

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2012 年 10 月 11 日(11.10.2012)



(10) 国際公開番号
WO 2012/137684 A1

- (51) 国際特許分類:
H04W 12/04 (2009.01) *H04W 92/18* (2009.01)
- (21) 国際出願番号: PCT/JP2012/058606
- (22) 国際出願日: 2012 年 3 月 30 日(30.03.2012)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2011-083696 2011 年 4 月 5 日(05.04.2011) JP
- (71) 出願人 (米国を除く全ての指定国について): 株式会社エヌ・ティ・ティ・ドコモ (NTT DOCOMO, INC.) [JP/JP]; 〒1006150 東京都千代田区永田町二丁目 1 1 番 1 号 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 岩村 幹生 (IWAMURA, Mikio) [JP/—]; 〒1006150 東京都千代田区永田町二丁目 1 1 番 1 号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP). ハプサリ ウリ アンダルマワンティ (HAPSARI, Wuri Andarmawanti) [ID/—]; 〒1006150 東京都千代田区永田町二丁目 1 1 番 1 号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP).

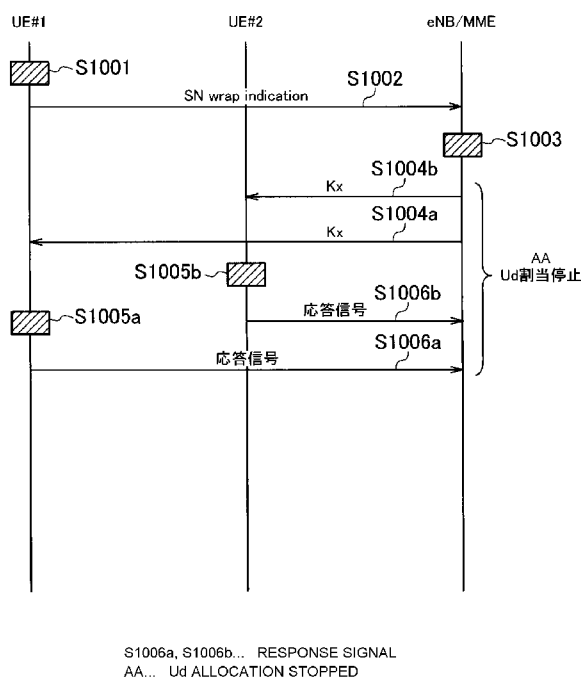
-]; 〒1006150 東京都千代田区永田町二丁目 1 1 番 1 号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP).
- (74) 代理人: 三好 秀和, 外 (MIYOSHI, Hidekazu et al.); 〒1050001 東京都港区虎ノ門一丁目 2 番 8 号 虎ノ門琴平タワー Tokyo (JP).
- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, 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, IS, KE, KG, KM, 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, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨー

[続葉有]

(54) Title: MOBILE COMMUNICATIONS METHOD, WIRELESS BASE STATION, MOBILE MANAGEMENT NODE, AND MOBILE STATION

(54) 発明の名称: 移動通信方法、無線基地局、移動管理ノード及び移動局

[図5]



送受信を継続する工程とを有する。

(57) Abstract: This mobile communications method has: a step in which a wireless base station (eNB) or a mobile management node (MME) refreshes a prescribed parameter (X) for calculating a key (K_x) or a key (K_x) used when sending and receiving data signals that have passed through a U_d interface, when an "SN wrap indication" or a key refresh request signal is received from a mobile station (UE#1) or a mobile station (UE#2); a step in which the wireless base station (eNB) or the mobile management node (MME) notify the mobile station (UE#1) and the mobile station (UE#2) of the refreshed key (K_x) or the prescribed parameter (X); and a step in which the mobile station (UE#1) and the mobile station (UE#2) continue to send and receive data signals that have passed through the U_d interface, using the key (K_x) calculated on the basis of the notified key (K_x) or prescribed parameter (X).

(57) 要約: 本発明に係る移動通信方法は、無線基地局 eNB 又は移動管理ノード MME が、移動局 UE # 1 又は移動局 UE # 2 から「SN wrap indication」又は鍵更新要求信号を受信した場合、U_d インタフェースを介したデータ信号の送受信に用いる鍵 K_x 又は鍵 K_x を算出するための所定パラメータ X を更新する工程と、無線基地局 eNB 又は移動管理ノード MME が、移動局 UE # 1 及び移動局 UE # 2 に対して、更新した鍵 K_x 又は所定パラメータ X を通知する工程と、移動局 UE # 1 及び移動局 UE # 2 が、通知された鍵 K_x 又は所定パラメータ X に基づいて算出した鍵 K_x を用いて、U_d インタフェースを介したデータ信号の



ロツパ (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), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ,
GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告 (条約第 21 条(3))

明 細 書

発明の名称：

移動通信方法、無線基地局、移動管理ノード及び移動局

技術分野

[0001] 本発明は、移動通信方法、無線基地局、移動管理ノード及び移動局に関する。

背景技術

[0002] W-CDMA (Wideband-Code Division Multiple Access) 方式やLTE (Long Term Evolution) の方式等のセルラー方式の移動通信システムでは、複数の移動局UE同士の通信は、無線アクセスネットワーク装置やコアネットワーク装置等を介して行われるように構成されている。

先行技術文献

非特許文献

[0003] 非特許文献1：3GPP TS 36.300

発明の概要

発明が解決しようとする課題

[0004] しかしながら、従来のセルラー方式の移動通信システムでは、複数の移動局UEが、同一セル（或いは、無線アクセスネットワーク装置配下のセル）内に配置されている場合であっても、データ信号及び制御信号の両方が、無線アクセスネットワーク装置を介して送受信されるように構成されているため、無線アクセスネットワーク装置の処理負荷が増大してしまうという問題点があった。

[0005] かかる問題点を解決するために、複数の移動局が、無線基地局との間で設定されているUuインタフェースを介することなく、移動局間インタフェース（以下、Udインタフェース）を介して、データ信号の送受信を行うことを想定することができる。

- [0006] また、かかる場合には、U d インタフェースを介して送受信されるデータ信号のセキュリティ（秘匿や改竄検出）を確保するために、U u インタフェースを介して送受信されるデータ信号のセキュリティ（秘匿や改竄検出）を確保するために用いられる鍵とは異なる移動局間通信用鍵（以下、鍵 K_x ）を用いることが想定される。
- [0007] ここで、一般に、通信に用いる鍵として、長時間同じ鍵を用いると、セキュリティの脆弱性に繋がるため、ある程度頻繁に、かかる鍵を更新することが重要となる。例えば、データのシーケンス番号（S N : S e q u e n c e N u m b e r）が一巡する前に、かかる鍵を更新することが望まれる。
- [0008] しかしながら、既存の移動通信システムの仕組みでは、かかる鍵 K_x を適切なタイミングで更新することができないという問題点があった。
- [0009] 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、適切なタイミングで鍵 K_x を更新することができる移動通信方法、無線基地局、移動管理ノード及び移動局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

