

(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
2010 年 4 月 29 日(29.04.2010)

PCT

(10) 国際公開番号
WO 2010/047367 A1

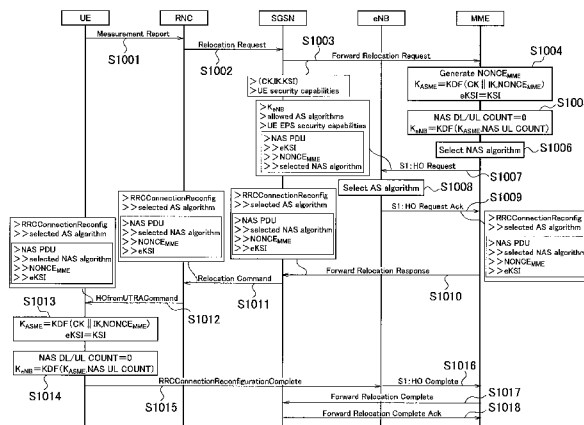
- (51) 国際特許分類:
H04W 12/08 (2009.01) H04W 88/06 (2009.01)
H04W 36/14 (2009.01)
- (21) 国際出願番号: PCT/JP2009/068176
- (22) 国際出願日: 2009 年 10 月 22 日(22.10.2009)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2008-272517 2008 年 10 月 22 日(22.10.2008) JP
- (71) 出願人 (米国を除く全ての指定国について): 株式会社エヌ・ティ・ティ・ドコモ(NTT DoCo-Mo, 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). 石井 美波 (ISHII, Minami). ツーゲンマイヤー アルフ (ZUGENMAIER, Alf).
- (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, 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, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (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, SE, SI, SK, SM, TR), OAPI (BF, BJ,

[続葉有]

(54) Title: MOBILE COMMUNICATION METHOD AND EXCHANGE

(54) 発明の名称: 移動通信方法及び交換局

[図5]



S1001 Measurement Report
S1002 Relocation Request
S1003 Forward Relocation Request
S1004 Generate NONCE_{MME}
K_{ASME}=KDF(CK||K, NONCE_{MME})
eKSI=KSI
S1006 Select NAS algorithm
S1007 S1:HO Request
S1008 Select AS algorithm
S1009 S1:HO Request Ack
S1010 Forward Relocation Response
S1011 Relocation Command
S1012 HOfromUTRACommand
S1015 RRCConnectionReconfigurationComplete
S1016 S1:HO Complete
S1017 Forward Relocation Complete
S1018 Forward Relocation Complete Ack

(57) Abstract: A procedure for performing an handover of a mobile station (UE) from a cell under control of a radio base station (NB) of UTRA system to a cell under control of a radio base station (eNB) of E-UTRA system comprises a step wherein an exchange (MME) of E-UTRA system receives, from the radio base station (eNB) of E-UTRA system, a handover request response message including a transparent container including a security processing algorithm of AS used in communication between the radio base station (eNB) of E-UTRA system and the mobile station (UE), and transmits, to an exchange (SGSN) of UTRA system, NAS PDU including the transparent container, a security processing algorithm of NAS and a security processing parameter of NAS.

(57) 要約: 移動局UEが、UTRA方式の無線基地局NB配下のセルからE-UTRA方式の無線基地局eNB配下のセルに対してハンドオーバーを行うための手順において、E-UTRA方式の交換局MMEが、E-UTRA方式の無線基地局eNBから、E-UTRA方式の無線基地局eNBと移動局UEとの間の通信で用いられるASのセキュリティ処理用アルゴリズムを含むトランスベアレントコンテナを含むハンドオーバー要求応答メッセージを受信し、UTRA方式の交換局SGSNに対して、トランスベアレントコンテナとNASのセキュリティ処理用アルゴリズムとNASのセキュリティ処理用パラメータを含むNAS PDUを送信する工程を有する。

WO 2010/047367 A1

CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, 添付公開書類:
TD, TG).

— 国際調査報告 (条約第 21 条(3))

明 細 書

発明の名称： 移動通信方法及び交換局

技術分野

[0001] 本発明は、移動通信方法及び交換局に関する。

背景技術

[0002] 現在、3GPPにおいて、UTRA (Universal Terrestrial Radio Access) 方式の無線アクセスネットワーク及びE-UTRA (Evolved Universal Terrestrial Radio Access) 方式の無線アクセスネットワークが混在する移動通信システムについての検討がなされている。

[0003] かかる移動通信システムにおいて、移動局UEが、UTRA方式の無線基地局配下のセルとE-UTRA方式の無線基地局配下のセルとの間でハンドオーバーを行うことが想定されている。

発明の概要

発明が解決しようとする課題

[0004] ここで、移動局UEは、UTRA方式の無線基地局配下のセル内で行う通信と、E-UTRA方式の無線基地局配下のセル内で行う通信とで、異なるセキュリティ処理を行うように構成されている。

[0005] しかしながら、上述の移動通信システムでは、移動局UEが、UTRA方式の無線基地局配下のセルとE-UTRA方式の無線基地局配下のセルとの間でハンドオーバーを行う場合に、どのようにして、ハンドオーバー前の通信で用いられていたセキュリティ処理に係る情報をハンドオーバー後の通信に引き継ぐべきかについて明確に規定されていないという問題点があった。

[0006] 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、移動局が、第1無線アクセス方式の無線基地局配下の第1セルから第2無線アクセス方式の無線基地局配下の第2セルに対してハンドオーバーを行うための手順において、適切に、セキュリティ処理に係る情報を、ハンドオーバー前の通信から

ハンドオーバー後の通信に引き継ぐことができる移動通信方法及び交換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

[0007] 本発明の第1の特徴は、移動通信方法であって、移動局が、第1無線アクセス方式の無線基地局配下の第1セルから第2無線アクセス方式の無線基地局配下の第2セルに対してハンドオーバーを行うための手順において、前記第2無線アクセス方式の交換局が、前記移動局との間の通信で用いる第1プロトコルのセキュリティ処理用アルゴリズムを選択する工程Aと、前記第2無線アクセス方式の交換局が、前記第1プロトコルのセキュリティ処理用パラメータを生成する工程Bと、前記第2無線アクセス方式の交換局が、該第2無線アクセス方式の無線基地局から、該第2無線アクセス方式の無線基地局と前記移動局との間の通信で用いられる第2プロトコルのセキュリティ処理用アルゴリズムを含むトランスペアレントコンテナを含むハンドオーバー要求応答メッセージを受信する工程Cと、前記第2無線アクセス方式の交換局が、前記第1無線アクセス方式の交換局に対して、前記トランスペアレントコンテナと前記第1プロトコルのセキュリティ処理用アルゴリズムと該第1プロトコルのセキュリティ処理用パラメータとを含む第1メッセージを送信する工程Dと、前記移動局が、前記第1セルにおいて、前記トランスペアレントコンテナと前記第1プロトコルのセキュリティ処理用アルゴリズムと該第1プロトコルのセキュリティ処理用パラメータとを受信する工程Eと、前記移動局が、前記第1プロトコルのセキュリティ処理用アルゴリズム及び該第1プロトコルのセキュリティ処理用パラメータを用いて、前記第2プロトコルのセキュリティ処理用パラメータを算出する工程Fと、前記移動局が、前記第2セルにおいて、前記第1プロトコルのセキュリティ処理用アルゴリズム及び該第1プロトコルのセキュリティ処理用パラメータを用いて、該第1プロトコルを用いた通信におけるセキュリティ処理を行う工程Gと、前記移動局が、前記第2セルにおいて、前記第2プロトコルのセキュリティ処理用アルゴリズム及び該第2プロトコルのセキュリティ処理用パラメータを用い

て、該第2プロトコルを用いた通信におけるセキュリティ処理を行う工程Hとを有することを要旨とする。

[0008] 本発明の第1の特徴において、前記工程Dにおいて、前記第1プロトコルのセキュリティ処理用アルゴリズム及び該第1プロトコルのセキュリティ処理用パラメータを含む第1プロトコル用メッセージが、前記トランスペアレントコンテナ内に含まれて送信されてもよい。

[0009] 本発明の第1の特徴において、前記工程Dにおいて、前記第2無線アクセス方式の交換局は、前記第1無線アクセス方式の交換局に対して、前記第1プロトコルのセキュリティ処理用アルゴリズム及び該第1プロトコルのセキュリティ処理用パラメータを含む第1プロトコル用メッセージを、前記トランスペアレントコンテナとは別に、前記第1メッセージ内に含めて送信してもよい。

[0010] 本発明の第1の特徴において、前記第1無線アクセス方式の交換局が、該第1無線アクセス方式の無線制御局に対して、受信した前記第1プロトコル用メッセージを、該第1無線アクセス方式の交換局と前記移動局との間の通信で用いられる第3プロトコル用メッセージに含めて送信する工程と、前記第1無線アクセス方式の無線制御局が、前記第1無線アクセス方式の交換局から受信した前記第3プロトコル用メッセージに含まれる前記第1プロトコル用メッセージに含まれる該第1プロトコルのセキュリティ処理用アルゴリズム及び該第1プロトコルのセキュリティ処理用パラメータを、該第1無線アクセス方式の無線制御局と前記移動局との間の通信で用いられる第4プロトコル用メッセージに含めて送信する工程とを更に有してもよい。

[0011] 本発明の第1の特徴において、前記工程Dにおいて、前記第2無線アクセス方式の交換局は、前記第1無線アクセス方式の交換局に対して、前記第1プロトコルのセキュリティ処理用アルゴリズム及び該第1プロトコルのセキュリティ処理用パラメータを、前記トランスペアレントコンテナとは別に、前記第1メッセージ内に含めて送信し、前記第1無線アクセス方式の交換局が、前記トランスペアレントコンテナとは別に、前記第1プロトコルのセキ

セキュリティ処理用アルゴリズム及び該第 1 プロトコルのセキュリティ処理用パラメータを含む第 1 プロトコル用メッセージを、該第 1 無線アクセス方式の交換局と前記移動局との間の通信で用いられる第 3 プロトコル用メッセージに含めて送信する工程を更に有してもよい。

