、本発明によれば、簡素化された手順で、再接続先セルを管理する無線基地局（Target eNB）で用いられる第1鍵を生成することができる移動通信方法を提供することができる。

【図面の簡単な説明】

【0020】

10

【図1】本発明の第1の実施形態に係る移動通信システムの全体構成図である。

【図2】本発明の第1の実施形態に係る移動通信システムで用いられる鍵の階層構造及び算出手順の一例を示す図である。

【図3】本発明の第1の実施形態に係る移動通信システムにおけるIntra-eNB再接続手順を示すシーケンス図である。

【図4】本発明の第1の実施形態に係る移動通信システムにおけるInter-eNB再接続手順を示すシーケンス図である。

【図5】本発明の第2の実施形態に係る移動通信システムで用いられる鍵の階層構造及び算出手順の一例を示す図である。

【図6】本発明の第2の実施形態に係る移動通信システムにおけるIntra-eNB再接続手順を示すシーケンス図である。

20

【図7】本発明の第2の実施形態に係る移動通信システムにおけるInter-eNB再接続手順を示すシーケンス図である。

【図8】従来技術に係る移動通信システムで用いられる鍵の算出手順の一例を示す図である。

【発明を実施するための形態】

【0021】

（本発明の第1の実施形態に係る移動通信システム）

図1乃至図4を参照して、本発明の第1の実施形態に係る移動通信システムについて説明する。

30

【0022】

本実施形態に係る移動通信システムは、LTE方式が適用されている移動通信システムであって、図1に示すように、複数の交換局MME#1、#2…と、複数の無線基地局eNB#11、#12、#21、#22…とを具備している。

【0023】

例えば、移動局UEは、無線基地局eNB#11配下のセル#111において、上述の所定鍵を用いて、無線基地局eNB#11との間で通信を行うように構成されている。

【0024】

また、移動局UEの再接続（Re-establishment）手順において、再接続先セルを管理する無線基地局（例えば、無線基地局eNB#12）は、再接続元セルを管理する無線基地局（例えば、無線基地局eNB#11）によって生成される中間鍵 K_{eNB}^* を用いることなく、移動局UEとの間の通信に用いられる所定鍵を生成するための第1鍵 $K_{eNB}[n+1]$ 、 $K_{eNB}[n+2]$ 等を取得するように構成されている。

40

【0025】

図2に、本実施形態に係る移動通信システムで用いられる鍵（すなわち、所定鍵の算出に用いられる鍵）の階層構造及び算出手順の一例について示す。

【0026】

図2に示すように、RRCプロトコルにおける「Integrity Protection」で用いられる鍵 K_{RRC-IP} 、RRCプロトコルにおける「Ciphering」で用いられる鍵 $K_{RRC-Ciph}$ 及びASのUプレーンにおける「Cipher i

50

ng」で用いられる鍵 K_{UP_Ciph} は、第 1 鍵 $K_{eNB[n]}$ を用いて生成される。

【0027】

また、第 1 鍵 $K_{eNB[n]}$ は、親鍵 K_{ASME} を用いて、下記の式によって算出される。

【0028】

$$K_{eNB[0]} = KDF_0(K_{ASME}, NAS_SN)$$

$$K_{eNB[n+1]} = KDF_1(K_{ASME}, K_{eNB[n]}), (n \geq 0)$$

ここで、親鍵 K_{ASME} は、移動局 UE 及び交換局 MME のみによって知られているものであり、無線基地局 eNB によって知られてはならないものである。

【0029】

また、NAS_SN は、移動局 UE と交換局 MME との間 (Non Access Stratum、NAS) の C プレーンプロトコルである NAS プロトコルのシーケンス番号 (Sequence Number、SN) である。