- [0010] 本発明の第1の特徴は、第1移動局と第2移動局との間で、無線基地局との間で設定されている無線基地局インタフェースを介することなく、該第1移動局と該第2移動局との間で設定されている移動局間インタフェースを介して、データ信号の送受信を行う移動通信方法であって、前記第1移動局又は前記第2移動局が、前記無線基地局に対して、前記移動局間インタフェースを介して送受信するデータ信号のシーケンス番号が一巡するタイミングが近づいていることを示す指示信号又は鍵の更新を要求する鍵更新要求信号を送信する工程と、前記無線基地局又は移動管理ノードが、前記指示信号又は前記鍵更新要求信号を受信した場合、前記移動局間インタフェースを介したデータ信号の送受信に用いる移動局間通信用鍵又は該移動局間通信用鍵を算出するための所定パラメータを更新する工程と、前記無線基地局又は移動管理ノードが、前記第1移動局及び前記第2移動局に対して、更新した前記移動局間通信用鍵又は前記所定パラメータを通知する工程と、前記第1移動局

及び前記第2移動局が、前記移動局間インタフェースを介したデータ信号の送受信に用いる移動局間通信用鍵を、通知された前記移動局間通信用鍵又は前記所定パラメータに基づいて算出した移動局間通信用鍵に更新する工程とを有することを要旨とする。

[0011] 本発明の第2の特徴は、第1移動局と第2移動局との間で、無線基地局との間で設定されている無線基地局インタフェースを介することなく、該第1移動局と該第2移動局との間で設定されている移動局間インタフェースを介して、データ信号の送受信を行うことができるように構成されている移動通信システムで用いられる無線基地局であって、前記第1移動局又は前記第2移動局から、前記移動局間インタフェースを介して送受信するデータ信号のシーケンス番号が一巡するタイミングが近づいていることを示す指示信号又は鍵の更新を要求する鍵更新要求信号を受信するように構成されている受信部と、前記指示信号又は前記鍵更新要求信号を受信した場合、前記移動局間インタフェースを介したデータ信号の送受信に用いる移動局間通信用鍵又は該移動局間通信用鍵を算出するための所定パラメータを更新するように構成されている更新部と、前記第1移動局及び前記第2移動局に対して、更新した前記移動局間通信用鍵又は前記所定パラメータを通知するように構成されている送信部とを具備することを要旨とする。

[0012] 本発明の第3の特徴は、第1移動局と第2移動局との間で、無線基地局との間で設定されている無線基地局インタフェースを介することなく、該第1移動局と該第2移動局との間で設定されている移動局間インタフェースを介して、データ信号の送受信を行うことができるように構成されている移動通信システムで用いられる移動管理ノードであって、前記第1移動局又は前記第2移動局から、前記移動局間インタフェースを介して送受信するデータ信号のシーケンス番号が一巡するタイミングが近づいていることを示す指示信号又は鍵の更新を要求する鍵更新要求信号を受信するように構成されている受信部と、前記指示信号又は前記鍵更新要求信号を受信した場合、前記移動局間インタフェースを介したデータ信号の送受信に用いる移動局間通信用鍵

又は該移動局間通信用鍵を算出するための所定パラメータを更新するように構成されている更新部と、前記第 1 移動局及び前記第 2 移動局に対して、更新した前記移動局間通信用鍵又は前記所定パラメータを通知するように構成されている送信部とを具備することを要旨とする。

[0013] 本発明の第 4 の特徴は、第 1 移動局と第 2 移動局との間で、無線基地局との間で設定されている無線基地局インタフェースを介することなく、該第 1 移動局と該第 2 移動局との間で設定されている移動局間インタフェースを介して、データ信号の送受信を行うことができるように構成されている移動通信システムにおいて該第 1 移動局として機能する移動局であって、前記無線基地局に対して、前記移動局間インタフェースを介して送受信するデータ信号のシーケンス番号が一巡するタイミングが近づいていることを示す指示信号又は鍵の更新を要求する鍵更新要求信号を送信するように構成されている送信部と、前記指示信号又は前記鍵更新要求信号を受信した前記無線基地局又は移動管理ノードから、前記移動局間インタフェースを介したデータ信号の送受信に用いる移動局間通信用鍵又は該移動局間通信用鍵を算出するための所定パラメータを受信するように構成されている受信部と、前記移動局間インタフェースを介したデータ信号の送受信に用いる移動局間通信用鍵を、受信した前記移動局間通信用鍵又は前記所定パラメータに基づいて算出した移動局間通信用鍵に更新するように構成されている更新部とを具備することを要旨とする。

発明の効果

[0014] 以上説明したように、本発明によれば、適切なタイミングで鍵 K_x を更新することができる移動通信方法、無線基地局、移動管理ノード及び移動局を提供することができる。

図面の簡単な説明

[0015] [図1]図 1 は、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]図 2 は、本発明の第 1 の実施形態に係る移動局の機能ブロック図である

。

[図3]図3は、本発明の第1の実施形態に係る移動局の動作を説明するための図である。

[図4]図4は、本発明の第1の実施形態に係る無線基地局又は移動管理ノードの機能ブロック図である。

[図5]図5は、本発明の第1の実施形態に係る移動通信システムの動作を示すシーケンス図である。

発明を実施するための形態

[0016] (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5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。

[0017] 本実施形態に係る移動通信システムは、LTE方式の移動通信システムであって、図1に示すように、移動管理ノードMME (Mobility Management Entity) と、移動管理ノードMME配下に接続されている無線基地局eNBとを具備している。なお、本発明は、LTE方式以外のセルラー方式の移動通信システムにも適用可能である。

[0018] ここで、無線基地局eNBと移動局UE#1/UE#2との間では、Uuインタフェースを介してデータ信号が送受信されるように構成されており、移動局UE#1と移動局UE#2との間では、Udインタフェースを介してデータ信号が送受信されるように構成されている。

[0019] すなわち、移動局UE#1は、移動局UE#2との間で、無線基地局eNBを介して (Uuインタフェースを介して) データ信号を送受信することもできるし、無線基地局eNBを介さないで (Udインタフェースを介して) データ信号を送受信することもできる。

[0020] 同様に、移動局UE#2は、移動局UE#1との間で、無線基地局eNBを介して (Uuインタフェースを介して) データ信号を送受信することもできるし、無線基地局eNBを介さないで (Udインタフェースを介して) データ信号を送受信することもできる。

- [0021] ここで、UuインタフェースやUdインタフェースを介して送受信されるデータ信号には、セキュリティ（秘匿や改竄検出）が適用される。セキュリティを適用するために、送受信エンティティ間で、共通の鍵が用意される。
- [0022] LTE方式のUuインタフェースにおいて用いられる鍵の生成方法及び更新方法は、3GPPのTS 33.401等に規定されている。本発明は、Udインタフェースにおいて用いられる鍵 K_x の更新方法に係るものである。
- [0023] 移動局UE#1の構成及び移動局UE#2の構成は、基本的に同一であるため、以下、代表して、移動局UE#1の構成について説明する。
- [0024] 図2に示すように、移動局UE#1は、管理部11と、PDCP (Packet Data Convergence Protocol) レイヤ機能部12aと、RLC (Radio Link Control) レイヤ機能部12bと、送信部13と、受信部14と、更新部15とを具備している。
- [0025] 管理部11は、Udインタフェースを介して送受信されるデータ信号のセキュリティに用いる鍵 K_x を管理するように構成されている。
- [0026] 送信部13は、Uuインタフェースを介して、無線基地局eNBに対して、データ信号や制御信号を送信するように構成されており、Udインタフェースを介して、移動局UE#2に対して、データ信号を送信するように構成されている。
- [0027] 受信部14は、Uuインタフェースを介して、無線基地局eNBから、データ信号や制御信号を受信するように構成されており、Udインタフェースを介して、移動局UE#2から、データ信号を受信するように構成されている。
- [0028] PDCPレイヤ機能部12aは、PDCPレイヤにおける処理を行うように構成されている。
- [0029] 例えば、図3に示すように、PDCPレイヤ機能部12aは、上位レイヤから受信したIPパケットを、PDCP-SDU (Service Data Unit) とし、かかるPDCP-SDUに対して、PDCPレイヤにおけ