[0012] 本発明の第 1 の特徴において、前記第 2 無線アクセス方式の交換局が、前記第 1 プロトコルのセキュリティ処理用アルゴリズム及び該第 1 プロトコルのセキュリティ処理用パラメータを用いたインテグリティプロテクション処理を行うことによって、前記第 1 プロトコル用メッセージを生成する工程と、前記移動局が、受信した前記第 1 プロトコルのセキュリティ処理用アルゴリズムと該第 1 プロトコルのセキュリティ処理用パラメータを用いたインテグリティプロテクション処理を行うことによって、前記第 1 プロトコル用メッセージに対する改竄の有無を検査する工程と、前記移動局が、前記第 1 プロトコル用メッセージに対する改竄があると判断された場合、前記第 1 無線アクセス方式の無線制御局に対して、前記ハンドオーバー手順が失敗した旨を通知する工程とを更に有してもよい。

[0013] 本発明の第 2 の特徴は、移動局が、第 1 無線アクセス方式の無線基地局配下の第 1 セルから第 2 無線アクセス方式の無線基地局配下の第 2 セルに対してハンドオーバーを行うための手順を行うことができる該第 2 無線アクセス方式の交換局として機能することができる交換局であって、前記手順において、前記移動局との間の通信で用いる第 1 プロトコルのセキュリティ処理用アルゴリズムを選択するように構成されている選択部と、前記手順において、前記第 1 プロトコルのセキュリティ処理用パラメータを生成するように構成されている生成部と、前記手順において、前記第 2 無線アクセス方式の無線基地局から、該第 2 無線アクセス方式の無線基地局と前記移動局との間の通信で用いられる第 2 プロトコルのセキュリティ処理用アルゴリズムを含むトランスペアレントコンテナを含むハンドオーバー要求応答メッセージを受信するように構成されている受信部と、前記手順において、前記第 1 無線アクセス方式の交換局に対して、前記トランスペアレントコンテナと前記第 1 プロ

トコルのセキュリティ処理用アルゴリズムと該第 1 プロトコルのセキュリティ処理用パラメータとを含む第 1 メッセージを送信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。

発明の効果

- [0014] 以上説明したように、本発明によれば、移動局が、第 1 無線アクセス方式の無線基地局配下の第 1 セルから第 2 無線アクセス方式の無線基地局配下の第 2 セルに対してハンドオーバを行うための手順において、適切に、セキュリティ処理に係る情報を、ハンドオーバ前の通信からハンドオーバ後の通信に引き継ぐことができる移動通信方法及び交換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 の実施形態に係る交換局の機能ブロック図である。
- [図3] 図 3 は、本発明の第 1 の実施形態に係る無線基地局の機能ブロック図である。
- [図4] 図 4 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例 1 を示すシーケンス図である。
- [図6] 図 6 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例 2 を示すシーケンス図である。
- [図7] 図 7 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例 3 を示すシーケンス図である。
- [図8] 図 8 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例 4 を示すシーケンス図である。
- [図9] 図 9 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例 5 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の構成)

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の構成について説明する。

[0017] 図1に示すように、本実施形態に係る移動通信システムは、UTRA方式(第1無線アクセス方式)の交換局SGSNと、UTRA方式の無線制御局RNCと、UTRA方式の無線基地局NBと、E-UTRA方式(第2無線アクセス方式)の交換局MMEと、E-UTRA方式の無線基地局eNBとを具備している。

[0018] ここで、本実施形態に係る移動通信システムにおいて、E-UTRA方式の交換局MMEと移動局UEとの間の通信では「NAS (Non Access Stratum、第1プロトコル)」が用いられ、E-UTRA方式の無線基地局eNBと移動局UEとの間の通信では「AS (Access Stratum、第2プロトコル)」が用いられ、UTRA方式の交換局SGSNと移動局UEとの間の通信では「NAS (第3プロトコル)」が用いられ、UTRA方式の無線制御局RNCと移動局UEとの間の通信では「AS (第4プロトコル)」が用いられるものとする。

[0019] そして、E-UTRA方式の交換局MMEと移動局UEとの間で送受信されるNASメッセージ(第1プロトコル用メッセージ)を「NAS PDU (E-UTRA)」と表現し、E-UTRA方式の無線基地局eNBと移動局UEとの間で送受信されるASメッセージ(第2プロトコル用メッセージ)を「AS PDU (E-UTRA)」と表現し、UTRA方式の交換局SGSNと移動局UEとの間で送受信されるNASメッセージ(第3プロトコル用メッセージ)を「NAS PDU (UTRA)」と表現し、UTRA方式の無線制御局RNCと移動局UEとの間で送受信されるASメッセージ(第4プロトコル用メッセージ)を「AS PDU (UTRA)」と表現する。

[0020] 図2に示すように、E-UTRA方式の交換局MMEは、eNBインターフェイス11と、SGSNインターフェイス12と、HO Request生

成部13と、Forward Relocation Response生成部14とを具備している。

[0021] eNBインターフェイス11は、E-UTRA方式の無線基地局eNBとの間のインターフェイスである。

[0022] また、eNBインターフェイス11は、E-UTRA方式の無線基地局eNBとの間の通信を行うために、「S1-Appl i c a t i o n P r o t o c o l」を終端する。

[0023] 例えば、eNBインターフェイス11は、移動局UEが、UTRA方式の無線基地局NB配下の第1セルからE-UTRA方式の無線基地局eNB配下の第2セルに対してハンドオーバを行うための手順において、E-UTRA方式の無線基地局eNBに対して、「HO R e q u e s t (S1メッセージ)」を送信したり、E-UTRA方式の無線基地局eNBから、「HO R e q u e s t A c k (S1メッセージ)」を受信したりするように構成されている。

[0024] ここで、「HO R e q u e s t A c k (S1メッセージ)」は、E-UTRA方式のASのセキュリティ処理用アルゴリズムを含むトランスペアレントコンテナ「RRCC o n n e c t i o n R e c o n f i g」を含むハンドオーバ要求応答メッセージである。

[0025] 例えば、かかるASのセキュリティ処理には、サイファリング(C i p h e r i n g)処理及びインテグリティプロテクション(I n t e g r i t y P r o t e c t i o n)処理が含まれる。

[0026] かかるASのサイファリング処理は、発側において、セキュリティ処理用パラメータを用いてASメッセージを暗号化し、着側において、セキュリティ処理用パラメータを用いてASメッセージを復号する処理である。

[0027] また、かかるASのインテグリティプロテクション処理は、送信側において、ASメッセージ及びセキュリティ処理用パラメータを用いてMAC(M e s s a g e A u t h e n t i c a t i o n C o d e、例えば、32ビット長)を算出してASメッセージに付与し、受信側において、ASメッセ

ージとセキュリティ処理用パラメータとMACとを用いてASメッセージにおける改竄の有無を検査する処理である。

[0028] また、例えば、かかるASのサイファリング処理用アルゴリズムとしては、「NULL」や「AES」や「Snow 3G」等が想定され、かかるASのインテグリティプロテクション処理用アルゴリズムとしては、「AES」や「Snow 3G」等が想定される。

[0029] SGSNインターフェイス12は、UTRA方式の交換局SGSNとの間のインターフェイスである。

[0030] 例えば、SGSNインターフェイス12は、移動局UEが、UTRA方式の無線基地局NB配下の第1セルからE-UTRA方式の無線基地局eNB配下の第2セルに対してハンドオーバを行うための手順において、UTRA方式の交換局SGSNに対して、「Forward Relocation Response（第1メッセージ）」を送信したり、UTRA方式の交換局SGSNから、「Forward Relocation Request」を受信したりするように構成されている。

[0031] HO Request生成部13は、上述の「HO Request（S1メッセージ）」を生成するように構成されている。

[0032] 具体的には、HO Request生成部13は、上述の「HO Request（S1メッセージ）」を生成する際に、E-UTRA方式のNASのセキュリティ処理用アルゴリズムを選択し、NASのセキュリティ処理用パラメータを生成するように構成されている。

[0033] ここで、HO Request生成部13は、「Forward Relocation Request」に含まれる「UE security capabilities（移動局UEのセキュリティ処理能力）」に応じて、E-UTRA方式のNASのセキュリティ処理用アルゴリズムを選択してもよい。

[0034] 例えば、かかるNASのセキュリティ処理には、サイファリング処理及びインテグリティプロテクション処理が含まれる。

- [0035] かかるNASのサイファリング処理は、発側において、セキュリティ処理用パラメータを用いてNASメッセージを暗号化し、着側において、セキュリティ処理用パラメータを用いてNASメッセージを復号する処理である。
- [0036] また、かかるNASのインテグリティプロテクション処理は、送信側において、NASメッセージ及びセキュリティ処理用パラメータを用いてMAC（例えば32ビット長）を算出してNASメッセージに付与し、受信側において、NASメッセージとセキュリティ処理用パラメータとMACとを用いてNASメッセージにおける改竄の有無を検査する処理である。
- [0037] また、例えば、かかるNASのサイファリング処理用アルゴリズムとしては、「NULL」や「AES」や「Snow3G」等が想定され、かかるNASのインテグリティプロテクション処理用アルゴリズムとしては、「AES」や「Snow3G」等が想定される。
- [0038] さらに、かかるNASのセキュリティ処理用パラメータとしては、「eKSI」や「NONCE_{MME}」等が想定される。
- [0039] Forward Relocation Response生成部14は、上述の「Forward Relocation Response」を生成するように構成されている。
- [0040] 具体的には、Forward Relocation Response生成部14は、トランスペアレントコンテナ「RRCCOnnection Reconfig」と、E-UTRA方式のNASのセキュリティ処理用アルゴリズムと、E-UTRA方式のNASのセキュリティ処理用パラメータとを含む「Forward Relocation Response」を生成するように構成されている。
- [0041] なお、Forward Relocation Response生成部14は、E-UTRA方式のNASのセキュリティ処理用アルゴリズム及びE-UTRA方式のNASのセキュリティ処理用パラメータを含む「NAS PDU（E-UTRA方式）」が、トランスペアレントコンテナ「RRCCOnnectionReconfig」内に含まれた状態の「Forward

Relocation Response」を送信するように構成されていてもよい（後述の図5参照）。

[0042] ここで、E-UTRA方式の無線基地局eNBが、かかる「NAS PDU（E-UTRA方式）」を、トランスペアレントコンテナ「RRCConnectionReconfig」に含めるように構成されている。

[0043] また、Forward Relocation Response生成部14は、E-UTRA方式のNASのセキュリティ処理用アルゴリズム及びE-UTRA方式のNASのセキュリティ処理用パラメータを含む「NAS PDU（E-UTRA方式）」を、トランスペアレントコンテナ「RRCConnectionReconfig」とは別に、「Forward Relocation Response」内に含めるように構成されていてもよい（後述の図6及び図7参照）。