【0030】

以下、図 3 及び図 4 を参照して、本実施形態に係る移動通信システムの動作について説明する。

【0031】

第 1 に、図 3 を参照して、本実施形態に係る移動通信システムにおける Intra-eNB 再接続手順 (無線基地局内再接続手順) について説明する。

【0032】

図 3 に示すように、Intra-eNB 再接続手順の開始前の段階では、移動局 UE は、 $K_{eNB[n]}$ 、「KI (=n)」を保持しており (ステップ S1001)、無線基地局 eNB は、 $K_{eNB[n]}$ 、 $K_{eNB[n+1]}$ 、「KI (=n)」を保持しており (ステップ S1002)、交換局 MME は、 K_{ASME} 、 $K_{eNB[n+1]}$ 、「KI (=n)」を保持している (ステップ S1003)。

【0033】

ステップ S1004 において、移動局 UE と無線基地局 eNB との間で RRC コネクションが確立されており、無線基地局 eNB と交換局 MME との間で S1 コネクションが確立されている状態で、移動局 UE は、上述の RRC コネクションにおいて、無線リンク障害 (RLF: Radio Link Failure) を検出する。例えば、移動局 UE は、以下の場合に、RLF を検出するものとする。

【0034】

- ・ RRC コネクションにおける RSRP (Reference Signal Received Power) が、所定期間、所定閾値を下回った場合
- ・ ランダムアクセス手順が成功しない場合
- ・ ハンドオーバー手順が失敗した場合

その後、移動局 UE は、ステップ S1005 において、セル選択処理を行い、ステップ S1006 において、選択したセル (或いは、選択したセルを管理する無線基地局 eNB) に対して、共通制御チャネルを介して、「RRC Connection Re-establishment Request (再接続要求信号)」を送信する。

【0035】

無線基地局 eNB は、ステップ S1007 において、移動局 UE に対して、「RRC Connection Re-establishment (再接続応答信号)」を送信する。なお、「RRC Connection Re-establishment」に「KI (=n+1)」が含まれていてもよい。

【0036】

ここで、無線基地局 eNB は、 $K_{eNB[n+1]}$ 、「KI (=n+1)」を保持している状態となる (ステップ S1008)。

【0037】

移動局 UE は、ステップ S1009 において、下記の式によって、 $K_{eNB[n+1]}$

10

20

30

40

50

を算出し、ステップS1010において、かかる $K_{eNB[n+1]}$ を用いて、無線基地局eNBに対して、「RRC Connection Re-establishment Complete（再接続完了信号）」を送信する。

【0038】

$$K_{eNB[n+1]} = KDF_1(K_{ASME}, K_{eNB[n]})$$

ここで、移動局UEは、 $K_{eNB[n+1]}$ 、「KI(=n+1)」を保持している状態となる（ステップS1011）。

【0039】

ステップS1012において、無線基地局eNBは、交換局MMEに対して、「KI(=n+1)」を含む「S1 Path Switch（パススイッチ信号）」を送信する。

10

【0040】

交換局MMEは、ステップS1013において、下記の式によって、 $K_{eNB[n+2]}$ を算出し、ステップS1014において、無線基地局eNBに対して、 $K_{eNB[n+2]}$ 、「KI(=n+1)」を含む「S1 Path Switch Ack（パススイッチ応答信号）」を送信する。

【0041】

$$K_{eNB[n+2]} = KDF_1(K_{ASME}, K_{eNB[n+1]})$$

ここで、交換局MMEは、 K_{ASME} 、 $K_{eNB[n+2]}$ 、「KI(=n+1)」を保持している状態となる（ステップS1015）。

20

【0042】

ステップS1016において、無線基地局eNBは、「S1 Path Switch Ack」を受信して、 $K_{eNB[n+1]}$ 、 $K_{eNB[n+2]}$ 、「KI(=n+1)」を保持している状態となる。

【0043】

すなわち、ここで、再接続先セルを管理する無線基地局eNBは、移動局UEの次の再接続先セルと移動局UEとの間の通信に用いられる予定の所定鍵を生成するための第1鍵 $K_{eNB[n+2]}$ を取得する。

【0044】

ステップS1017において、無線基地局eNBは、移動局UEに対して、「RRC Connection Reconfiguration」を送信し、ステップS1018において、移動局UEは、無線基地局eNBに対して、「RRC Connection Reconfiguration Complete」を送信する。