るシーケンス番号SNを含むヘッダを付与することによって、PDCP-PDU (Protocol Data Unit) を生成して、RLCレイヤ機能部12bに送信するように構成されている。

[0030] ここで、PDCPレイヤ機能部12aは、鍵 K_x 或いは鍵 K_x から算出される鍵を用いて、送信するPDCP-SDUごとにサイファリング処理を施すように構成されている。

[0031] 同様に、PDCPレイヤ機能部12aは、鍵 K_x 或いは鍵 K_x から算出される鍵を用いて、受信したPDCP-SDUごとにデサイファリング処理を施すように構成されている。

[0032] また、PDCPレイヤ機能部12aは、鍵 K_x 或いは鍵 K_x から算出される鍵を用いて、PDCP-SDUごとにインテグリティプロテクション処理を施すように構成されていてもよい。

[0033] すなわち、PDCPレイヤ機能部12aは、送信するPDCP-SDUごとにチェックサムに当たるMAC-Iを生成し、ヘッダに含めてもよい。この場合、PDCPレイヤ機能部12aは、受信したPDCP-SDUごとにMAC-Iを検証し、改竄検出する。

[0034] また、PDCPレイヤ機能部12aは、RLCレイヤ機能部12bから受信したRLC-SDU内のPDCP-PDUのヘッダに含まれるシーケンス番号SNに基づいて、「PDCP status report」を生成するように構成されている。

[0035] また、PDCPレイヤ機能部12aは、Udインタフェースを介して送受信するデータ信号のシーケンス番号（例えば、PDCPレイヤで用いられているシーケンス番号）が一巡するタイミングが近づいていることを検出した場合、「SN wrap indication」を生成するように構成されている。

[0036] 例えば、PDCPレイヤにおけるシーケンス番号が「0」～「127」の範囲で巡回して用いられる場合には、PDCPレイヤ機能部12aは、シーケンス番号「120」を含むヘッダを付与した場合に、送信部13に対して

、「SN wrap indication」を生成するように構成されていてもよい。

[0037] 或いは、PDCPレイヤにおけるシーケンス番号が「0」～「127」の範囲で巡回して用いられる場合には、PDCPレイヤ機能部12aは、シーケンス番号「120」を含むヘッダが付与されたPDCP-PDUを受信した場合に、送信部13に対して、「SN wrap indication」を生成するように構成されていてもよい。

[0038] RLCレイヤ機能部12bは、PDCPレイヤ機能部12aから受信したPDCP-PDUに対して、所定サイズとなるように1以上のPDCP-SDUを適宜分割・結合し、これにヘッダを付与することによって、RLC-PDUを生成して、MAC(Media Access Control)レイヤに送信するように構成されている。

[0039] ここで、送信部13は、上述したPDCPやRLCやMACの各レイヤで処理されたPDUについて、Uuインタフェースを介することなく、Udインタフェースを介して、移動局UE#2に対して、データ信号として送信するように構成されている。

[0040] また、送信部13は、PDCPレイヤ機能部12aによって生成された「SN wrap indication」について、移動管理ノードMME又は無線基地局eNBに対して送信するように構成されている。

[0041] なお、かかる「SN wrap indication」は、PDCPレイヤの制御信号としてではなく、RRCメッセージ又はNASメッセージとして送信されてもよい。

[0042] また、かかる「SN wrap indication」は、鍵の更新を要求する「鍵更新要求信号」として定義されてもよい。

[0043] また、受信部14は、移動局UE#2から、Uuインタフェースを介することなく、Udインタフェースを介して、「PDCP status report」を含むデータ信号を受信するように構成されている。

[0044] 更新部15は、管理部11によって管理されている鍵 K_x を更新するように

構成されている。

[0045] 例えば、更新部 15 は、管理部 11 によって管理されている鍵 K_x を、受信部 14 によって移動管理ノード MME 又は無線基地局 eNB から受信した鍵 K_x に置換するように構成されていてもよい。

[0046] 或いは、更新部 15 は、受信部 14 によって移動管理ノード MME 又は無線基地局 eNB から受信した所定パラメータ X に基づいて鍵 K_x を算出し、管理部 11 によって管理されている鍵 K_x を、算出した鍵 K_x に置換するように構成されていてもよい。

[0047] また、更新部 15 は、Ud インタフェースを介したデータ信号の送受信に用いる鍵 K_x を更新する際に、Ud インタフェースにおける RLC レイヤ（レイヤ 2）以下のプロトコルエンティティをリセットするように構成されていてもよい。

[0048] なお、PDCP レイヤ機能部 12a は、受信部 14 によって上述の鍵 K_x 又は所定パラメータ X が受信された際に、「PDCP status report」を生成するように構成されていてもよい。

[0049] 図 4 に示すように、無線基地局 eNB 又は移動管理ノード MME は、管理部 21 と、受信部 22 と、更新部 23 と、送信部 24 とを具備している。

[0050] 管理部 21 は、各移動局 UE における Ud インタフェースを介した通信用の鍵 K_x （或いは、かかる鍵 K_x を算出するための所定パラメータ X ）を管理するように構成されている。

[0051] 受信部 22 は、各移動局 UE によって送信されたデータ信号や制御信号を受信するように構成されている。

[0052] 例えば、受信部 22 は、各移動局 UE によって送信された「SN wrap indication」を受信するように構成されている。

[0053] 更新部 23 は、受信部 22 によって「SN wrap indication」が受信された場合、かかる「SN wrap indication」の送信元の移動局 UE（例えば、移動局 UE #1）と通信相手の移動局 UE（例えば、移動局 UE #2）との間で Ud インタフェースを介して行われ

る通信用の鍵 K_x （或いは、かかる鍵 K_x を算出するための所定パラメータ X ）を更新するように構成されている。

[0054] ここで、更新部23は、送信元の移動局UEに対して送信すべきの鍵 K_x （或いは、かかる鍵 K_x を算出するための所定パラメータ X ）と通信相手の移動局UEに対して送信すべき鍵 K_x （或いは、かかる鍵 K_x を算出するための所定パラメータ X ）とを同じものにしてもよいし異なるものにしてもよい。

