

(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
2022年11月24日(24.11.2022)



(10) 国際公開番号

WO 2022/244658 A1

(51) 国際特許分類:
H04W 74/08 (2009.01) *H04W 12/122* (2021.01)

(21) 国際出願番号: PCT/JP2022/019896

(22) 国際出願日: 2022年5月11日(11.05.2022)

(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 2021-082994 2021年5月17日(17.05.2021) JP

(71) 出願人: 株式会社デンソー (DENSO CORPORATION) [JP/JP]; 〒4488661 愛知県刈谷市昭和町1丁目1番地 Aichi (JP).

(72) 発明者: ▲高▼橋 秀明(TAKAHASHI, Hideaki); 〒4488661 愛知県刈谷市昭和町1丁目1番地 株式会社デンソー内 Aichi (JP).

(74) 代理人: 弁理士法人小澤知的財産事務所 (OZAWA IP FIRM); 〒1050004 東京都港区新橋二丁目11-10 BUREX FIVE 905 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, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY,

(54) Title: BASE STATION AND CONTROL METHOD

(54) 発明の名称: 基地局及び制御方法

[図6]

UE Contention Resolution Identity									Oct 1
UE Contention Resolution Identity									Oct 2
UE Contention Resolution Identity									Oct 3
UE Contention Resolution Identity									Oct 4
UE Contention Resolution Identity									Oct 5
UE Contention Resolution Identity									Oct 6

(57) Abstract: A base station (200) receives a message which is transmitted from a user equipment (100) over an uplink shared channel in a contention based random access procedure, and, if the received message is in compliance with a predetermined format, performs an echo-back process for sending the received message back to the user equipment as identifying data for contention resolution in the contention based random access procedure. If the received message is not in compliance with the predetermined format, the base station (200) does not perform the echo-back process.



WO 2022/244658 A1



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,
ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG,
US, UZ, VC, VN, WS, 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, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (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, KM, ML, MR, NE, SN, TD, TG).

添付公開書類：

- 一 国際調査報告(条約第21条(3))

(57) 要約：基地局(200)は、競合ベースランダムアクセスプロシージャにおいてユーザ装置(100)から上りリンク共有チャネル上で送信されるメッセージを受信し、前記受信したメッセージが所定フォーマットに準拠している場合、前記受信したメッセージを前記競合ベースランダムアクセスプロシージャにおける競合解決用の識別データとして前記ユーザ装置に送り返すエコーバック処理を行う。前記基地局(200)は、前記受信したメッセージが前記所定フォーマットに準拠していない場合、前記エコーバック処理を行わない。

明 細 書

発明の名称： 基地局及び制御方法

関連出願の相互参照

[0001] 本出願は、2021年5月17日に提出された特許出願番号2021-082994号に基づくものであって、その優先権の利益を主張するものであり、その特許出願のすべての内容が、参照により本明細書に組み入れられる。

技術分野

[0002] 本開示は、移動通信システムにおいて用いる基地局及び制御方法に関する。

背景技術

[0003] 3GPP（登録商標。以下同じ）（3rd Generation Partnership Project）の技術仕様に準拠した移動通信システムにおいて、ユーザ装置は、例えば基地局への初期アクセスの際に、基地局との競合ベースランダムアクセスプロシージャを行う。

[0004] 一般的な競合ベースランダムアクセスプロシージャは次の4つのステップからなる。

[0005] 1番目のステップ（MSG1）：

ユーザ装置から基地局に対するランダムアクセスプリアンブル送信。ここで、ユーザ装置は、競合ベースランダムアクセス用のランダムアクセスプリアンブルセットの中から1つのランダムアクセスプリアンブルをランダムに選択し、選択したランダムアクセスプリアンブルを送信する。そのため、複数のユーザ装置が同じランダムアクセスプリアンブルを選択及び送信し得るため、競合が発生し得る。