30

【0045】

以上の手順により、Intra-eNB再接続手順において、 K_{eNB} 及び所定鍵が更新される。

【0046】

図4に示すように、Inter-eNB再接続手順の開始前の段階では、移動局UEは、 $K_{eNB[n]}$ 、「KI(=n)」を保持しており（ステップS2001）、無線基地局eNB#1は、 $K_{eNB[n]}$ 、 $K_{eNB[n+1]}$ 、「KI(=n)」を保持しており（ステップS2002）、交換局MMEは、 K_{ASME} 、 $K_{eNB[n+1]}$ 、「KI(=n)」を保持している（ステップS2003）。

40

【0047】

ステップS2004において、無線基地局eNB#1は、周辺の無線基地局eNB#2に対して、 $K_{eNB[n+1]}$ 、「KI(=n+1)」を含む「X2 HO Preparation（ハンドオーバー準備信号）」を送信する。

【0048】

無線基地局eNB#2は、ステップS2005において、受信した $K_{eNB[n+1]}$ 、「KI(=n+1)」を記憶し、ステップS2006において、無線基地局eNB#1に対して、「X2 HO Preparation Ack（ハンドオーバー準備応答信号）」を送信する。

50

)」を送信する。

【0049】

すなわち、ここで、再接続先セルを管理する無線基地局 eNB # 2 は、移動局 UE との間の通信に用いられる予定の所定鍵を生成するための第 1 鍵 $K_{eNB[n+1]}$ を取得する。

【0050】

ステップ S2007 において、移動局 UE と無線基地局 eNB # 1 との間で RRC コネクションが確立されており、無線基地局 eNB # 1 と交換局 MME との間で S1 コネクションが確立されている状態で、移動局 UE は、上述の RRC コネクションにおいて、RLF を検出する。

10

【0051】

その後、移動局 UE は、ステップ S2008 において、セル選択処理を行い、ステップ S2009 において、選択した再接続先セル（或いは、再接続先無線基地局）eNB # 2 に対して、共通制御チャネルを介して、「RRC Connection Re-establishment Request（再接続要求信号）」を送信する。

【0052】

再接続先無線基地局 eNB # 2 は、ステップ S2010 において、移動局 UE に対して、「RRC Connection Re-establishment（再接続応答信号）」を送信する。なお、「RRC Connection Re-establishment」に「KI (=n+1)」が含まれていてもよい。

20

【0053】

移動局 UE は、ステップ S2011 において、下記の式によって、 $K_{eNB[n+1]}$ を算出し、ステップ S2013 において、かかる $K_{eNB[n+1]}$ を用いて、再接続先無線基地局 eNB # 2 に対して、「RRC Connection Re-establishment Complete（再接続完了信号）」を送信する。

【0054】

$$K_{eNB[n+1]} = KDF_1(K_{ASME}, K_{eNB[n]})$$

ここで、移動局 UE は、 $K_{eNB[n+1]}$ 、「KI (=n+1)」を保持している状態となる（ステップ S2012）。

【0055】

ステップ S2014 において、無線基地局 eNB # 2 は、交換局 MME に対して、「KI (=n+1)」を含む「S1 Path Switch（パススイッチ信号）」を送信する。

30

【0056】

ステップ S2015 において、無線基地局 eNB # 2 は、移動局 UE に対して、「RRC Connection Reconfiguration」を送信し、ステップ S2016 において、移動局 UE は、無線基地局 eNB # 2 に対して、「RRC Connection Reconfiguration Complete」を送信する。

【0057】

交換局 MME は、ステップ S2017 において、下記の式によって、 $K_{eNB[n+2]}$ を算出し、ステップ S2019 において、再接続先無線基地局 # 2 に対して、 $K_{eNB[n+2]}$ 、「KI (=n+1)」を含む「S1 Path Switch Ack（パススイッチ応答信号）」を送信する。

40

【0058】

$$K_{eNB[n+2]} = KDF_1(K_{ASME}, K_{eNB[n+1]})$$

ここで、交換局 MME は、 K_{ASME} 、 $K_{eNB[n+2]}$ 、「KI (=n+1)」を保持している状態となる（ステップ S2018）。

【0059】

ステップ S2010 において、再接続先無線基地局 eNB # 2 は、「S1 Path Switch Ack」を受信して、 $K_{eNB[n+1]}$ 、 $K_{eNB[n+2]}$ 、「KI