[0055] 送信部24は、移動局UEに対して、データ信号や制御信号を送信するように構成されている。

[0056] 例えば、送信部24は、更新部23によって更新された鍵 K_x （或いは、かかる鍵 K_x を算出するための所定パラメータ X ）について、「SN wrap indication」の送信元の移動局UE及び通信相手の移動局UEに対して送信するように構成されている。

[0057] 送信部24は、更新部23によって更新された鍵 K_x （或いは、かかる鍵 K_x を算出するための所定パラメータ X ）を、PDCPレイヤの制御信号として送信してもよいし、RRCメッセージ又はNASメッセージとして送信してもよい。

[0058] 以下、図5を参照して、本実施形態に係る移動通信システムにおいて、移動局UE#1と移動局UE#2との間でUdインタフェースを介したデータ信号の送受信が行われている場合の動作について説明する。

[0059] 図5に示すように、移動局UE#1は、ステップS1001において、送信側のPDCPレイヤで用いられているシーケンス番号が一巡するタイミングが近づいていることを検出すると、ステップS1002において、無線基地局eNB又は移動管理ノードMMEに対して、「SN wrap indication」を送信する。

[0060] ここで、移動局UE#1は、ステップS1001において、受信側のPDCPレイヤで用いられているシーケンス番号が一巡するタイミングが近づいていることを検出した場合にも、ステップS1002において、無線基地局eNB又は移動管理ノードMMEに対して、「SN wrap indic

a t i o n」を送信してもよい。

- [0061] 無線基地局 eNB 又は移動管理ノード MME は、「SN wrap in d i c a t i o n」を受信すると、ステップ S 1 0 0 3 において、移動局 U E # 1 と移動局 U E # 2 との間の通信用の鍵 K_x （或いは、かかる鍵 K_x を算出するための所定パラメータ X）を更新し、ステップ S 1 0 0 4 a において、移動局 U E # 1 に対して、かかる鍵 K_x （或いは、かかる鍵 K_x を算出するための所定パラメータ X）を送信し、ステップ S 1 0 0 4 b において、移動局 U E # 2 に対して、かかる鍵 K_x （或いは、かかる鍵 K_x を算出するための所定パラメータ X）を送信する。
- [0062] ここで、移動局 U E # 1 に対して送信される鍵 K_x （或いは、かかる鍵 K_x を算出するための所定パラメータ X）及び移動局 U E # 2 に対して送信される鍵 K_x （或いは、かかる鍵 K_x を算出するための所定パラメータ X）は、同じものであってもよいし、異なるものであってもよい。
- [0063] ステップ S 1 0 0 5 a において、移動局 U E # 1 は、移動局 U E # 2 との間の通信用の鍵 K_x を更新し、ステップ S 1 0 0 5 b において、移動局 U E # 2 は、移動局 U E # 1 との間の通信用の鍵 K_x を更新する。
- [0064] ステップ S 1 0 0 6 a において、移動局 U E # 1 は、無線基地局 eNB 又は移動管理ノード MME に対して、移動局 U E # 2 との間の通信用の鍵 K_x の更新が完了したことを通知する応答信号を送信し、ステップ S 1 0 0 6 b において、移動局 U E # 2 は、無線基地局 eNB 又は移動管理ノード MME に対して、移動局 U E # 1 との間の通信用の鍵 K_x の更新が完了したことを通知する応答信号を送信する。
- [0065] その後、移動局 U E # 1 と移動局 U E # 2 との間のデータ信号の送受信は、更新された鍵 K_x を用いて継続される。
- [0066] なお、無線基地局 eNB 又は移動管理ノード MME は、ステップ S 1 0 0 4 a / S 1 0 0 4 b において鍵 K_x （或いは、かかる鍵 K_x を算出するための所定パラメータ X）を送信してから、ステップ S 1 0 0 6 a / S 1 0 0 6 b において応答信号を受信するまでの間、新たな U d インタフェースの割り当てを

停止してもよい。

[0067] また、移動局UE # 1 及び移動局UE # 2 は、無線基地局eNB又は移動管理ノードMMEから、ステップS1004 a/S1004 bにおいて鍵 K_x （或いは、かかる鍵 K_x を算出するための所定パラメータX）を受信した際に、UdインタフェースのRLCレイヤ以下のプロトコルエンティティをリセットする。

[0068] すなわち、かかる場合、移動局UE # 1 及び移動局UE # 2 は、バッファに溜まっていたPDUを破棄し、MACのHARQプロセス等をリセットする。

[0069] また、移動局UE # 1 及び移動局UE # 2 は、その後、無線基地局eNBから新たなUdインタフェース上の送受信のリソース割当てを受信した際に、互いに「PDCP status report」を交換し、送受信を再開すべきPDCP-SDUのSNについての状態を一致させる。

[0070] 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、送信側或いは受信側の移動局UE # 1 が、PDCPレイヤで用いられているシーケンス番号が一巡するタイミングが近づいていることを検出した場合に、移動局UE # 1 と移動局UE # 2 との間の通信用の鍵 K_x を更新することができるため、移動局UE # 1 と移動局UE # 2 との間の通信におけるセキュリティを確保することができる。

[0071] 以上に述べた本実施形態の特徴は、以下のように表現されていてもよい。

[0072] 本実施形態の第1の特徴は、移動局UE # 1（第1移動局）と移動局UE # 2（第2移動局）との間で、無線基地局eNBとの間で設定されているUuインタフェース（無線基地局インタフェース）を介することなく、移動局UE # 1 と移動局UE # 2 との間に設定されているUdインタフェース（移動局間インタフェース）を介して、データ信号の送受信を行う移動通信方法であって、移動局UE # 1 又は移動局UE # 2 が、無線基地局eNBに対して、「SN wrap indication（移動局間インタフェースを介して送受信するデータ信号のシーケンス番号が一巡するタイミングが近づ

いていることを示す指示信号)」又は鍵の更新を要求する鍵更新要求信号を送信する工程と、無線基地局 eNB 又は移動管理ノード MME が、「SN wrap indication」又は鍵更新要求信号を受信した場合、Ud インタフェースを介したデータ信号の送受信に用いる鍵 K_x （移動局間通信用鍵）又は鍵 K_x を算出するための所定パラメータ X を更新する工程と、無線基地局 eNB 又は移動管理ノード MME が、移動局 UE # 1 及び移動局 UE # 2 に対して、更新した鍵 K_x 又は所定パラメータ X を通知する工程と、移動局 UE # 1 及び移動局 UE # 2 が、Ud インタフェースを介したデータ信号の送受信に用いる鍵 K_x を、通知された鍵 K_x 又は所定パラメータ X に基づいて算出した鍵 K_x に更新する工程とを有することを要旨とする。

[0073] 本実施形態の第 1 の特徴において、移動局 UE # 1 と移動局 UE # 2 との間で、Uu インタフェースを介することなく、Ud インタフェースを介して、「PDCP status report (PDCP ステータスレポート)」の送受信を行う工程を有してもよい。

[0074] 本実施形態の第 1 の特徴において、「PDCP status report」の送受信は、更新された鍵 K_x 又は所定パラメータ X が受信された際に行われてもよい。