[0006] 2番目のステップ（MSG2）：

基地局からユーザ装置に対するランダムアクセス応答送信。ここで、基地局は、MSG1で受信したランダムアクセスプリアンブルを示す情報をラン

ダムアクセス応答に含める。また、基地局は、MSG 3送信のための上りリンクグラントをユーザ装置に与える。

[0007] 3番目のステップ（MSG 3）：

ユーザ装置から基地局に対するメッセージ送信。ここで、ユーザ装置が送信したランダムアクセスプリアンプルを示す情報がランダムアクセス応答に含まれているとする。このような場合、当該ユーザ装置は、上りリンクグラントで割り当てられた上りリンク共有チャネル（UL-SCH）リソースを用いて、メッセージ、具体的には、無線リソース制御（RRC）メッセージを基地局に送信する。上述のMSG 1送信の際に、複数のユーザ装置が同じランダムアクセスプリアンプルを選択及び送信していた場合、当該複数のユーザ装置が1つのランダムアクセス応答に反応してMSG 3送信を行うことになる。なお、各ユーザ装置が送信するメッセージは、ユーザ装置固有の情報要素を含む。

[0008] 4番目のステップ（MSG 4）：

基地局からユーザ装置に対する競合解決用の識別データ送信。基地局は、1つのランダムアクセス応答に反応した複数のユーザ装置からの複数のメッセージを受信し得る。基地局は、MSG 3として受信したメッセージのうち1つを競合解決用の識別データとして送り返すエコーバック処理を行う。ユーザ装置は、自身がMSG 3として送信したメッセージが基地局からMSG 4として送り返されてきた場合、競合解決が成功したとみなす。よって、競合ベースランダムアクセスプロシージャでは、MSG 4により競合が解決される仕組みになっている。

[0009] このような競合ベースランダムアクセスプロシージャにおける脆弱性の問題が指摘されている（非特許文献1参照）。具体的には、悪意ある第1ユーザ装置が、例えばプライベートなメッセージをMSG 3として送信する。悪意ある第2ユーザ装置は、基地局からの下りリンク信号をスキャンすることにより、基地局がエコーバックするメッセージ（MSG 4）を受信する。その結果、第1ユーザ装置から基地局を介して第2ユーザ装置にメッセージが

伝送され、悪意あるユーザ装置間で基地局を中継ノードとして用いた不正なメッセージ伝送が行われ得るという問題がある。

先行技術文献

非特許文献

- [0010] 非特許文献1：3GPP寄書 R2-2106454 “Stealth Pirating Attack by RACH Rebroadcast Overwriting (SPARROW) (FSAG Doc 93_009) GSMA”

発明の概要

- [0011] 上述のような脆弱性の問題を解決するためには、競合ベースランダムアクセスプロシーダの仕組みを変更する、すなわち、技術仕様の大幅な変更を行うことが必要になり得る。しかしながら、上述のような脆弱性の問題は3GPPリリース8から起こり得る問題であるため、発明者は、過去及び現在の技術仕様で規定されたユーザ装置の動作を今から変更することは非現実的であると考えた。
- [0012] そこで、本開示は、ユーザ装置の動作を変更することなく、競合ベースランダムアクセスプロシーダにおける脆弱性の問題を解決可能とする基地局及び制御方法を提供することを目的とする。
- [0013] 第1の態様に係る基地局は、移動通信システムで用いる基地局であって、競合ベースランダムアクセスプロシーダにおいてユーザ装置から上りリンク共有チャネル上で送信されるメッセージを受信する通信部と、前記受信したメッセージが所定フォーマットに準拠している場合、前記受信したメッセージを前記競合ベースランダムアクセスプロシーダにおける競合解決用の識別データとして前記ユーザ装置に送り返すエコーバック処理を行う制御部と、を備える。前記制御部は、前記受信したメッセージが前記所定フォーマットに準拠していない場合、前記エコーバック処理を行わないように制御する。
- [0014] 第2の態様に係る制御方法は、移動通信システムで用いる基地局における