50

($=n+1$)」を保持している状態となる。

【0060】

すなわち、ここで、再接続先セルを管理する無線基地局 $eNB\#2$ は、移動局 UE の次の再接続先セルと移動局 UE との間の通信に用いられる予定の所定鍵を生成するための第1鍵 $K_{eNB[n+2]}$ を取得する。

【0061】

以上の手順により、 $Inter-eNB$ 再接続手順において、 K_{eNB} 及び所定鍵が更新される。

【0062】

(本発明の第1の実施形態に係る移動通信システムの作用・効果)

10

本発明の第1の実施形態に係る移動通信システムによれば、簡素化された手順で、再接続先セルを管理する無線基地局 eNB 又は $eNB\#2$ で用いられる $K_{eNB[n+1]}$ 等を生成することができる。

【0063】

(本発明の第2の実施形態に係る移動通信システム)

図5乃至図7を参照して、本発明の第2の実施形態に係る移動通信システムについて、上述の第1の実施形態に係る移動通信システムとの相違点に着目して説明する。

【0064】

図5に、本実施形態に係る移動通信システムで用いられる鍵(すなわち、所定鍵の算出に用いられる鍵)の階層構造及び算出手順の一例について示す。

20

【0065】

図5に示すように、 RRC プロトコルにおける「Integrity Protection」で用いられる鍵 K_{RRC_IP} 、 RRC プロトコルにおける「Ciphering」で用いられる鍵 K_{RRC_Ciph} 及び AS の U プレーンにおける「Ciphering」で用いられる鍵 K_{UP_Ciph} は、 $K_{eNB[n][m]}$ を用いて生成される。

【0066】

また、 $K_{eNB[n][m]}$ は、 $K_{eNB[n]}$ を用いて、下記の式によって算出される。

【0067】

$$K_{eNB[n][0]} = K_{eNB[n]}$$

30

$$K_{eNB[n][m+1]} = KDF_2(K_{eNB[n][m]}), (m \geq 0)$$

さらに、 $K_{eNB[n]}$ は、 K_{ASME} を用いて、下記の式によって算出される。

【0068】

$$K_{eNB[0]} = KDF_0(K_{ASME}, NAS_SN)$$

$$K_{eNB[n+1]} = KDF_1(K_{ASME}, K_{eNB[n]}), (n \geq 0)$$

以下、図6及び図7を参照して、本実施形態に係る移動通信システムの動作について説明する。

【0069】

第1に、図6を参照して、本実施形態に係る移動通信システムにおける $Intra-eNB$ 再接続手順(無線基地局内再接続手順)について説明する。

40

【0070】

図11に示すように、 $Intra-eNB$ 再接続手順の開始前の段階では、移動局 UE は、 $K_{eNB[n]}$ 、 $K_{eNB[n][m]}$ 、「 $KI(=n)$ 」、「 $RC(=m)$ 」を保持しており(ステップ $S3001$)、無線基地局 eNB は、 $K_{eNB[n]}$ 、 $K_{eNB[n+1]}$ 、 $K_{eNB[n][m]}$ 、「 $KI(=n)$ 」、「 $RC(=m)$ 」を保持しており(ステップ $S3002$)、交換局 MME は、 K_{ASME} 、 $K_{eNB[n+1]}$ 、「 $KI(=n)$ 」を保持している(ステップ $S3003$)。

【0071】

ステップ $S3004$ において、移動局 UE と無線基地局 eNB との間で RRC コネクションが確立されており、無線基地局 eNB と交換局 MME との間で $S1$ コネクションが確

50

立されている状態で、移動局UEは、上述のRRCコネクションにおいて、無線リンク障害(RLF: Radio Link Failure)を検出する。

【0072】

その後、移動局UEは、ステップS3005において、セル選択処理を行い、ステップS3006において、選択したセル(或いは、選択したセルを管理する無線基地局eNB)に対して、共通制御チャネルを介して、「RRC Connection Re-establishment Request (再接続要求信号)」を送信する。