[0075] 本実施形態の第 1 の特徴において、移動局 UE # 1 及び移動局 UE # 2 が、Ud インタフェースを介したデータ信号の送受信に用いる鍵 K_x を、通知された鍵 K_x 又は所定パラメータ X に基づいて算出した鍵 K_x に更新した場合に、無線基地局 eNB 又は移動管理ノード MME に対して、その旨を示す応答信号を送信する工程を有してもよい。

[0076] 本実施形態の第 1 の特徴において、無線基地局 eNB 又は移動管理ノード MME は、移動局 UE # 1 及び移動局 UE # 2 に対して鍵 K_x 又は所定パラメータ X を通知してから応答信号を受信するまでの間、新たな Ud インタフェースの割当を停止してもよい。

[0077] 本実施形態の第 1 の特徴において、移動局 UE # 1 及び移動局 UE # 2 は、Ud インタフェースを介したデータ信号の送受信に用いる鍵 K_x を更新する

際に、U d インタフェースにおける R L C レイヤ（レイヤ 2）以下のプロトコルエンティティをリセットしてもよい。

[0078] 本実施形態の第 2 の特徴は、移動局 U E # 1 と移動局 U E # 2 との間で、U u インタフェースを介することなく、U d インタフェースを介して、データ信号の送受信を行うことができるように構成されている移動通信システムで用いられる無線基地局 e N B であって、移動局 U E # 1 又は移動局 U E # 2 から、「S N w r a p i n d i c a t i o n」又は鍵更新要求信号を受信するように構成されている受信部 2 2 と、「S N w r a p i n d i c a t i o n」又は鍵更新要求信号を受信した場合、鍵 K_x 又は所定パラメータ X を更新するように構成されている更新部 2 3 と、移動局 U E # 1 及び移動局 U E # 2 に対して、更新した鍵 K_x 又は所定パラメータ X を通知するように構成されている送信部 2 4 とを具備することを要旨とする。

[0079] 本実施形態の第 2 の特徴において、移動局 U E # 1 及び移動局 U E # 2 に対して鍵 K_x 又は所定パラメータ X を通知してから、移動局 U E # 1 及び移動局 U E # 2 から鍵 K_x の更新が完了した旨を示す応答信号を受信するまでの間、新たな U d インタフェースの割当を停止するように構成されていてもよい。

[0080] 本実施形態の第 3 の特徴は、移動局 U E # 1 と移動局 U E # 2 との間で、U u インタフェースを介することなく、U d インタフェースを介して、データ信号の送受信を行うことができるように構成されている移動通信システムで用いられる移動管理ノード M M E であって、移動局 U E # 1 又は移動局 U E # 2 から、「S N w r a p i n d i c a t i o n」又は鍵更新要求信号を受信するように構成されている受信部 2 2 と、「S N w r a p i n d i c a t i o n」又は鍵更新要求信号を受信した場合、鍵 K_x 又は所定パラメータ X を更新するように構成されている更新部 2 3 と、移動局 U E # 1 及び移動局 U E # 2 に対して、更新した鍵 K_x 又は所定パラメータ X を通知するように構成されている送信部 2 4 とを具備することを要旨とする。

[0081] 本実施形態の第 3 の特徴において、移動局 U E # 1 及び移動局 U E # 2 に

対して鍵 K_x 又は所定パラメータ X を通知してから、移動局UE # 1及び移動局UE # 2から鍵 K_x の更新が完了した旨を示す応答信号を受信するまでの間、新たなUdインタフェースの割当を停止するように構成されていてもよい。

[0082] 本実施形態の第4の特徴は、移動局UE # 2との間で、Uuインタフェースを介することなく、Udインタフェースを介して、データ信号の送受信を行うことができるように構成されている移動通信システムにおいて用いられる移動局UE # 1であって、無線基地局eNBに対して、「SN wrap indication」又は鍵更新要求信号を送信するように構成されている送信部13と、「SN wrap indication」又は鍵更新要求信号を受信した無線基地局eNB又は移動管理ノードMMEから、鍵 K_x 又は所定パラメータ X を受信するように構成されている受信部14と、Udインタフェースを介したデータ信号の送受信に用いる鍵 K_x を、受信した鍵 K_x 又は所定パラメータ X に基づいて算出した鍵 K_x に更新するように構成されている更新部15とを具備することを要旨とする。

[0083] 本実施形態の第4の特徴において、送信部13及び受信部14は、移動局UE # 2との間で、Uuインタフェースを介することなく、Udインタフェースを介して、「PDCP status report」の送受信を行うように構成されていてもよい。

[0084] 本実施形態の第4の特徴において、送信部13及び受信部14は、更新された鍵 K_x 又は所定パラメータ X が受信された際に、「PDCP status report」の送受信を行うように構成されていてもよい。

[0085] 本実施形態の第4の特徴において、更新部15は、Udインタフェースを介したデータ信号の送受信に用いる鍵 K_x を更新する際に、UdインタフェースにおけるRLCレイヤ（レイヤ2）以下のプロトコルエンティティをリセットするように構成されていてもよい。

[0086] なお、上述の無線基地局eNBや移動局UE等の動作は、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。

[0087] 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 (Electrically 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。

[0088] 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、無線基地局eNBや移動局UE等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無線基地局eNBや移動局UE等内に設けられていてもよい。

[0089] 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ある。本発明は、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

[0090] UE…移動局

eNB…無線基地局 eNB

MME…移動管理ノード

11、21…管理部

12a…PDCPレイヤ機能部

1 2 b...R L C レイヤ機能部

1 3、2 4...送信部

1 4、2 2...受信部

1 5、2 4...更新部

請求の範囲

- [請求項1] 第1移動局と第2移動局との間で、無線基地局との間で設定されている無線基地局インタフェースを介することなく、該第1移動局と該第2移動局との間で設定されている移動局間インタフェースを介して、データ信号の送受信を行う移動通信方法であって、
- 前記第1移動局又は前記第2移動局が、前記無線基地局に対して、前記移動局間インタフェースを介して送受信するデータ信号のシーケンス番号が一巡するタイミングが近づいていることを示す指示信号又は鍵の更新を要求する鍵更新要求信号を送信する工程と、
- 前記無線基地局又は移動管理ノードが、前記指示信号又は前記鍵更新要求信号を受信した場合、前記移動局間インタフェースを介したデータ信号の送受信に用いる移動局間通信用鍵又は該移動局間通信用鍵を算出するための所定パラメータを更新する工程と、
- 前記無線基地局又は移動管理ノードが、前記第1移動局及び前記第2移動局に対して、更新した前記移動局間通信用鍵又は前記所定パラメータを通知する工程と、
- 前記第1移動局及び前記第2移動局が、前記移動局間インタフェースを介したデータ信号の送受信に用いる移動局間通信用鍵を、通知された前記移動局間通信用鍵又は前記所定パラメータに基づいて算出した移動局間通信用鍵に更新する工程とを有することを特徴とする移動通信方法。
- [請求項2] 前記第1移動局と前記第2移動局との間で、前記無線基地局インタフェースを介することなく、前記移動局間インタフェースを介して、PDCPステータスレポートの送受信を行う工程を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。
- [請求項3] 前記PDCPステータスレポートの送受信は、更新された前記移動局間通信用鍵又は前記所定パラメータが受信された際に行われることを特徴とする請求項2に記載の移動通信方法。