制御方法であって、競合ベースランダムアクセスプロシージャにおいてユーザ装置から上りリンク共有チャネル上で送信されるメッセージを受信するステップと、前記受信したメッセージが所定フォーマットに準拠している場合、前記受信したメッセージを前記競合ベースランダムアクセスプロシージャにおける競合解決用の識別データとして前記ユーザ装置に送り返すエコーバック処理を行うステップと、前記受信したメッセージが前記所定フォーマットに準拠していない場合、前記エコーバック処理を行わないように制御するステップと、を有する。

図面の簡単な説明

- [0015] 本開示についての上記目的およびその他の目的、特徴や利点は、添付の図面を参照しながら下記の詳細な記述により、より明確になる。その図面は、
- [図1]図1は、実施形態に係る移動通信システムの構成を示す図であり、
- [図2]図2は、実施形態に係るプロトコルスタックの構成例を示す図であり、
- [図3]図3は、競合ベースランダムアクセス（C B R A）プロシージャを示す図であり、
- [図4]図4は、MSG3を構成するUL-CCCH-Messageを示す図であり、
- [図5]図5は、MSG3を構成するUL-CCCH1-Messageを示す図であり、
- [図6]図6は、MSG4を構成するUE contention resolution MAC CEを示す図であり、
- [図7]図7は、C B R Aプロシージャにおける脆弱性の問題について説明するための図であり、
- [図8]図8は、実施形態に係る基地局の構成を示す図であり、
- [図9]図9は、実施形態に係る基地局の動作について説明するための図であり、
- [図10]図10は、実施形態に係る基地局の制御方法を示す図であり、
- [図11]図11は、その他の実施形態に係る基地局の動作について説明するた

めの図である。

発明を実施するための形態

[0016] 図面を参照しながら、実施形態に係る移動通信システムについて説明する。図面の記載において、同一又は類似の部分には同一又は類似の符号を付している。

[0017] (システム構成)

まず、図1を参照して、本実施形態に係る移動通信システム1の構成について説明する。移動通信システム1は、例えば、3GPPの技術仕様(Technical Specification: TS)に準拠したシステムである。以下において、移動通信システム1として、3GPP規格の第5世代システム(5th Generation System: 5GS)、すなわち、NR(New Radio)に基づく移動通信システムを例に挙げて説明する。

[0018] 移動通信システム1は、ネットワーク10と、ネットワーク10と通信するユーザ装置(User Equipment: UE)100とを有する。ネットワーク10は、5Gの無線アクセスネットワークであるNG-RAN(Next Generation Radio Access Network)20と、5Gのコアネットワークである5GC(5G Core Network)30とを含む。

[0019] UE100は、ユーザにより利用される装置である。UE100は、例えば、スマートフォンなどの携帯電話端末、タブレット端末、ノートPC、通信モジュール、又は通信カードなどの移動可能な装置である。UE100は、車両(例えば、車、電車など)又はこれに設けられる装置であってよい。UE100は、車両以外の輸送機体(例えば、船、飛行機など)又はこれに設けられる装置であってよい。UE100は、センサ又はこれに設けられる装置であってよい。なお、UE100は、移動局、移動端末、移動装置、移動ユニット、加入者局、加入者端末、加入者装置、加入者ユニット、ワイヤレス局、ワイヤレス端末、ワイヤレス装置、ワイヤレスユニット、リモート

局、リモート端末、リモート装置、又はリモートユニット等の別の名称で呼ばれてもよい。

[0020] NG-RAN20は、複数の基地局200を含む。各基地局200は、少なくとも1つのセルを管理する。セルは、通信エリアの最小単位を構成する。1つのセルは、1つの周波数（キャリア周波数）に属し、1つのコンポーネントキャリアにより構成される。用語「セル」は、無線通信リソースを表すことがあり、UE100の通信対象を表すこともある。各基地局200は、自セルに在圏するUE100との無線通信を行うことができる。基地局200は、RANのプロトコルスタックを使用してUE100と通信する。基地局200は、UE100へ向けたNRユーザプレーン及び制御プレーンプロトコル終端を提供し、NGインターフェイスを介して5GC30に接続される。このようなNRの基地局200は、gNodeB（gNB）と称されることがある。