[0044] ここで、Forward Relocation Response生成部14は、かかる「NAS PDU（E-UTRA方式）」に対して、E-UTRA方式のNASのセキュリティ処理用アルゴリズム及びE-UTRA方式のNASのセキュリティ処理用パラメータを用いた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。

[0045] また、Forward Relocation Response生成部14は、E-UTRA方式のNASのセキュリティ処理用アルゴリズム及びE-UTRA方式のNASのセキュリティ処理用パラメータを、トランスペアレントコンテナ「RRCConnectionReconfig」とは別に、「Forward Relocation Response」内に、SGSNインターフェイス12上に見える情報要素として含めるように構成されていてもよい（後述の図8参照）。

[0046] 図3に示すように、E-UTRA方式の無線基地局eNBは、MMEインターフェイス21と、HO Request Ack生成部22とを具備している。

[0047] MMEインターフェイス21は、E-UTRA方式の交換局MMEとの間の

インターフェイスである。

- [0048] また、MMEインターフェイス21は、E-UTRA方式の交換局MMEとの間の通信を行うために、「S1-Application Protocol」を終端する。
- [0049] 例えば、MMEインターフェイス21は、移動局UEが、UTRA方式の無線基地局NB配下の第1セルからE-UTRA方式の無線基地局eNB配下の第2セルに対してハンドオーバを行うための手順において、E-UTRA方式の交換局MMEに対して、「HO Request Ack (S1メッセージ)」を送信したり、E-UTRA方式の交換局MMEから、「HO Request (S1メッセージ)」を受信したりするように構成されている。
- [0050] HO Request Ack生成部22は、上述の「HO Request Ack (S1メッセージ)」を生成するように構成されている。
- [0051] 具体的には、HO Request Ack生成部22は、上述の「HO Request Ack (S1メッセージ)」を生成する際に、E-UTRA方式のASのセキュリティ処理用アルゴリズムを選択し、E-UTRA方式のASのセキュリティ処理用パラメータを生成するように構成されている。
- [0052] ここで、HO Request Ack生成部22は、「HO Request (S1メッセージ)」に含まれる「UE EPS security capabilities (移動局UEのセキュリティ処理能力)」に応じて、E-UTRA方式のASのセキュリティ処理用アルゴリズムを選択してもよい。
- [0053] また、HO Request Ack生成部22は、「HO Request (S1メッセージ)」に含まれている「allowed AS algorithms」によって特定されるE-UTRA方式のASのセキュリティ処理用アルゴリズムの中から、E-UTRA方式のASのセキュリティ処理用アルゴリズムを選択してもよい。
- [0054] 図4に示すように、移動局UEは、ハンドオーバ処理部31と、NAS PDU解析部32とを具備している。

- [0055] ハンドオーバ処理部 31 は、移動局 UE が、UTRA 方式の無線基地局 NB 配下の第 1 セルから E-UTRA 方式の無線基地局 eNB 配下の第 2 セルに対してハンドオーバを行うための手順において要求されている処理を行うように構成されている。
- [0056] 例えば、ハンドオーバ処理部 31 は、E-UTRA 方式の NAS のセキュリティ処理用アルゴリズム及び E-UTRA 方式の NAS のセキュリティ処理用パラメータを用いて、E-UTRA 方式の AS のセキュリティ処理用パラメータを算出するように構成されている。
- [0057] また、ハンドオーバ処理部 31 は、ハンドオーバ先のセルにおいて、E-UTRA 方式の NAS のセキュリティ処理用アルゴリズム及び E-UTRA 方式の NAS のセキュリティ処理用パラメータを用いて、E-UTRA 方式の NAS を用いた通信におけるセキュリティ処理を行い、E-UTRA 方式の AS のセキュリティ処理用アルゴリズム及び E-UTRA 方式の AS のセキュリティ処理用パラメータを用いて、E-UTRA 方式の AS を用いた通信におけるセキュリティ処理を行うように構成されている。
- [0058] NAS PDU 解析部 32 は、受信した E-UTRA 方式の NAS のセキュリティ処理用アルゴリズムと E-UTRA 方式の NAS のセキュリティ処理用パラメータを用いたインテグリティプロテクション処理を行うことによって、受信した「NAS PDU (E-UTRA 方式)」に対する改竄の有無を検査するように構成されている。
- [0059] ここで、NAS PDU 解析部 32 が、「NAS PDU (E-UTRA 方式)」に対する改竄があると判断された場合、ハンドオーバ処理部 31 が、ハンドオーバ元の無線アクセス装置（例えば、無線制御局 RNC 又は交換局 SGSN）に対して、上述のハンドオーバ手順が失敗した旨を通知するように構成されている。
- [0060] （本発明の第 1 実施形態に係る移動通信システムの動作）
- 図 5 乃至図 9 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の動作例 1 乃至 4 について説明する。具体的には、移動局 UE が、UTR

A方式の無線基地局NB配下の第1セルからE-UTRA方式の無線基地局eNB配下の第2セルに対してハンドオーバーを行うための手順について説明する。

- [0061] 第1に、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の動作例1について説明する。
- [0062] 図5に示すように、ステップS1001において、UTRA方式の無線基地局NB配下の第1セルにおいて通信中の移動局UEが、UTRA方式の無線制御局RNCに対して、「Measurement Report」を送信する。
- [0063] ステップS1002において、UTRA方式の無線制御局RNCが、UTRA方式の交換局SGSNに対して、「Relocation Request」を送信する。
- [0064] ステップS1003において、UTRA方式の交換局SGSNが、E-UTRA方式の交換局MMEに対して、「Forward Relocation Request」を送信する。
- [0065] ここで、「Forward Relocation Request」には、UTRA方式のNASのセキュリティ処理用パラメータである「CK」や「IK」や「KSI」や、移動局UEのセキュリティ処理能力を示す「UE security capabilities」が含まれている。
- [0066] かかる「UE security capabilities」には、E-UTRA方式における移動局UEのセキュリティ処理能力を示す「UE EPS security capabilities」が含まれる。
- [0067] また、かかる「UE security capabilities」には、UTRA方式や、他の無線アクセス方式における移動局UEのセキュリティ処理能力を示す情報要素が含まれてもよい。
- [0068] ステップS1004において、E-UTRA方式の交換局MMEが、「NONCE_{MME}」を生成する。ここで、「NONCE_{MME}」は、32ビット長のランダムに選択されるビットストリングである。

[0069] また、E-UTRA方式の交換局MMEが、(式1)によって、「 K_{ASME} 」を生成する。

[0070] $K_{ASME} = KDF(CK || IK, NONCE_{MME}) \dots$ (式1)

また、E-UTRA方式の交換局MMEが、(式2)によって、「 $eKSI$ 」を生成する。

[0071] $eKSI = KSI \dots$ (式2)

ステップS1005において、E-UTRA方式の交換局MMEが、「NAS DL COUNT」及び「NAS UL COUNT」を「0」とした後、(式3)によって、「 K_{eNB} 」を生成する。ここで、「NAS DL COUNT」は、下りリンクにおけるE-UTRA方式のNASメッセージのシーケンス番号であり、「NAS UL COUNT」は、上りリンクにおけるE-UTRA方式のNASメッセージのシーケンス番号である。

[0072] $K_{eNB} = KDF(K_{ASME}, NAS\ UL\ COUNT) \dots$ (式3)

ステップS1006において、E-UTRA方式の交換局MMEが、「UE EPS security capabilities」に応じて、E-UTRA方式のNASのセキュリティ処理用アルゴリズムを選択する。

[0073] ステップS1007において、E-UTRA方式の交換局MMEが、E-UTRA方式の無線基地局eNBに対して、「HO Request (S1メッセージ)」を送信する。

[0074] ここで、「HO Request (S1メッセージ)」には、「 K_{eNB} 」や「allowed AS algorithms」や「UE EPS security capabilities」が含まれている。なお、「HO Request (S1メッセージ)」には、「allowed AS algorithms」が含まれていなくてもよい。

[0075] また、「HO Request (S1メッセージ)」には、トランスポートコンテナとして、「 $eKSI$ 」や「 $NONCE_{MME}$ 」や「selected NAS algorithm」を含む「NAS PDU (E-UTRA方式)」が含まれている。ここで、「selected NAS algo

「*algorithm*」は、ステップS1006において選択されたE-UTRA方式のNASのセキュリティ処理用アルゴリズムを示す。

[0076] ステップS1008において、E-UTRA方式の無線基地局eNBが、「*UE EPS security capabilities*」に基づいて、「*allowed AS algorithms*」によって指定されているE-UTRA方式のASのセキュリティ処理用アルゴリズムの中から、1つのE-UTRA方式のASのセキュリティ処理用アルゴリズムを選択する。

[0077] 具体的には、E-UTRA方式のASのサイファリング処理用アルゴリズム及びE-UTRA方式のASのインテグリティプロテクション処理用アルゴリズムが、それぞれ選択される。

[0078] ステップS1009において、E-UTRA方式の無線基地局eNBが、E-UTRA方式の交換局MMEに対して、「*HO Request Ack (S1メッセージ)*」を送信する。

[0079] 「*HO Request Ack (S1メッセージ)*」には、トランスペアレントコンテナ「*RRCCConnectionReconfig*」が含まれており、トランスペアレントコンテナ「*RRCCConnectionReconfig*」内には、「*selected AS algorithm*」と、「*eKSI*」や「*NONCE_{MME}*」や「*selected NAS algorithm*」を含む「*NAS PDU*」が含まれている。ここで、「*selected AS algorithm*」は、ステップS1008において選択されたE-UTRA方式のASのセキュリティ処理用アルゴリズムを示す。

[0080] ステップS1010において、E-UTRA方式の交換局MMEが、UTRA方式の交換局SGSNに対して、かかるトランスペアレントコンテナ「*RRCCConnectionReconfig*」を含む「*Forward Relocation Response*」を送信する。

[0081] ステップS1011において、UTRA方式の交換局SGSNが、UTRA方式の無線制御局RNCに対して、かかるトランスペアレントコンテナ「

RRCCo n n e c t i o n R e c o n f i g」を含む「R e l o c a t i o n C o m m a n d」を送信する。

[0082] ステップS1012において、UTRA方式の無線制御局RNCが、移動局UEに対して、かかるトランスペアレントコンテナ「RRCCo n n e c t i o n R e c o n f i g」を含む「H O f r o m U T R A C o m m a n d（ハンドオーバ指示メッセージ）」を送信する。