[請求項4] 前記第1移動局及び前記第2移動局が、前記移動局間インタフェースを介したデータ信号の送受信に用いる移動局間通信用鍵を、通知された前記移動局間通信用鍵又は前記所定パラメータに基づいて算出した前記移動局間通信用鍵に更新した場合に、前記無線基地局又は前記移動管理ノードに対して、その旨を示す応答信号を送信する工程を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。

[請求項5] 前記無線基地局又は前記移動管理ノードは、前記第1移動局及び前記第2移動局に対して前記移動局間通信用鍵又は前記所定パラメータを通知してから前記応答信号を受信するまでの間、新たな移動局間インタフェースの割当を停止することを特徴とする請求項4に記載の移動通信方法。

[請求項6] 前記第1移動局及び前記第2移動局は、前記移動局間インタフェースを介したデータ信号の送受信に用いる移動局間通信用鍵を更新する際に、該移動局間インタフェースにおけるRLCレイヤ以下のプロトコルエンティティをリセットすることを特徴とする請求項1に記載の移動通信方法。

[請求項7] 第1移動局と第2移動局との間で、無線基地局との間で設定されている無線基地局インタフェースを介することなく、該第1移動局と該第2移動局との間で設定されている移動局間インタフェースを介して、データ信号の送受信を行うことができるように構成されている移動通信システムで用いられる無線基地局であって、

前記第1移動局又は前記第2移動局から、前記移動局間インタフェースを介して送受信するデータ信号のシーケンス番号が一巡するタイミングが近づいていることを示す指示信号又は鍵の更新を要求する鍵更新要求信号を受信するように構成されている受信部と、

前記指示信号又は前記鍵更新要求信号を受信した場合、前記移動局間インタフェースを介したデータ信号の送受信に用いる移動局間通信用鍵又は該移動局間通信用鍵を算出するための所定パラメータを更新

するように構成されている更新部と、

前記第 1 移動局及び前記第 2 移動局に対して、更新した前記移動局間通信用鍵又は前記所定パラメータを通知するように構成されている送信部とを具備することを特徴とする無線基地局。

[請求項8]

前記第 1 移動局及び前記第 2 移動局に対して前記移動局間通信用鍵又は前記所定パラメータを通知してから、該第 1 移動局及び該第 2 移動局から該移動局間通信用鍵の更新が完了した旨を示す応答信号を受信するまでの間、新たな移動局間インタフェースの割当を停止するように構成されていることを特徴とする請求項 7 に記載の無線基地局。

[請求項9]

第 1 移動局と第 2 移動局との間で、無線基地局との間で設定されている無線基地局インタフェースを介することなく、該第 1 移動局と該第 2 移動局との間で設定されている移動局間インタフェースを介して、データ信号の送受信を行うことができるように構成されている移動通信システムで用いられる移動管理ノードであって、

前記第 1 移動局又は前記第 2 移動局から、前記移動局間インタフェースを介して送受信するデータ信号のシーケンス番号が一巡するタイミングが近づいていることを示す指示信号又は鍵の更新を要求する鍵更新要求信号を受信するように構成されている受信部と、

前記指示信号又は前記鍵更新要求信号を受信した場合、前記移動局間インタフェースを介したデータ信号の送受信に用いる移動局間通信用鍵又は該移動局間通信用鍵を算出するための所定パラメータを更新するように構成されている更新部と、

前記第 1 移動局及び前記第 2 移動局に対して、更新した前記移動局間通信用鍵又は前記所定パラメータを通知するように構成されている送信部とを具備することを特徴とする移動管理ノード。

[請求項10]

前記第 1 移動局及び前記第 2 移動局に対して前記移動局間通信用鍵又は前記所定パラメータを通知してから、該第 1 移動局及び該第 2 移動局から該移動局間通信用鍵の更新が完了した旨を示す応答信号を受

信するまでの間、新たな移動局間インタフェースの割当を停止するように構成されていることを特徴とする請求項 9 に記載の移動管理ノード。

[請求項11]

第 1 移動局と第 2 移動局との間で、無線基地局との間で設定されている無線基地局インタフェースを介することなく、該第 1 移動局と該第 2 移動局との間で設定されている移動局間インタフェースを介して、データ信号の送受信を行うことができるように構成されている移動通信システムにおいて該第 1 移動局として機能する移動局であって、

前記無線基地局に対して、前記移動局間インタフェースを介して送受信するデータ信号のシーケンス番号が一巡するタイミングが近づいていることを示す指示信号又は鍵の更新を要求する鍵更新要求信号を送信するように構成されている送信部と、

前記指示信号又は前記鍵更新要求信号を受信した前記無線基地局又は移動管理ノードから、前記移動局間インタフェースを介したデータ信号の送受信に用いる移動局間通信用鍵又は該移動局間通信用鍵を算出するための所定パラメータを受信するように構成されている受信部と、

前記移動局間インタフェースを介したデータ信号の送受信に用いる移動局間通信用鍵を、受信した前記移動局間通信用鍵又は前記所定パラメータに基づいて算出した移動局間通信用鍵に更新するように構成されている更新部とを具備することを特徴とする移動局。

[請求項12]

前記送信部及び前記受信部は、前記第 2 移動局との間で、前記無線基地局インタフェースを介することなく、前記移動局間インタフェースを介して、PDCP ステータスレポートの送受信を行うように構成されていることを特徴とする請求項 11 に記載の移動局。

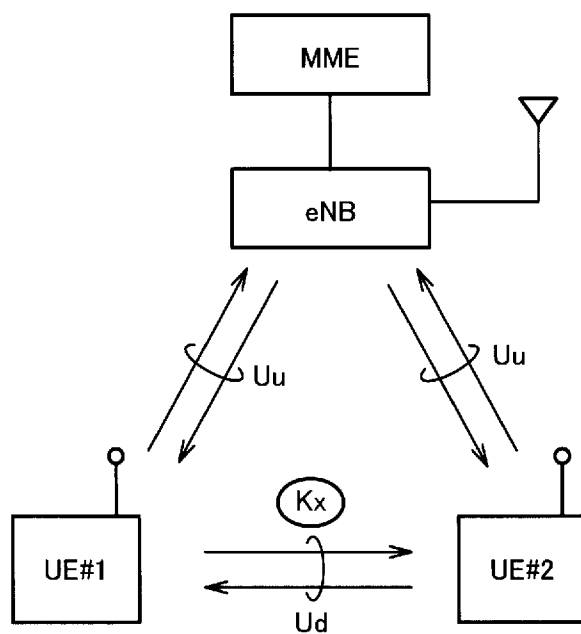
[請求項13]

前記送信部及び前記受信部は、更新された前記移動局間通信用鍵又は前記所定パラメータが受信された際に、前記 PDCP ステータスレポートの送受信を行うように構成されていることを特徴とする請求項