[0021] 5GC30は、コアネットワーク装置300を含む。コアネットワーク装置300は、例えば、AMF（Access and Mobility Management Function）及び／又はUPF（User Plane Function）を含む。AMFは、UE100のモビリティ管理を行う。UPFは、ユーザプレーン処理に特化した機能を提供する。AMF及びUPFは、NGインターフェイスを介して基地局200と接続される。

[0022] 次に、図2を参照して、本実施形態に係るプロトコルスタックの構成例について説明する。

[0023] UE100と基地局200との間の無線区間のプロトコルは、物理（PHY）レイヤと、MAC（Medium Access Control）レイヤと、RLC（Radio Link Control）レイヤと、PDCP（Packet Data Convergence Protocol）レイヤと、RRCレイヤとを有する。

[0024] PHYレイヤは、符号化・復号、変調・復調、アンテナマッピング・デマ

ッピング、及びリソースマッピング・デマッピングを行う。UE 100のPHYレイヤと基地局200のPHYレイヤとの間では、物理チャネルを介してデータ及び制御情報が伝送される。

[0025] MACレイヤは、データの優先制御、ハイブリッドARQ (HARQ: Hybrid Automatic Repeat request) による再送処理、及びランダムアクセスプロシージャ等を行う。UE 100のMACレイヤと基地局200のMACレイヤとの間では、トランスポートチャネルを介してデータ及び制御情報が伝送される。基地局200のMACレイヤはスケジューラを含む。スケジューラは、上下リンクのトランスポートフォーマット (トランスポートブロックサイズ、変調・符号化方式 (MCS)) 及びUE 100への割り当りリソースを決定する。

[0026] RLCレイヤは、MACレイヤ及びPHYレイヤの機能を利用してデータを受信側のRLCレイヤに伝送する。UE 100のRLCレイヤと基地局200のRLCレイヤとの間では、論理チャネルを介してデータ及び制御情報が伝送される。

[0027] PDCPレイヤは、ヘッダ圧縮・伸張、及び暗号化・復号化を行う。

[0028] PDCPレイヤの上位レイヤとしてSDAP (Service Data Adaptation Protocol) レイヤが設けられていてもよい。SDAP (Service Data Adaptation Protocol) レイヤは、コアネットワークがQoS制御を行う単位であるIPフローとAS (Access Stratum) がQoS制御を行う単位である無線ベアラとのマッピングを行う。

[0029] RRCレイヤは、無線ベアラの確立、再確立及び解放に応じて、論理チャネル、トランスポートチャネル、及び物理チャネルを制御する。UE 100のRRCレイヤと基地局200のRRCレイヤとの間では、各種設定のためのRRCシグナリングが伝送される。UE 100のRRCと基地局200のRRCとの間にRRC接続がある場合、UE 100はRRCコネクティッド状態にある。UE 100のRRCと基地局200のRRCとの間にRRC接

続がない場合、UE 100はRRCアイドル状態にある。UE 100のRRCと基地局200のRRCとの間のRRC接続がサスペンドされている場合、UE 100はRRCインアクティブ状態にある。

[0030] RRCレイヤの上位に位置するNASレイヤは、UE 100のセッション管理及びモビリティ管理を行う。UE 100のNASレイヤとコアネットワーク装置300（AMF）のNASレイヤとの間では、NASシグナリングが伝送される。なお、UE 100は、無線インターフェースのプロトコル以外にアプリケーションレイヤ等を有する。