【0073】

無線基地局eNBは、ステップS3007において、移動局UEに対して、「KI(=n)」、「RC(=m+1)」を含む「RRC Connection Re-establishment (再接続応答信号)」を送信する。 10

【0074】

ここで、移動局UEは、ステップS3008において、下記の式によって、 $K_{eNB[n][m+1]}$ を算出し、ステップS3009において、 $K_{eNB[n]}$ 、 $K_{eNB[n][m+1]}$ 、「KI(=n+1)」、「RC(=m+1)」を保持している状態になる。

【0075】

$$K_{eNB[n][m+1]} = KDF_2(K_{eNB[n][m]})$$

同様に、無線基地局eNBは、ステップS3010において、下記の式によって、 $K_{eNB[n][m+1]}$ を算出し、ステップS3011において、 $K_{eNB[n]}$ 、 $K_{eNB[n+1]}$ 、 $K_{eNB[n][m+1]}$ 、「KI(=n+1)」、「RC(=m+1)」を保持している状態になる。 20

【0076】

$$K_{eNB[n][m+1]} = KDF_2(K_{eNB[n][m]})$$

移動局UEは、ステップS3012において、かかる $K_{eNB[n+1]}$ を用いて、無線基地局eNBに対して、「RRC Connection Re-establishment Complete (再接続完了信号)」を送信する。

【0077】

ステップS3013において、無線基地局eNBは、移動局UEに対して、「RRC Connection Reconfiguration」を送信し、ステップS3014において、移動局UEは、無線基地局eNBに対して、「RRC Connection Reconfiguration Complete」を送信する。 30

【0078】

本実施例により、Intra-eNB再接続手順における「Path Switch」を省くことができる。

【0079】

第2に、図7を参照して、本実施形態に係る移動通信システムにおけるInter-eNB再接続手順(異無線基地局間再接続手順)について説明する。

【0080】

図7に示すように、Inter-eNB再接続手順の開始前の段階では、移動局UEは、 $K_{eNB[n]}$ 、 $K_{eNB[n][m]}$ 、「KI(=n)」、「RC(=m)」を保持しており(ステップS4001)、無線基地局eNB#1は、 $K_{eNB[n]}$ 、 $K_{eNB[n+1]}$ 、 $K_{eNB[n][m]}$ 、「KI(=n)」、「RC(=m)」を保持しており(ステップS4002)、交換局MMEは、 K_{ASME} 、 $K_{eNB[n+1]}$ 、「KI(=n)」を保持している(ステップS4003)。 40

【0081】

ステップS4004において、無線基地局eNB#1は、周辺の無線基地局eNB#2に対して、 $K_{eNB[n+1]}$ 、「KI(=n+1)」を含む「X2 HO Preparation (ハンドオーバー準備信号)」を送信する。

【0082】

無線基地局 eNB # 2 は、ステップ S 4 0 0 5 及び S 4 0 0 6 において、 $K_{eNB[n+1]}$ 、 $K_{eNB[n+1][0]}$ 、「KI (=n+1)」、「RC (=0)」を記憶する。ここで、 $K_{eNB[n+1][0]} = K_{eNB[n+1]}$ であるものとする。

【0083】

ステップ S 4 0 0 7 において、無線基地局 eNB # 2 は、無線基地局 eNB # 1 に対して、「X2 HO Preparation Ack (ハンドオーバー準備応答信号)」を送信する。

【0084】

すなわち、ここで、再接続先セルを管理する無線基地局 eNB # 2 は、移動局 UE との間の通信に用いられる予定の所定鍵を生成するための第 1 鍵 $K_{eNB[n+1][0]}$ を取得する。

【0085】

ステップ S 2 4 0 0 8 において、移動局 UE と無線基地局 eNB # 1 との間で RRC コネクションが確立されており、無線基地局 eNB # 1 と交換局 MME との間で S1 コネクションが確立されている状態で、移動局 UE は、上述の RRC コネクションにおいて、RLF を検出する。