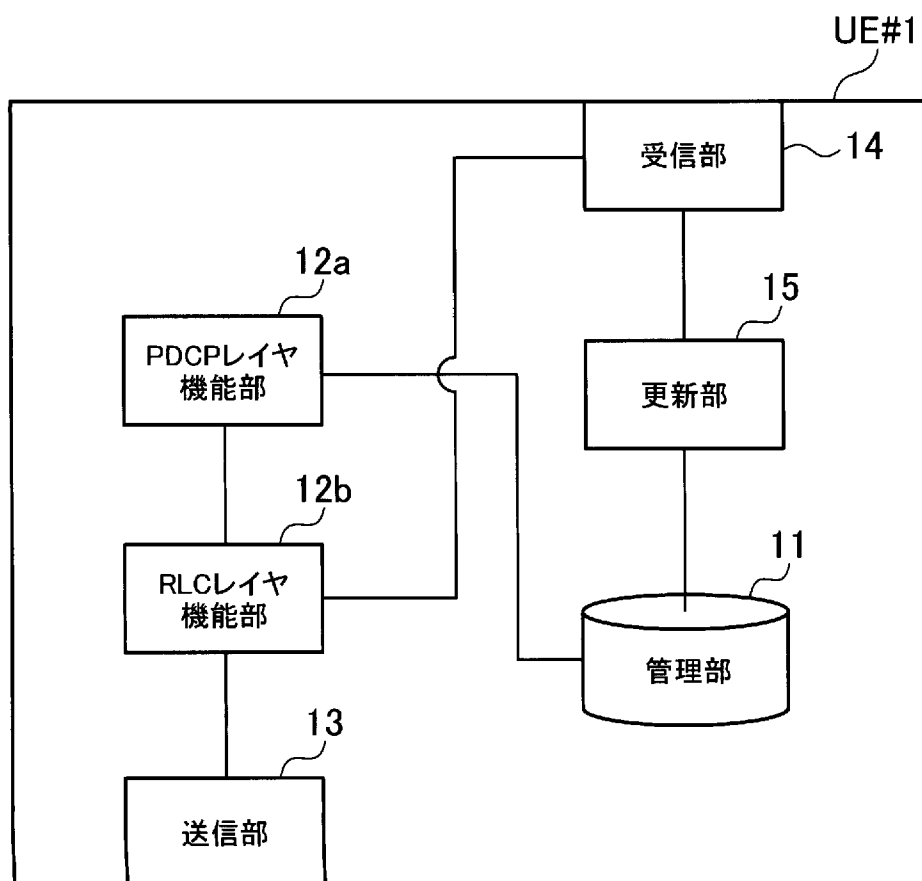
1 2 に記載の移動局。

[請求項14] 前記更新部は、前記移動局間インタフェースを介したデータ信号の送受信に用いる移動局間通信用鍵を更新する際に、該移動局間インタフェースにおける R L C レイヤ以下のプロトコルエンティティをリセットするように構成されていることを特徴とする請求項 1 1 に記載の移動局。

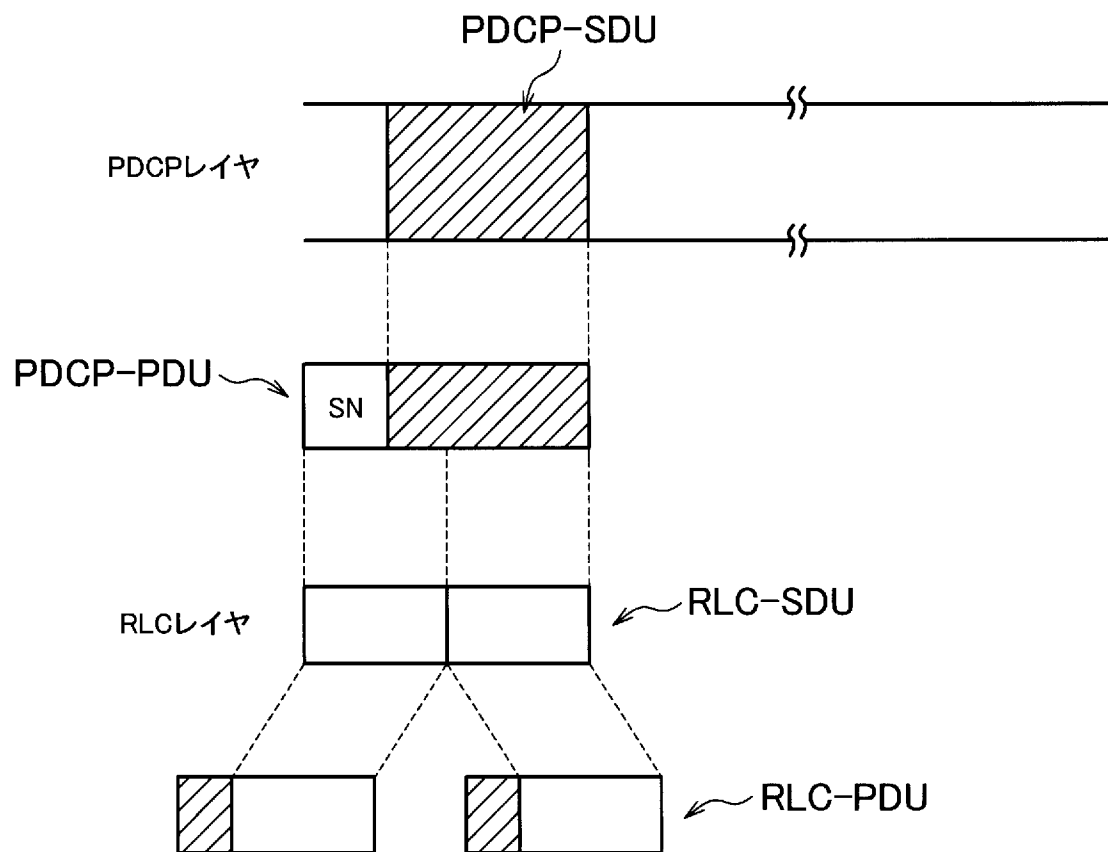
[図1]



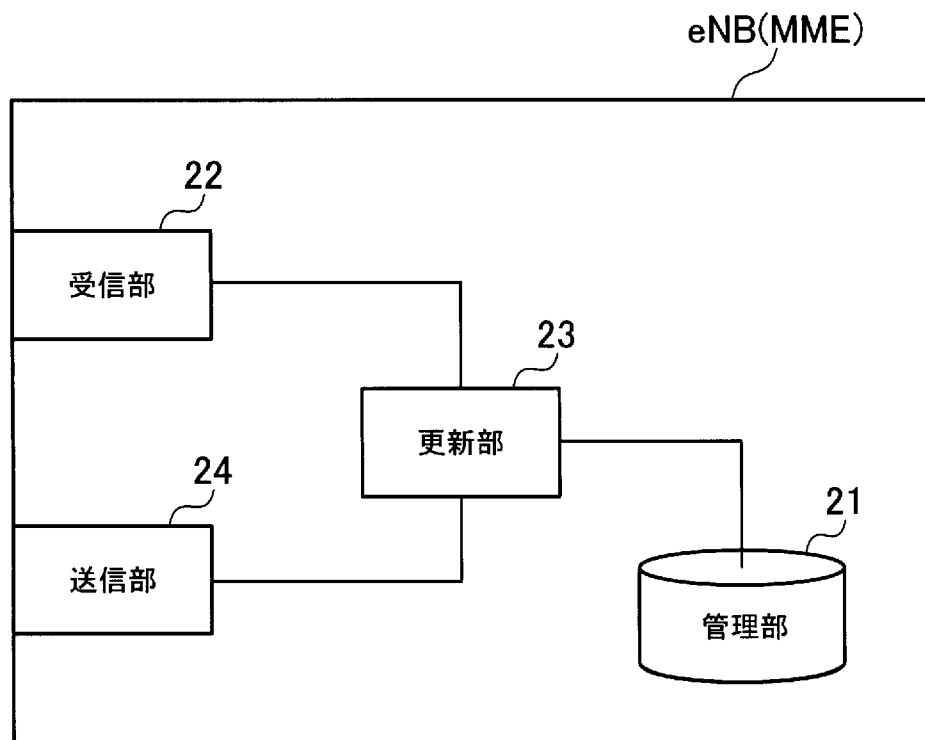
[図2]