[0031] （競合ベースランダムアクセスプロシージャの概要）

次に、図3を参照して、競合ベースランダムアクセスプロシージャの概要について説明する。ランダムアクセスプロシージャには、競合フリーランダムアクセス（CFRA）と競合ベースランダムアクセス（CBRA）の2種類がある。

[0032] CFRAにおいては、UE 100に専用のランダムアクセスプリアンブル（RAプリアンブル）を基地局200からUE 100に割り当て、UE 100が、割り当てられたRAプリアンブルを物理ランダムアクセスチャネル（PRACH）上で基地局200に送信する。基地局200は、UE 100から受信したRAプリアンブルに基づいて、このRAプリアンブルの送信元UEを一意に特定できる。

[0033] 一方、CBRAプロシージャにおいては、UE 100は、CBRA用に用意されたRAプリアンブルセットの中から1つのRAプリアンブルをランダムに選択し、選択したRAプリアンブルをPRACH上で基地局200に送信する。基地局200は、このRAプリアンブルの送信元UEを一意に特定できない。CBRAプロシージャにおいては、複数のUE 100が同じRAプリアンブルを選択してCBRAプロシージャを開始し得るため、競合を解決する動作が必要になる。一般的なCBRAプロシージャは、4つのステップによってRAプロシージャを完了させる4ステップRAプロシージャである。例えば、RRCアイドル状態又はRRCインアクティブ状態にあるUE

100は、RRCコネクティッド状態に遷移するためにCBRAプロシージャを開始する。

[0034] 4ステップのCBRAプロシージャは、MSG1乃至MSG4の4つのステップからなる。

[0035] MSG1 :

UE100は、選択したRAプリアンプル(RAプリアンプル)を基地局200に送信する。RAプリアンプル若しくはその送信は、4ステップRAプロシージャにおけるメッセージ1(MSG1)と呼ばれる。

[0036] MSG2 :

基地局200は、UE100からのRAプリアンプルの受信に応じて、RA応答をUE100に送信する。ここで、基地局200は、RA-RNTI(Random Access-Radio Network Temporary Identifier)でRA応答をスクランブルして送信する。そのため、基地局200配下の全てのUE100がRA応答を受信可能である。RA応答若しくはその送信は、4ステップRAプロシージャにおけるメッセージ2(MSG2)と呼ばれる。

[0037] MSG2は、UE100から受信したRAプリアンプルを示すプリアンプル情報と、上りリンクグラント(UL grant)と、タイミングアドバンス値と、一時識別子とを含む。プリアンプル情報は、UE100から受信したRAプリアンプルを示す情報である。UL grantは、後述するMSG3をUE100が送信するために用いるUL-SCHリソース(具体的には、PUSCH(Physical Uplink Access Channel)リソース)を示す情報である。タイミングアドバンス値は、無線信号の伝搬遅延を補償するための送信タイミング調整値である。一時識別子は、基地局200がUE100に割り当てたTemporary C-RNTI(Cell-Radio Network Temporary Identifier)である。RA応答を受信したUE100は、自身が送信したRAプリアンプルと、ステップS102で基地局200から受信した

プリアンプル情報が示すRAプリアンプルとが一致する場合、MSG3に処理を進める。

[0038] MSG3 :

UE100は、RA応答の受信に応じて、メッセージをUL-SCH (PUSCH) 上で送信する。UE100は、自身が送信したRAプリアンプルを示す情報がRA応答に含まれている場合、UL grantで割り当てられたUL-SCHリソースを用いて、メッセージ、具体的には、RRCメッセージを基地局に送信する。上述のMSG1送信の際に、複数のUE100が同じRAプリアンプルを選択及び送信していた場合、当該複数のUE100が1つのRA応答に反応してMSG3送信を行うことになる。なお、各UE100が送信するメッセージは、UE固有の情報要素を含む。このような基地局200により最初にスケジューリングされたメッセージ若しくはその送信は、4ステップRAプロシージャにおけるメッセージ3 (MSG3) と呼ばれる。