【0086】

その後、移動局 UE は、ステップ S 4 0 0 9 において、セル選択処理を行い、ステップ S 4 0 1 0 において、選択した再接続先セル（或いは、再接続先無線基地局）eNB # 2 に対して、共通制御チャネルを介して、「RRC Connection Re-establishment Request」を送信する。

【0087】

再接続先無線基地局 eNB # 2 は、ステップ S 4 0 1 1 において、移動局 UE に対して、「KI (=n+1)」、「RC (=0)」を含む「RRC Connection Re-establishment」を送信する。

【0088】

移動局 UE は、ステップ S 4 0 1 2 において、下記の式によって、 $K_{eNB[n+1]}$ 、 $K_{eNB[n+1][0]}$ を算出し、ステップ S 4 0 1 3 において、 $K_{eNB[n+1]}$ 、 $K_{eNB[n+1][0]}$ 、「KI (=n+1)」、「RC (=0)」を保持している状態となる（ステップ S 4 0 1 3）。

【0089】

$$K_{eNB[n+1]} = KDF_1(K_{ASME}, K_{eNB[n]})$$

$$K_{eNB[n+1][0]} = K_{eNB[n+1]}$$

移動局 UE は、ステップ S 4 0 1 4 において、かかる $K_{eNB[n+1]}$ を用いて、再接続先無線基地局 eNB # 2 に対して、「RRC Connection Re-establishment Complete」を送信する。

【0090】

ステップ S 4 0 1 5 において、再接続先無線基地局 eNB # 2 は、交換局 MME に対して、「KI (=n+1)」を含む「S1 Path Switch」を送信する。

【0091】

ステップ S 4 0 1 6 において、再接続先無線基地局 eNB # 2 は、移動局 UE に対して、「RRC Connection Reconfiguration」を送信し、ステップ S 4 0 1 7 において、移動局 UE は、再接続先無線基地局 eNB # 2 に対して、「RRC Connection Reconfiguration Complete」を送信する。

【0092】

交換局 MME は、ステップ S 4 0 1 8 において、下記の式によって、 $K_{eNB[n+2]}$ を算出し、ステップ S 4 0 1 9 において、 K_{KASME} 、 $K_{eNB[n+2]}$ 、「KI (=n+1)」を保持している状態となる。

【0093】

10

20

30

40

50

$K_{eNB[n+2]} = KDF_1(K_{ASME}, K_{eNB[n+1]})$

ステップS4020において、交換局MMEは、再接続先無線基地局eNB#2に対して、 $K_{eNB[n+2]}$ 、「KI(=n+1)」を含む「S1 Path Switch Ack」を送信する。

【0094】

ここで、再接続先無線基地局eNB#2は、ステップS4021において、 $K_{eNB[n+1]}$ 、 $K_{eNB[n+2]}$ 、「KI(=n+1)」、 $K_{eNB[n+1][0]}$ 、「RC(=0)」を保持している状態となる。

【0095】

以上、図6及び図7に示したように、パラメータ「RC」による無線基地局での K_{eNB} の更新を導入することで、交換局MMEへの問い合わせを省きつつ、 K_{eNB} を更新できる。

【0096】

なお、図6及び図7の手順において、「RRC RRC Re-establishment」では、パラメータ「RC」を省いてもよい。

【0097】

パラメータ「RC」を「RRC RRC Re-establishment」に含めずに省いた場合、パラメータ「KI」がインクリメントされたか否かに基づき、「RC」をインクリメントすべきか否かを判定することができる。

【0098】

「KI」がインクリメントされた場合は、「RC」を「0」にリセットし、「KI」がインクリメントされなかった場合には、「RC」をインクリメントすればよい。

【0099】

或いは、パラメータ「RC」を「RRC RRC Re-establishment」に含めずに省いた場合、移動局UEは、「RC」の値を現在値のまま維持した場合と、現在値からインクリメントした場合と、「0」にリセットした場合の各場合を試行し、受信したメッセージに対する「Integrity」をチェックすることで、どの場合が正しかったかを自律的に判定してもよい。

【0100】

(変更例)