[0083] ステップS1013において、移動局UEが、受信した「H O f r o m U T R A C o m m a n d」に含まれる「NAS PDU（E-UTRA方式）」を抽出し、「NAS PDU（E-UTRA方式）」に含まれる「NONCE_{MME}」と、ハンドオーバ前の通信で用いている「CK」及び「IK」とを用いて、（式4）によって、「K_{ASME}」を生成する。

[0084] $K_{ASME} = KDF(CK || IK, NONCE_{MME}) \dots$ （式4）

また、移動局UEが、ハンドオーバ前の通信で用いている「KSI」を用いて、（式5）によって、「eKSI」を生成してもよい。

[0085] $eKSI = KSI \dots$ （式5）

ここで、移動局UEは、E-UTRA方式のNASのセキュリティ処理において、（式5）によって生成された「eKSI」の代わりに、受信した「H O f r o m U T R A C o m m a n d」内の「NAS PDU（E-UTRA方式）」に含まれる「eKSI」を用いてもよい。

[0086] ステップS1014において、移動局UEが、「NAS DL COUNT」及び「NAS UL COUNT」を「0」とした後、（式6）によって、「K_{eNB}」を生成する。

[0087] $K_{eNB} = KDF(K_{ASME}, NAS\ UL\ COUNT) \dots$ （式6）

ステップS1015において、移動局UEは、E-UTRA方式の無線基地局eNBに対して、「K_{eNB}」を用いたE-UTRA方式のASのセキュリティ処理を施した状態の「RRCCo n n e c t i o n R e c o n f i g u r a t i o n C o m p l e t e（E-UTRA方式のASメッセージ）」を送信する。

- [0088] ここで、移動局UEは、「 K_{ASME} 」及び「 $eKSI$ 」を用いて、E-UTRA方式のNASのセキュリティ処理用アルゴリズム（「AES」等）によって、「HO from UTRA Command」に含まれていた「NAS PDU（E-UTRA方式）」に対して、インテグリティプロテクション処理を行うことによって、「NAS PDU（E-UTRA方式）」に対する改竄の有無を検査し、「NAS PDU（E-UTRA方式）」に対する改竄があったと判断された場合には、UTRA方式の無線制御局RNC、又は、交換局SGSNに対して、かかるハンドオーバー手順が失敗したことを通知するUTRA方式のASメッセージ、又は、UTRA方式のNASメッセージを送信してもよい。
- [0089] ステップS1016において、E-UTRA方式の無線基地局eNBが、E-UTRA方式の交換局MMEに対して、「HO Complete（S1メッセージ）」を送信する。
- [0090] ステップS1017において、E-UTRA方式の交換局MMEが、UTRA方式の交換局SGSNに対して、「Forward Relocation Complete」を送信し、ステップS1018において、UTRA方式の交換局SGSNが、E-UTRA方式の交換局MMEに対して、「Forward Relocation Complete Ack」を送信する。
- [0091] 第2に、図6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の動作例2について説明する。
- [0092] 図6に示すように、ステップS2001乃至S2006の動作は、図5に示すステップS1001乃至S1006の動作と同一である。
- [0093] ステップS2007において、E-UTRA方式の交換局MMEが、E-UTRA方式の無線基地局eNBに対して、「HO Request（S1メッセージ）」を送信する。
- [0094] ここで、「HO Request（S1メッセージ）」には、「 K_{eNB} 」や「allowed AS algorithms」や「UE EPS se

curity capabilities」が含まれている。なお、「HO Request (S1メッセージ)」には、「allowed AS algorithms」が含まれていなくてもよい。

[0095] また、「HO Request (S1メッセージ)」には、トランスペアレントコンテナとして、図5に示す「eKSI」や「NONCE_{MME}」や「selected NAS algorithm」を含む「NAS PDU」が含まれていない。

[0096] ステップS2008において、E-UTRA方式の無線基地局eNBが、「UE EPS security capabilities」に基づいて、「allowed AS algorithms」によって指定されているE-UTRA方式のASのセキュリティ処理用アルゴリズムの中から、1つのE-UTRA方式のASのセキュリティ処理用アルゴリズムを選択する。

[0097] 具体的には、E-UTRA方式のASのサイファリング処理用アルゴリズム及びE-UTRA方式のASのインテグリティプロテクション処理用アルゴリズムが、それぞれ選択される。

[0098] ステップS2009において、E-UTRA方式の無線基地局eNBが、E-UTRA方式の交換局MMEに対して、「HO Request Ack (S1メッセージ)」を送信する。

[0099] 「HO Request Ack (S1メッセージ)」には、トランスペアレントコンテナ「RRCConnectionReconfig」が含まれている。また、トランスペアレントコンテナ「RRCConnectionReconfig」内には、「selected AS algorithm」のみが含まれており、図5に示すような「eKSI」や「NONCE_{MME}」や「selected NAS algorithm」を含む「NAS PDU (E-UTRA方式)」は含まれていない。

[0100] ステップS2010において、E-UTRA方式の交換局MMEが、UTRA方式の交換局SGSNに対して、かかるトランスペアレントコンテナ「RRCConnectionReconfig」を含む「Forward R

「Relocation Response」を送信する。

[0101] ここで、E-UTRA方式の交換局MMEは、「Forward Relocation Response」内に、トランスペアレントコンテナ「RRCConnectionReconfig」とは別に、図5に示すような「eKSI」や「NONCE_{MME}」や「selected NAS algorithm」を含む「NAS PDU (E-UTRA方式)」を含める。

[0102] ステップS2011において、UTRA方式の交換局SGSNが、UTRA方式の無線制御局RNCに対して、トランスペアレントコンテナ「RRCConnectionReconfig」及び「NAS PDU (UTRA方式)」を含む「Relocation Command」を送信する。

[0103] ここで、UTRA方式の交換局SGSNは、E-UTRA方式の交換局MMEから受信した「NAS PDU (E-UTRA方式)」を、「NAS PDU (UTRA方式)」に含めて送信する。

[0104] ステップS2012において、UTRA方式の無線制御局RNCが、移動局UEに対して、トランスペアレントコンテナ「RRCConnectionReconfig」及び「NAS PDU (UTRA方式)」を含む「HofromUTRACommand (ハンドオーバー指示メッセージ)」を送信する。

[0105] 以下、ステップS2013乃至S2018の動作は、図5に示すステップS1013乃至S1018の動作と同一である。

[0106] 第3に、図7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の動作例3について説明する。

[0107] 図7に示すように、ステップS3001乃至S2011の動作は、図6に示すステップS2001乃至S2011の動作と同一である。

[0108] ステップS3012Aにおいて、UTRA方式の無線制御局RNCが、UTRA方式の交換局SGSNから受信した「Relocation Command」に含まれる「NAS PDU (UTRA方式)」を含む「Direct Transfer (ASメッセージ)」を、トランスペアレントコ

ンテナ「RRCCo n n e c t i o n R e c o n f i g」とは別に、移動局UEに対して送信する。

- [0109] ステップS3012において、UTRA方式の無線制御局RNCが、移動局UEに対して、トランスペアレントコンテナ「RRCCo n n e c t i o n R e c o n f i g」を含み、「NAS PDU (UTRA方式)」や「NAS PDU (E-UTRA方式)」を含まない「HO f r o m U T R A C o m m a n d (ハンドオーバ指示メッセージ)」を送信する。
- [0110] ここで、移動局UEにおける「Direct Transfer」及び「HO f r o m U T R A C o m m a n d」の受信処理の順序が保障されるように、「Direct Transfer」及び「HO f r o m U T R A C o m m a n d」が順序保障される同一無線ベアラにて送信されてもよい。
- [0111] また、移動局UEが、「Direct Transfer」に対する応答信号(UTRA方式のASメッセージ)を送信し、UTRA方式の無線制御局RNCが、応答信号(UTRA方式のASメッセージ)を受信した後に、UTRA方式の無線制御局RNCが、「HO f r o m U T R A C o m m a n d」を送信するように構成されていてもよい。
- [0112] また、移動局UEが、「Direct Transfer」に含まれる「NAS PDU (UTRA方式)」に対する応答信号(UTRA方式のNASメッセージ)を送信し、UTRA方式の交換局SGSNが、応答信号(UTRA方式のNASメッセージ)を受信した後に、UTRA方式の交換局SGSNが、UTRA方式の無線制御局RNCに対して、かかる応答信号を受信した旨を通知し、UTRA方式の無線制御局RNCが、かかる通知を受信した後に、「HO f r o m U T R A C o m m a n d」を送信するように構成されていてもよい。
- [0113] 以下、ステップS3013乃至S3018の動作は、図5に示すステップS1013乃至S1018の動作と同一である。
- [0114] 第4に、図8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の動作例4について説明する。

- [0115] 図8に示すように、ステップS4001乃至S4009の動作は、図6に示すステップS3001乃至S3009の動作と同一である。
- [0116] ステップS4010において、E-UTRA方式の交換局MMEが、UTRA方式の交換局SGSNに対して、上述のトランスペアレントコンテナ「RRCConnectionReconfig」を含む「Forward Relocation Response」を送信する。
- [0117] ここで、E-UTRA方式の交換局MMEは、「Forward Relocation Response」内に、トランスペアレントコンテナ「RRCConnectionReconfig」とは別に、「eKSI」や「NONCE_{MME}」や「selected NAS algorithm」のそれぞれを、情報要素として含める。
- [0118] UTRA方式の交換局SGSNが、ステップS4011Aにおいて、「Forward Relocation Response」に含まれている「eKSI」や「NONCE_{MME}」や「selected NAS algorithm」を含む「NAS PDU (UTRA方式)」を生成して移動局UEに送信し、ステップS4011Bにおいて、かかる「NAS PDU (UTRA方式)」を受信した旨を示す「Ack」を移動局UEから受信する。
- [0119] ステップS4011において、UTRA方式の交換局SGSNが、UTRA方式の無線制御局RNCに対して、トランスペアレントコンテナ「RRCConnectionReconfig」を含み、上述の「eKSI」や「NONCE_{MME}」や「selected NAS algorithm」を含まない「Relocation Command」を送信する。
- [0120] ステップS4012において、UTRA方式の無線制御局RNCが、移動局UEに対して、トランスペアレントコンテナ「RRCConnectionReconfig」を含み、上述の「eKSI」や「NONCE_{MME}」や「selected NAS algorithm」を含まない「HO from UTRACommand (ハンドオーバー指示メッセージ)」を送信する。