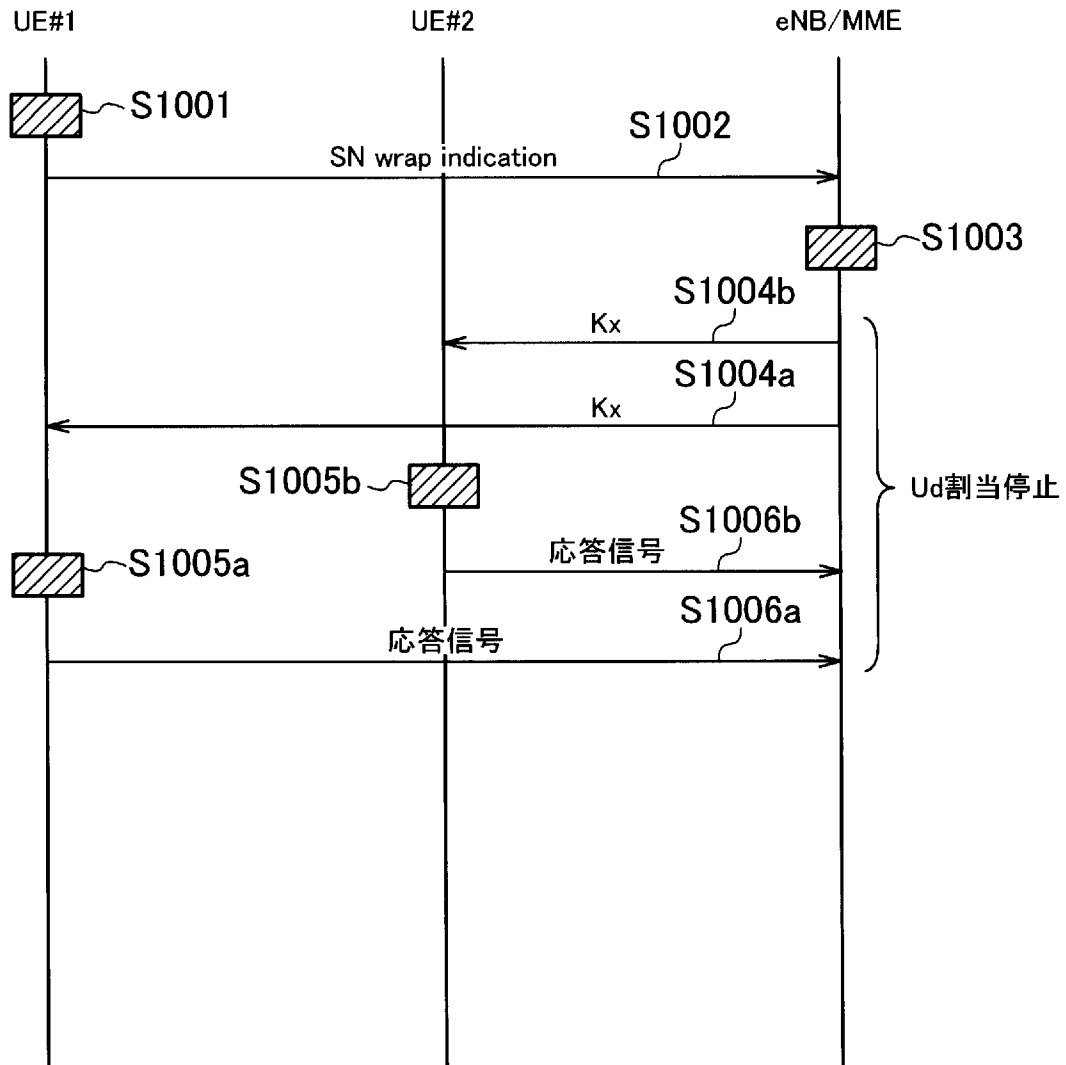
[図3]



[図4]



[図5]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2012/058606

A. CLASSIFICATION OF SUBJECT MATTER

H04W12/04 (2009.01) i, H04W92/18 (2009.01) i

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)

H04B7/24-7/26, H04W4/00-99/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2012
Kokai Jitsuyo Shinan Koho	1971-2012	Toroku Jitsuyo Shinan Koho	1994-2012

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2004-72565 A (TDK Corp.), 04 March 2004 (04.03.2004), paragraphs [0003] to [0005], [0018] to [0020] (Family: none)	1-14
Y	JP 2007-165977 A (Seiko Epson Corp.), 28 June 2007 (28.06.2007), paragraphs [0005] to [0011], [0033], [0035], [0036] (Family: none)	1-14
Y	JP 2003-283481 A (Canon Inc.), 03 October 2003 (03.10.2003), paragraph [0020] (Family: none)	1-14



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search
23 April, 2012 (23.04.12)

Date of mailing of the international search report
01 May, 2012 (01.05.12)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

A. 発明の属する分野の分類（国際特許分類（I P C））
Int.Cl. H04W12/04(2009.01)i, H04W92/18(2009.01)i

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（I P C））

Int.Cl. H04B7/24-7/26, H04W4/00-99/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1 9 2 2 - 1 9 9 6 年
日本国公開実用新案公報	1 9 7 1 - 2 0 1 2 年
日本国実用新案登録公報	1 9 9 6 - 2 0 1 2 年
日本国登録実用新案公報	1 9 9 4 - 2 0 1 2 年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
Y	JP 2004-72565 A (T D K株式会社) 2004. 03. 04, 段落 3-5, 18-20, (ファミリーなし)	1-14
Y	JP 2007-165977 A (セイコーエプソン株式会社) 2007. 06. 28, 段落 5-11, 33, 35, 36 (ファミリーなし)	1-14
Y	JP 2003-283481 A (キヤノン株式会社) 2003. 10. 03, 段落 20 (ファミリーなし)	1-14

☐ C 欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日

2 3 . 0 4 . 2 0 1 2

国際調査報告の発送日

0 1 . 0 5 . 2 0 1 2

国際調査機関の名称及びあて先

日本国特許庁 (I S A / J P)

郵便番号 1 0 0 - 8 9 1 5

東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員）

中村 信也

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 3 4

5 J

4 0 5 8