なお、上述の交換局MMEや無線基地局eNBや移動局UEの動作は、ハードウェアによって実施されてもよいし、プロセッサによって実行されるソフトウェアモジュールによって実施されてもよいし、両者の組み合わせによって実施されてもよい。

【0101】

ソフトウェアモジュールは、RAM(Random Access Memory)や、フラッシュメモリや、ROM(Read Only Memory)や、EPROM(Erasable Programmable ROM)や、EEPROM(Electronically Erasable and Programmable ROM)や、レジスタや、ハードディスクや、リムーバブルディスクや、CD-ROMといった任意形式の記憶媒体内に設けられていてもよい。

【0102】

かかる記憶媒体は、プロセッサが当該記憶媒体に情報を読み書きできるように、当該プロセッサに接続されている。また、かかる記憶媒体は、プロセッサに集積されていてもよい。また、かかる記憶媒体及びプロセッサは、ASIC内に設けられていてもよい。かかるASICは、交換局MMEや無線基地局eNBや移動局UE内に設けられていてもよい。また、かかる記憶媒体及びプロセッサは、ディスクリットコンポーネントとして交換局MMEや無線基地局eNBや移動局UE内に設けられていてもよい。

【0103】

以上、上述の実施形態を用いて本発明について詳細に説明したが、当業者にとっては、本発明が本明細書中に説明した実施形態に限定されるものではないということは明らかで

10

20

30

40

50

ある。本発明は、特許請求の範囲の記載により定まる本発明の趣旨及び範囲を逸脱することなく修正及び変更態様として実施することができる。従って、本明細書の記載は、例示説明を目的とするものであり、本発明に対して何ら制限的な意味を有するものではない。