[0121] 以下、ステップS4013乃至S4018の動作は、図5に示すステップS1013乃至S1018の動作と同一である。

[0122] 第5に、図9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の動作例5について説明する。

[0123] 図9に示すように、ステップS5001乃至S5006の動作は、図5に示すステップS1001乃至S1006の動作と同一である。

[0124] ステップS5007において、E-UTRA方式の交換局MMEが、E-UTRA方式の無線基地局eNBに対して、「HO Request (S1メッセージ)」を送信する。

[0125] ここで、「HO Request (S1メッセージ)」には、「K_{eNB}」や「allowed AS algorithms」や「UE EPS security capabilities」や「eKSI」や「NONCE_{MME}」や「selected NAS algorithm」が含まれている。なお、「HO Request (S1メッセージ)」には、「allowed AS algorithms」が含まれていなくてもよい。

[0126] ステップS5008において、E-UTRA方式の無線基地局eNBが、「UE EPS security capabilities」に基づいて、「allowed AS algorithms」によって指定されているE-UTRA方式のASのセキュリティ処理用アルゴリズムの中から、1つのE-UTRA方式のASのセキュリティ処理用アルゴリズムを選択する。

[0127] 具体的には、E-UTRA方式のASのサイファリング処理用アルゴリズム及びE-UTRA方式のASのインテグリティプロテクション処理用アルゴリズムが、それぞれ選択される。

[0128] ステップS5009において、E-UTRA方式の無線基地局eNBが、E-UTRA方式の交換局MMEに対して、「HO Request Ack (S1メッセージ)」を送信する。

[0129] 「HO Request Ack (S1メッセージ)」には、トランスポートコンテナ「RRCConnectionReconfig」が含ま

れており、トランスペアレントコンテナ「RRCConnectionReconfi g」内には、「selected AS algorithm」や「eKSI」や「NONCE_{MME}」や「selected NAS algorithm」が含まれている。

[0130] 以下、ステップS5010乃至S5018の動作は、図5に示すステップS1010乃至S1018の動作と同一である。

[0131] (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)

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、移動局UEが、UTRA方式の無線基地局NB配下のセルからE-UTRA方式の無線基地局eNB配下のセルに対してハンドオーバを行うための手順において、UTRA方式のNASのセキュリティ用パラメータやUTRA方式のASのセキュリティ用パラメータ等を、E-UTRA方式のNASのセキュリティ用パラメータやE-UTRA方式のASのセキュリティ用パラメータ等として、適切に引き継がせることができる。

[0132] また、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、図5乃至図8の例に示すように、E-UTRA方式のNASのセキュリティ処理用アルゴリズムを示す「selected NAS algorithm」や、E-UTRA方式のNASのセキュリティ処理用パラメータである「eKSI」や「NONCE_{MME}」が、E-UTRA方式のASメッセージである「RRCConnectionReconfi g」内に情報要素として直接含まれないように構成されているため、NASとASとの独立性を維持することができる。

[0133] また、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、「selected NAS algorithm」や「eKSI」や「NONCE_{MME}」が含まれる「NAS PDU」に対して、インテグリティプロテクションを施すことによって、ユーザ側に近いE-UTRA方式の無線基地局eNBにおいて、かかる「NAS PDU (E-UTRA方式)」に対して改竄が行われた場合に、かかるハンドオーバ手順を中止することができる。

- [0134] なお、上述の移動局UEや無線基地局NB及びeNBや交換局SGSN及びMMEや無線制御局RNC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。
- [0135] 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。
- [0136] 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、移動局UEや無線基地局NB及びeNBや交換局SGSN及びMMEや無線制御局RNC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移動局UEや無線基地局NB及びeNBや交換局SGSN及びMMEや無線制御局RNC内に設けられていてもよい。
- [0137] 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、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。

請求の範囲

[請求項1]

移動局が、第1無線アクセス方式の無線基地局配下の第1セルから第2無線アクセス方式の無線基地局配下の第2セルに対してハンドオーバーを行うための手順において、

前記第1無線アクセス方式の交換局が、前記第2無線アクセス方式の交換局に対して、前記移動局と該第1無線アクセス方式の交換局との間の通信で用いられる該第1無線アクセス方式の第1プロトコルのセキュリティ処理用パラメータ及び該移動局の該第2無線アクセス方式におけるセキュリティ処理能力を含むハンドオーバー要求メッセージを送信する工程Aと、

前記第2無線アクセス方式の交換局が、前記移動局の該第2無線アクセス方式におけるセキュリティ処理能力に基づいて、該移動局と該第2無線アクセス方式の交換局との間の通信で用いられる該第2無線アクセス方式の第1プロトコルのセキュリティ処理用アルゴリズムを選択する工程Bと、

前記第2無線アクセス方式の交換局が、該第2無線アクセス方式の第1プロトコルのセキュリティ処理用パラメータを生成する工程Cと、

前記第2無線アクセス方式の交換局が、該第2無線アクセス方式の無線基地局に対して、前記移動局の該第2無線アクセス方式におけるセキュリティ処理能力と、前記工程Bで選択された該第2無線アクセス方式の第1プロトコルのセキュリティ処理用アルゴリズム及び該第2無線アクセス方式の第1プロトコルのセキュリティ処理用パラメータとを含むハンドオーバー要求メッセージを送信する工程Dと、

前記第2無線アクセス方式の無線基地局が、前記移動局の該第2無線アクセス方式におけるセキュリティ処理能力に基づいて、該移動局と該第2無線アクセス方式の無線基地局との間の通信で用いられる該第2無線アクセス方式の第2プロトコルのセキュリティ処理用アルゴ

リズムを選択する工程Eと、

前記第2無線アクセス方式の無線基地局が、該第2無線アクセス方式の交換局に対して、該第2無線アクセス方式の第1プロトコルのセキュリティ処理用アルゴリズム、該第2無線アクセス方式の第1プロトコルのセキュリティ処理用パラメータ、及び、前記工程Eで選択された該第2無線アクセス方式の第2プロトコルのセキュリティ処理用アルゴリズムを、トランスペアレントコンテナに含むハンドオーバー要求応答メッセージを送信する工程Fと、

前記第2無線アクセス方式の交換局が、受信した前記ハンドオーバー要求応答メッセージに応じて、前記第1無線アクセス方式の交換局に対して、前記トランスペアレントコンテナを含むメッセージを送信する工程Gと、

前記移動局が、前記第1セルにおいて、前記トランスペアレントコンテナを受信すると、前記第2無線アクセス方式の第1プロトコルのセキュリティ処理用アルゴリズム及び該第2無線アクセス方式の第1プロトコルのセキュリティ処理用パラメータを用いて、該第2無線アクセス方式の第2プロトコルのセキュリティ処理用パラメータを算出する工程Hと、

前記移動局が、前記第2セルにおいて、前記第2無線アクセス方式の第1プロトコルのセキュリティ処理用アルゴリズム及び該第2無線アクセス方式の第1プロトコルのセキュリティ処理用パラメータを用いて、前記第2無線アクセス方式の第1プロトコルを用いた通信におけるセキュリティ処理を行う工程Iと、

前記移動局が、前記第2セルにおいて、前記第2無線アクセス方式の第2プロトコルのセキュリティ処理用アルゴリズム及び該第2無線アクセス方式の第2プロトコルのセキュリティ処理用パラメータを用いて、該第2無線アクセス方式の第2プロトコルを用いた通信におけるセキュリティ処理を行う工程J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2無線アクセス方式の交換局が、前記第1プロトコルのセキュリティ処理用アルゴリズム及び該第1プロトコルのセキュリティ処理用パラメータを用いたインテグリティプロテクション処理を行うことによって、前記第1プロトコル用メッセージを生成する工程と、

前記移動局が、受信した前記第1プロトコルのセキュリティ処理用アルゴリズムと該第1プロトコルのセキュリティ処理用パラメータを用いたインテグリティプロテクション処理を行うことによって、前記第1プロトコル用メッセージに対する改竄の有無を検査する工程と、

前記移動局が、前記第1プロトコル用メッセージに対する改竄があると判断された場合、前記第1無線アクセス方式の無線制御局又は該第1無線アクセス方式の交換局に対して、前記ハンドオーバー手順が失敗した旨を通知する工程と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。

[請求項3]

移動局が、第1無線アクセス方式の無線基地局配下の第1セルから第2無線アクセス方式の無線基地局配下の第2セルに対してハンドオーバーを行うための手順を行うことができる該第2無線アクセス方式の交換局として機能することができる交換局であって、

前記手順において、前記第1無線アクセス方式の交換局から、前記移動局と該第1無線アクセス方式の交換局との間の通信で用いられる該第1無線アクセス方式の第1プロトコルのセキュリティ処理用パラメータ及び前記移動局の前記第2無線アクセス方式におけるセキュリティ処理能力を含むハンドオーバー要求メッセージを受信するように構成されている第1受信部と、

前記手順において、前記第1受信部によって受信された前記移動局の前記第2無線アクセス方式におけるセキュリティ処理能力に基づいて、該移動局との間の通信で用いられる該第2無線アクセス方式の第1プロトコルのセキュリティ処理用アルゴリズムを選択するように構

成されている選択部と、

前記手順において、該第2無線アクセス方式の第1プロトコルのセキュリティ処理用パラメータを生成するように構成されている生成部と、

前記第2無線アクセス方式の無線基地局に対して、前記移動局の該第2無線アクセス方式におけるセキュリティ処理能力と、前記選択部によって選択された該第2無線アクセス方式の第1プロトコルのセキュリティ処理用アルゴリズムと、該第2無線アクセス方式の第1プロトコルのセキュリティ処理用パラメータとを含むハンドオーバー要求メッセージを送信するように構成されている第1送信部と、

前記手順において、前記第2無線アクセス方式の無線基地局から、該第2無線アクセス方式の無線基地局の第1プロトコルのセキュリティ処理用アルゴリズム、該第2無線アクセス方式の無線基地局第1プロトコルのセキュリティ処理用パラメータ、及び、該第2無線アクセス方式の無線基地局と前記移動局との間の通信で用いられる該第2無線アクセス方式の第2プロトコルのセキュリティ処理用アルゴリズムを、トランスペアレントコンテナに含むハンドオーバー要求応答メッセージを受信するように構成されている第2受信部と、