【符号の説明】

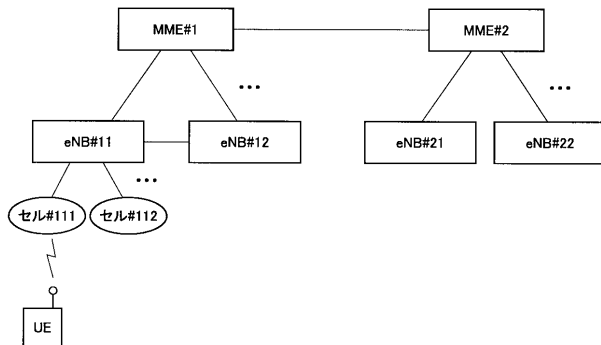
【 0 1 0 4 】

M M E … 交換局

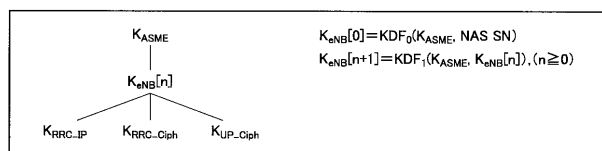
e N B … 無線基地局

U E … 移動局

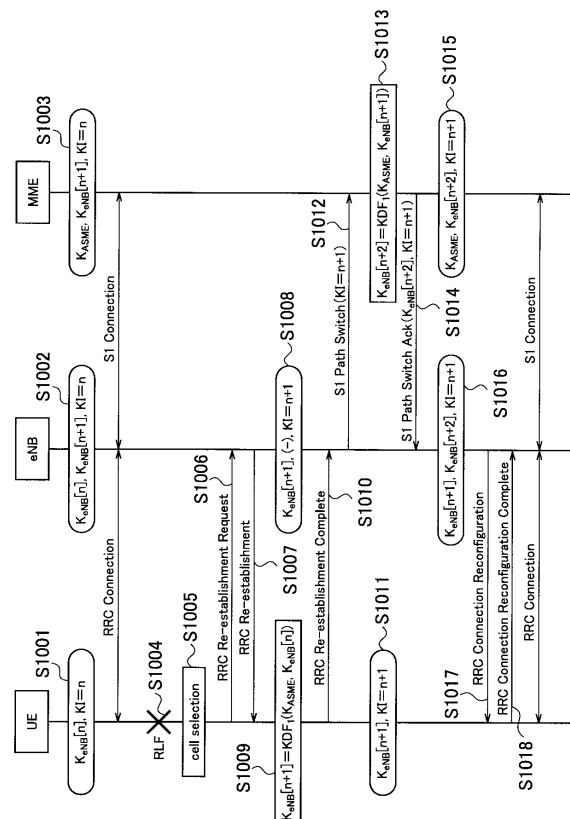
【 図 1 】



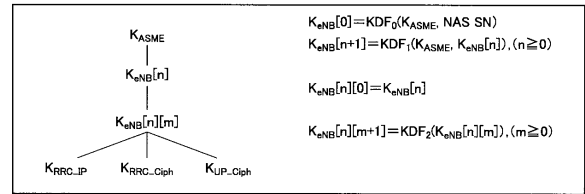
【 図 2 】



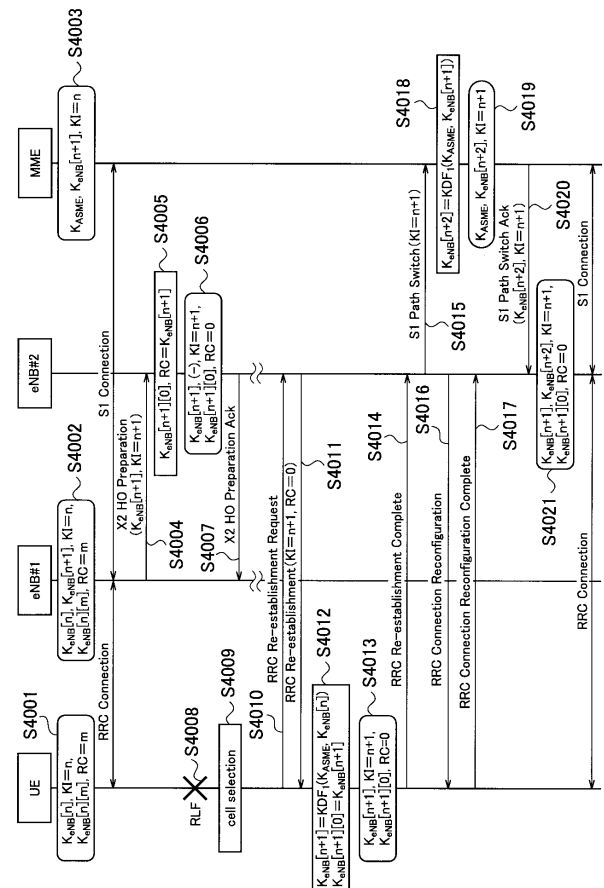
【 図 3 】



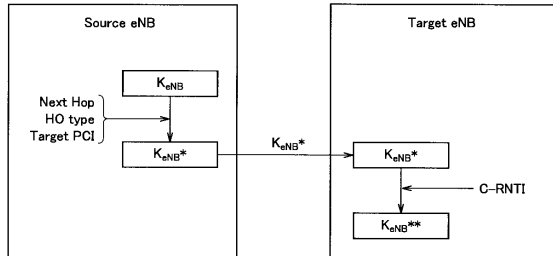
【図 5】



【图 7】



【図 8】



フロントページの続き

- (72)発明者 岩村 幹生
東京都千代田区永田町二丁目1 1 番1 号 株式会社エヌ・ティ・ティ・ドコモ内
- (72)発明者 ウリ A. ハプサリ
東京都千代田区永田町二丁目1 1 番1 号 株式会社エヌ・ティ・ティ・ドコモ内
- (72)発明者 矢葺 匠吾
東京都千代田区永田町二丁目1 1 番1 号 株式会社エヌ・ティ・ティ・ドコモ内
- (72)発明者 アルフ ツーゲンマイヤー
東京都千代田区永田町二丁目1 1 番1 号 株式会社エヌ・ティ・ティ・ドコモ内
- F ターム(参考) 5J104 AA16 AA32 EA04 EA16 JA03 NA02 NA37 PA01
5K067 AA34 AA42 BB32 DD17 DD24 DD51 EE02 EE10 EE16 FF02
HH11 HH22 HH23 KK15