前記手順において、前記第1無線アクセス方式の交換局に対して、前記トランスペアレントコンテナを含むメッセージを送信するように構成されている第2送信部とを具備することを特徴とする交換局。

[請求項4]

移動局が、第1無線アクセス方式の無線基地局配下の第1セルから第2無線アクセス方式の無線基地局配下の第2セルに対してハンドオーバーを行うための手順を行うことができる該第2無線アクセス方式の無線基地局として機能することができる無線基地局であって、

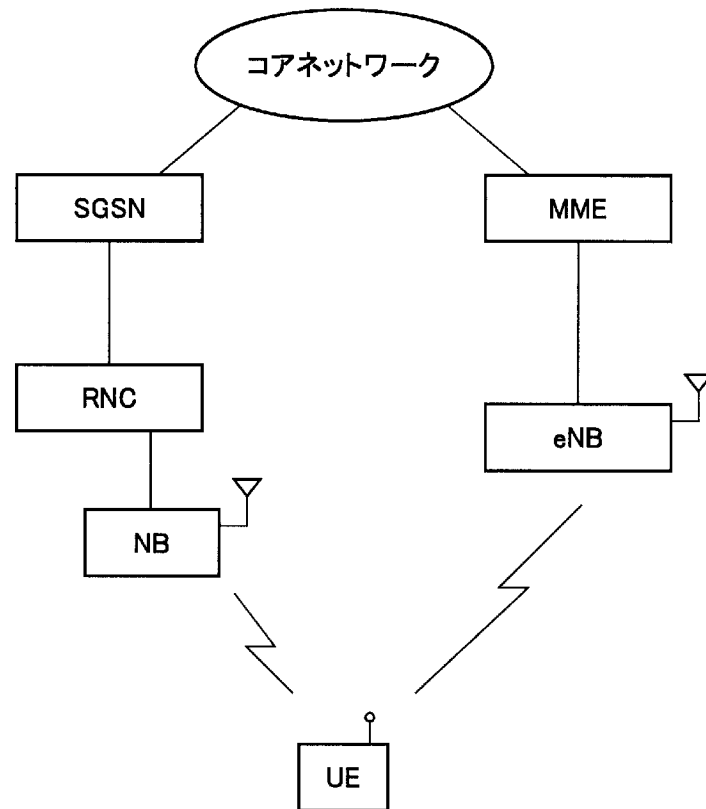
前記手順において、前記第2無線アクセス方式の交換局から、前記移動局の該第2無線アクセス方式におけるセキュリティ処理能力と、該移動局と該第2無線アクセス方式の交換局との間の通信で用いられ

る該第2無線アクセス方式の第1プロトコルのセキュリティ処理用アルゴリズムと、該第2無線アクセス方式の第1プロトコルのセキュリティ処理用パラメータとを含むハンドオーバー要求メッセージを受信するように構成されている受信部と、

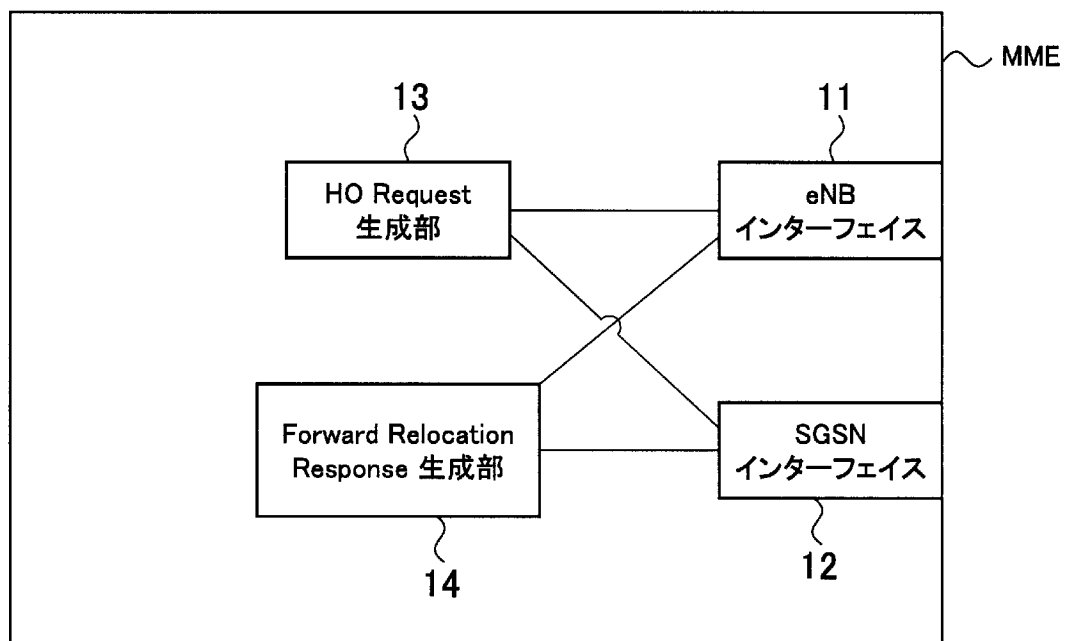
前記手順において、前記移動局の前記第2無線アクセス方式におけるセキュリティ処理能力に基づいて、該移動局と該第2無線アクセス方式の無線基地局との間で用いられる該第2無線アクセス方式の第2プロトコルのセキュリティ処理用アルゴリズムを選択するように構成されている選択部と、

前記手順において、前記第2無線アクセス方式の交換局に対して、前記選択部によって選択された該第2無線アクセス方式の第2プロトコルのセキュリティ処理用アルゴリズムと、該第2無線アクセス方式の第1プロトコルのセキュリティ処理用アルゴリズム及び該第2無線アクセス方式の第1プロトコルのセキュリティ処理用パラメータを含むトランスペアレントコンテナとを含むハンドオーバー要求応答メッセージを送信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。

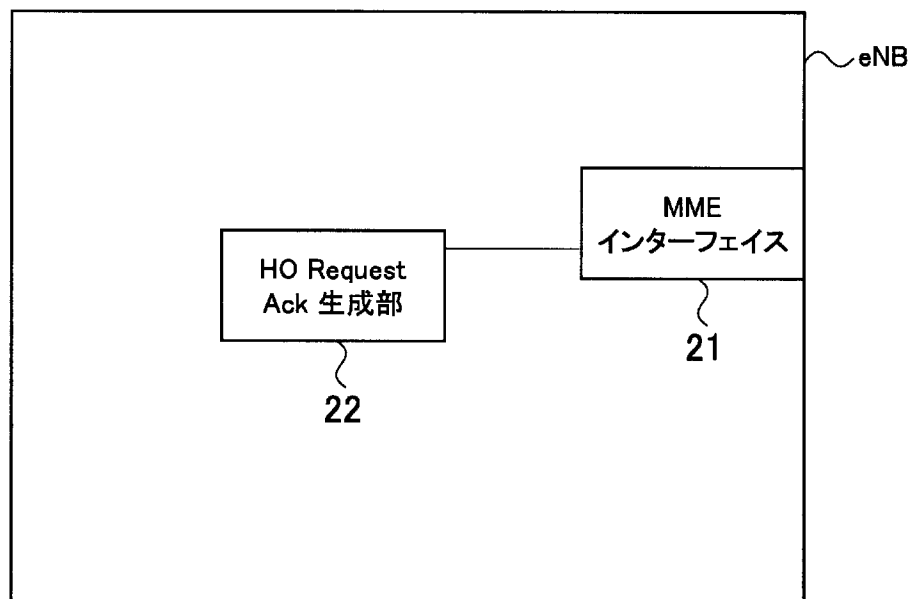
[図1]



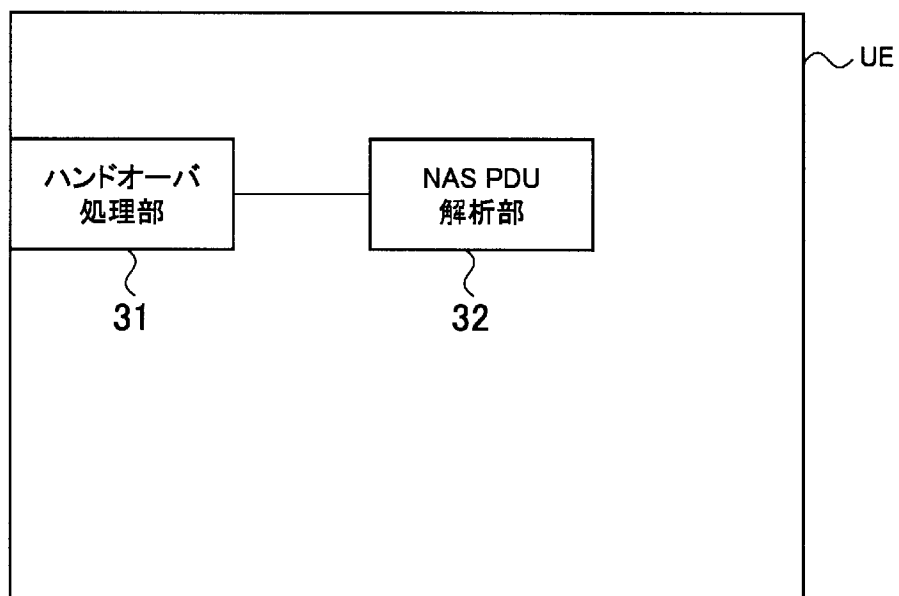
[図2]



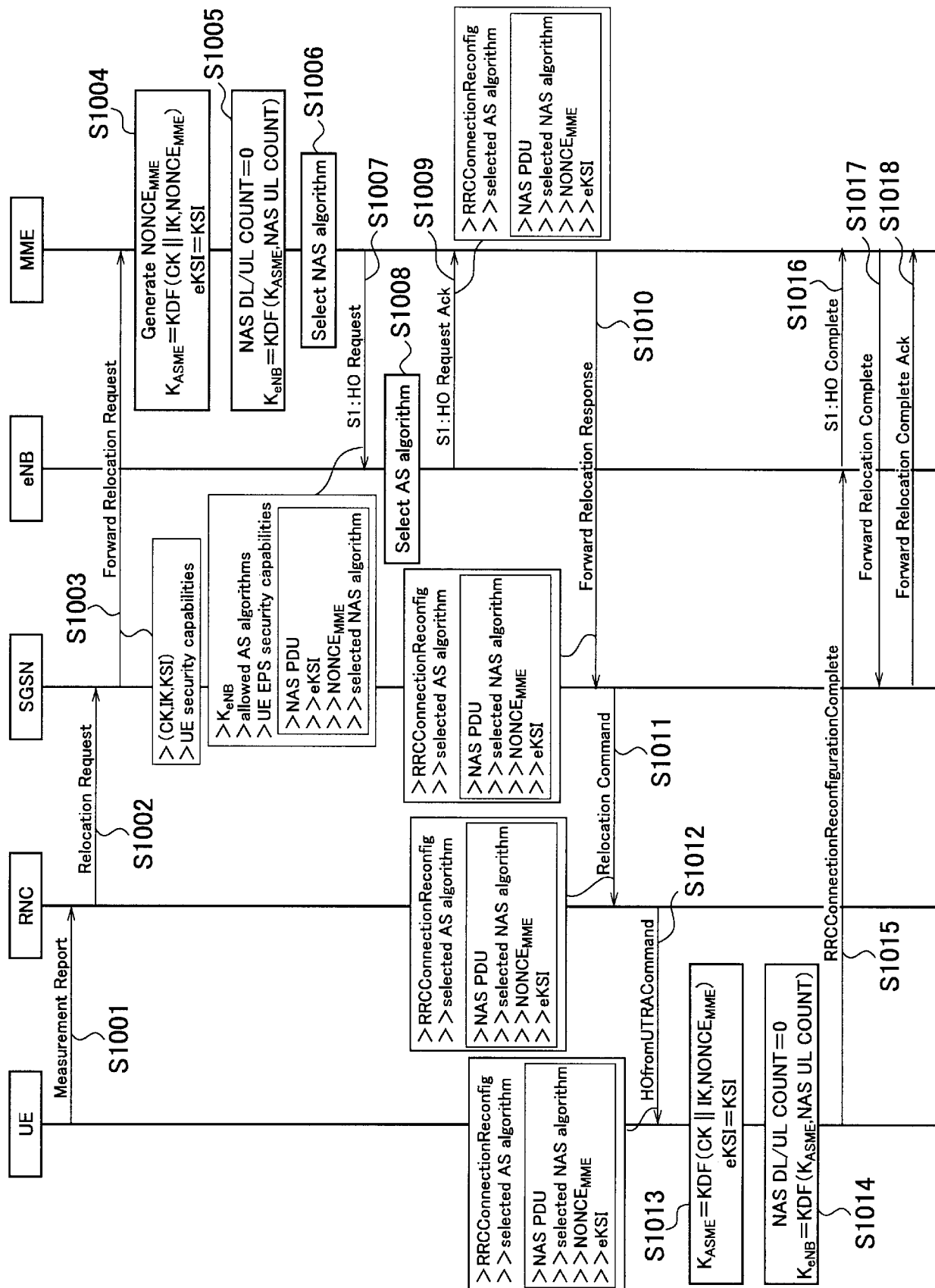
[図3]



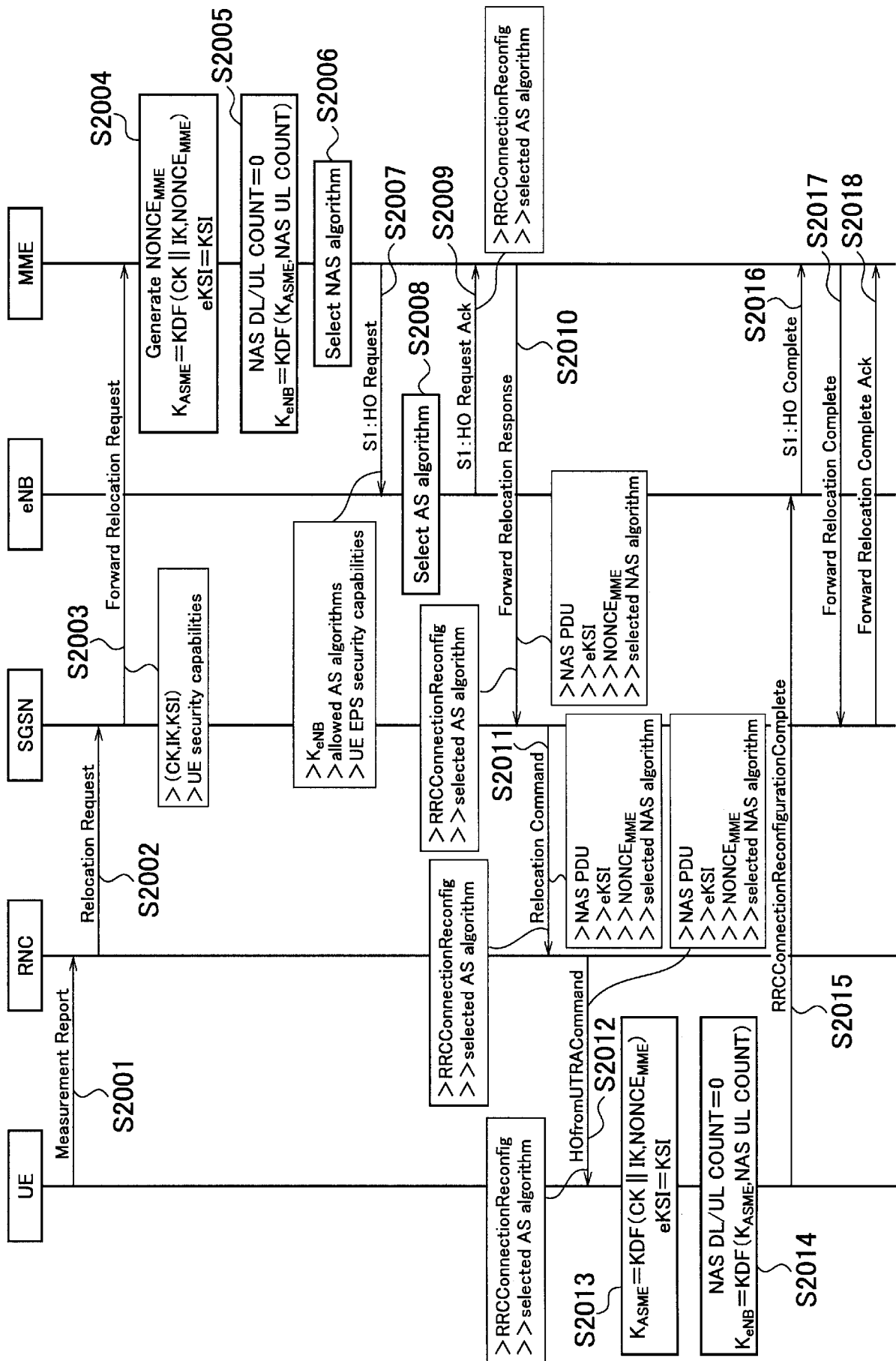
[図4]



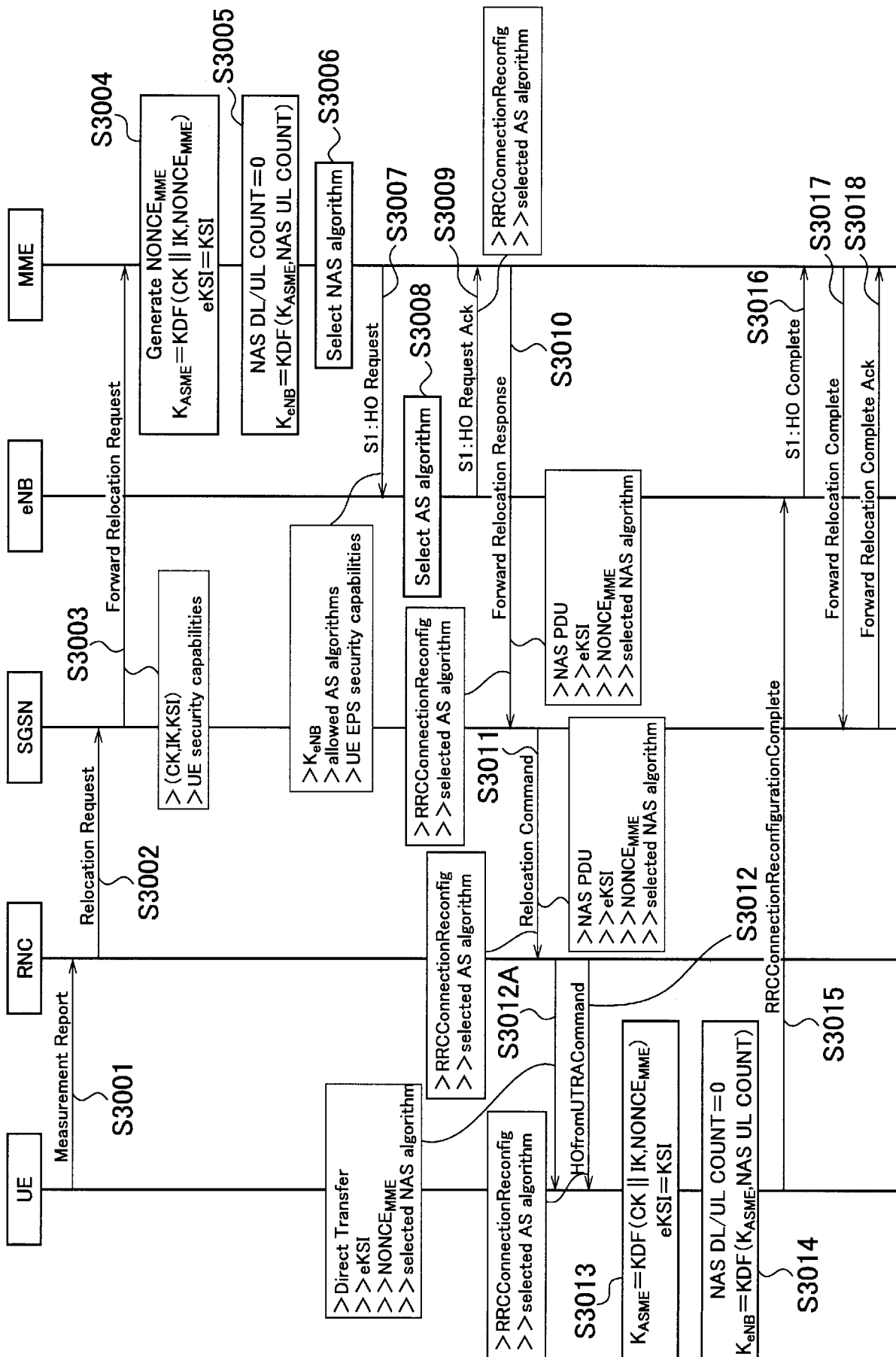
[5]



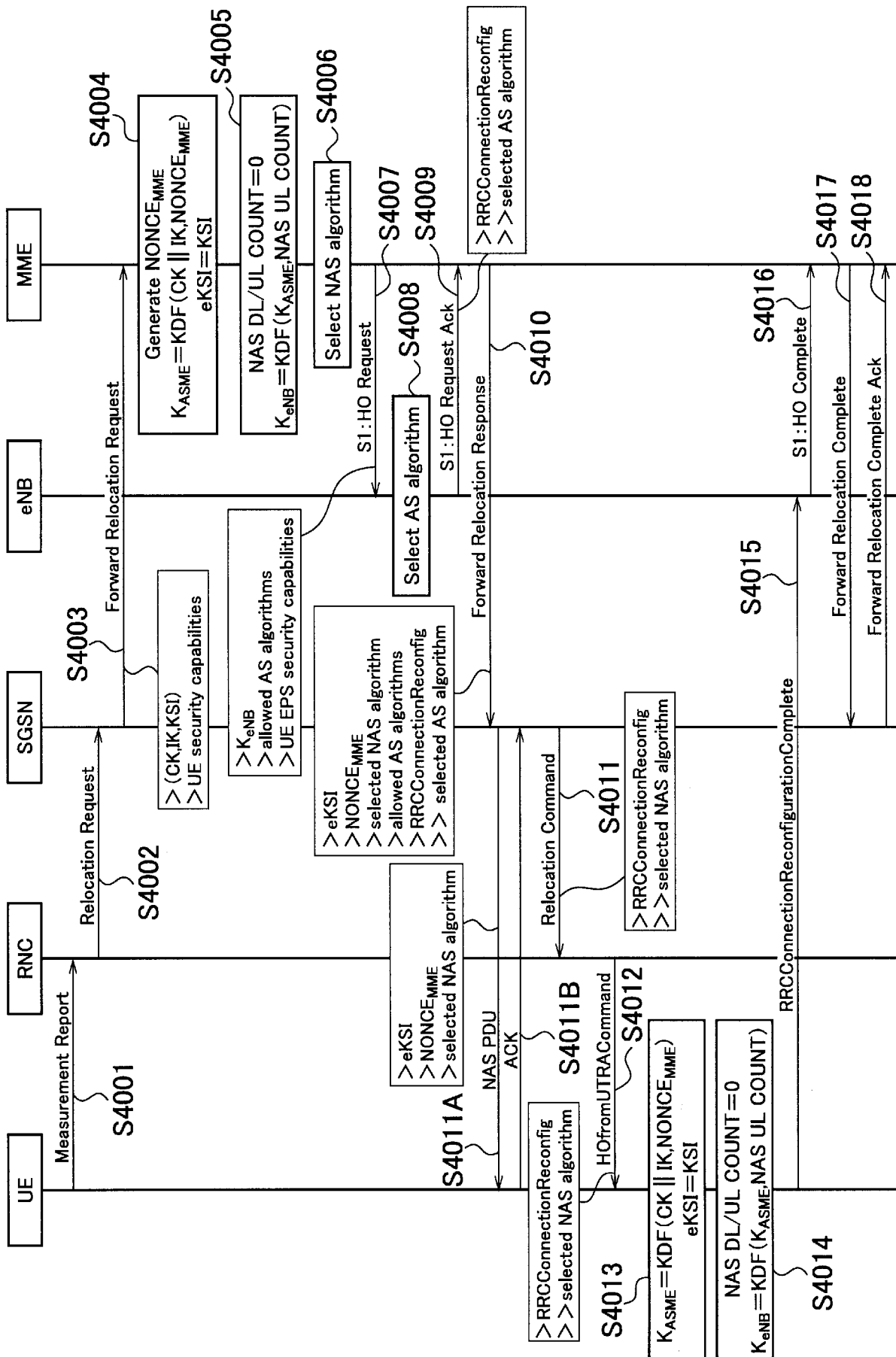
[6]



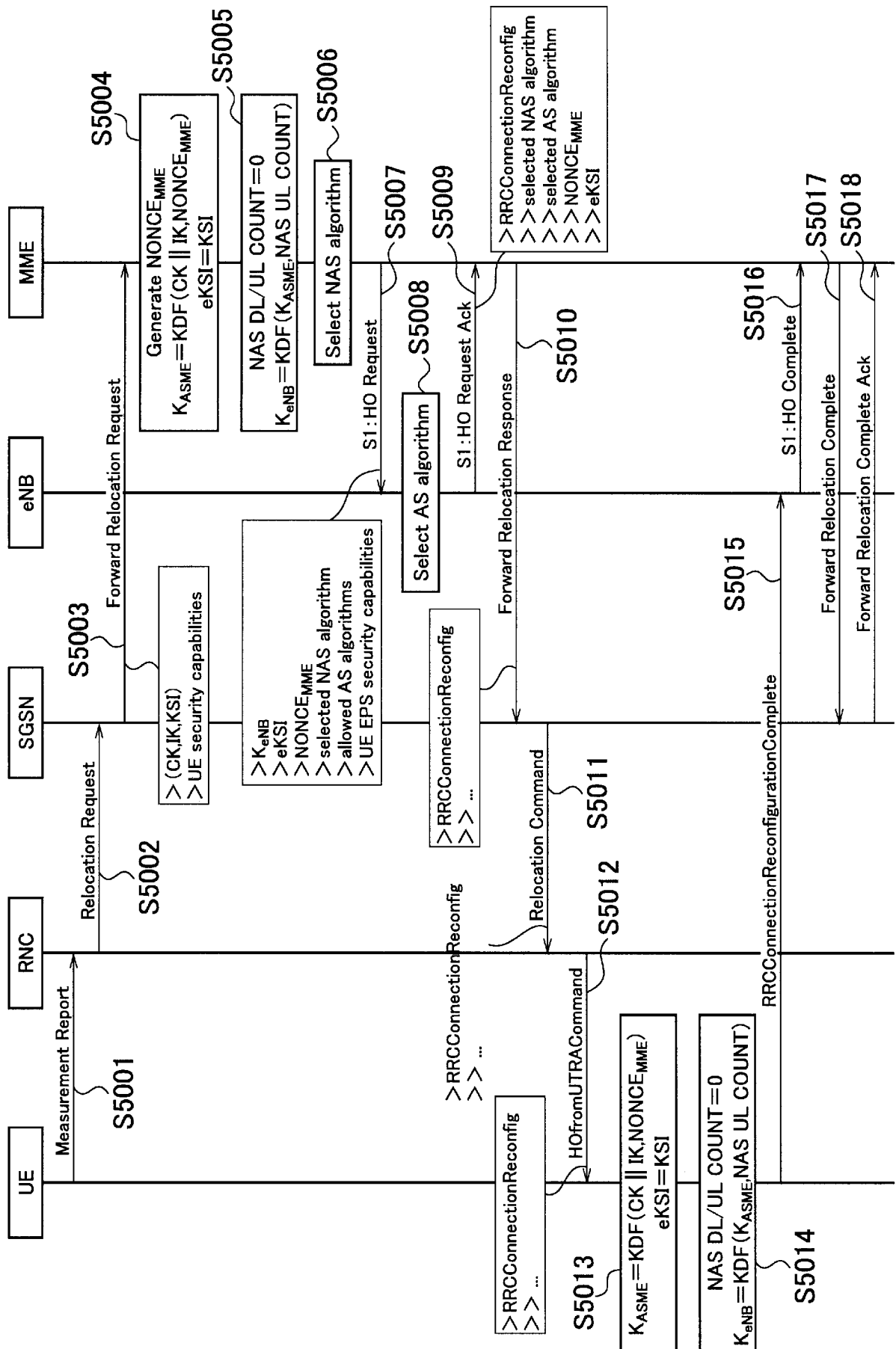
[7]



[8]



[9]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2009/068176

A. CLASSIFICATION OF SUBJECT MATTER

H04W12/08(2009.01) i, H04W36/14(2009.01) i, H04W88/06(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	1996-2009
Kokai Jitsuyo Shinan Koho	1971-2009	Toroku Jitsuyo Shinan Koho	1994-2009

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.
A	JP 2007-515827 A (NTT Docomo Inc.), 14 June 2007 (14.06.2007), entire text & JP 2007-505531 A & US 2007/0064647 A1 & EP 1665855 A & EP 1665856 A & WO 2005/027557 A1 & WO 2005/027559 A1 & WO 2005/027560 A1	1-4
A	JP 2003-516000 A (Nokia Corp.), 07 May 2003 (07.05.2003), entire text & US 6587680 B1 & EP 1232662 A & WO 2001/039538 A1 & CA 2391996 A1	1-4



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
12 November, 2009 (12.11.09)Date of mailing of the international search report
24 November, 2009 (24.11.09)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2009/068176

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2006-332788 A (Toshiba Corp.), 07 December 2006 (07.12.2006), entire text & US 2007/0190973 A1	1-4

A. 発明の属する分野の分類（国際特許分類（I P C））

Int.Cl. H04W12/08(2009.01)i, H04W36/14(2009.01)i, H04W88/06(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 0 9 年
日本国実用新案登録公報	1 9 9 6 - 2 0 0 9 年
日本国登録実用新案公報	1 9 9 4 - 2 0 0 9 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
A	JP 2007-515827 A (株式会社エヌ・ティ・ティ・ドコモ) 2007.06.14, 全文 & JP 2007-505531 A & US 2007/0064647 A1 & EP 1665855 A & EP 1665856 A & WO 2005/027557 A1 & WO 2005/027559 A1 & WO 2005/027560 A1	1-4
A	JP 2003-516000 A (ノキア コーポレイション) 2003.05.07, 全文 & US 6587680 B1 & EP 1232662 A & WO 2001/039538 A1 & CA 2391996 A1	1-4

☒ 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

1 2 . 1 1 . 2 0 0 9

国際調査報告の発送日

2 4 . 1 1 . 2 0 0 9

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）

松野 吉宏

5 J

3 5 7 1

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

C (続き) . 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
A	JP 2006-332788 A (株式会社東芝) 2006. 12. 07, 全文 & US 2007/0190973 A1	1-4