[0039] 具体的には、UE100のMACエンティティは、上りリンクの共通制御チャネル (CCCH) のサービスデータユニット (SDU) をMSG3として送信する。このUL CCCH SDUには、RRCエンティティが生成したRRCメッセージ (UL-CCCH-Message又はUL-CCCH-H1-Message) が含まれている。このようなRRCメッセージは、UE固有の情報要素、例えばUE100の識別子を含む。図4に示すように、UL-CCCH-Messageは、48ビットのRRCメッセージであって、CCCH論理チャネル上でUE100から基地局200に送信されるメッセージである。UL-CCCH-Messageのメッセージタイプ (UL-CCCH-MessageType) には、RRCSetupRequest、RRCResumeRequest、RRCReestablishmentRequest、及びRRCSystemInfoRequestがあり、これらのタイプのいずれかのメッセージがセットされる。RRCSetupRequestは、RRC接続の確立を要求するために用いる

メッセージである。RRCResumeRequestは、サスペンドされたRRC接続の復旧(resumption)の要求又はRNA(RAN Notification Area)更新の実行のために用いるメッセージである。RRCReestablishmentRequestは、RRC接続の再確立を要求するために用いるメッセージである。RRCSystemInfoRequestは、UE100が必要とするシステム情報メッセージの送信を要求するために用いるメッセージである。図5に示すように、UL-CCCH1-Messageは、64ビットのRRCメッセージであって、CCCH1論理チャネル上でUE100から基地局200に送信されるメッセージである。UL-CCCH1-Messageのメッセージタイプ(UL-CCCH1-MessageType)には、RRCResumeRequest1がある。RRCResumeRequest1は、サスペンドされたRRC接続の復旧の要求又はRNA更新の実行のために用いるメッセージである。

[0040] MSG4:

基地局200は、UE100に対する競合解決用の識別データ(UE contention resolution MAC CE)を送信する。このような競合解決用の識別データ若しくはその送信は、4ステップRAプロシージャにおけるメッセージ4(MSG4)と呼ばれる。基地局200は、1つのRA応答に反応した複数のUE100からの複数のMSG3を受信し得る。基地局200は、最初に受信したMSG3を選択し、このMSG3で受信したメッセージを競合解決用の識別データ(MSG4)として送り返すエコーバック処理を行う。UE100は、自身がMSG3として送信したメッセージが基地局からMSG4として送り返されてきた場合、競合解決が成功したとみなす。よって、競合ベースRAプロシージャでは、MSG4により競合が解決される仕組みになっている。

[0041] 具体的には、基地局200は、MSG3で受信したUL-CCCH-SDUを、図6に示すUE contention resolution M

AC CEに含めて送信する。UE contention resolution MAC CEは、固定サイズであり、特定のLCIDを持つMACサブヘッダーによって識別される。UE contention resolution MAC CEの「UE Contention Resolution Identity」フィールドには、UL CCCH SDUが含まれる。UE 100は、自身が送ったUL CCCH SDUと基地局200から受信したUE contention resolution MAC CEとが一致する場合には、競合解決成功とみなす。一方、両者が一致しない場合には、UE 100は、競合解決失敗とみなし、復号したMAC PDU (Protocol Data Unit) を破棄する。

[0042] 次に、図7を参照し、CBRAプロシージャにおける脆弱性の問題について説明する。

[0043] 悪意あるUE 100Aが、不正なメッセージ、例えば、プライベートなメッセージをMSG3として送信する。悪意あるUE 100Bは、基地局200からの下りリンク信号をスキャンすることにより、基地局200がエコーバックするメッセージ(MSG4)を受信する。その結果、UE 100Aから基地局200を介してUE 100Bにメッセージが伝送され、悪意あるUE間で基地局200を中継ノードとして用いた不適切なメッセージ伝送が行われ得る。特に、MSG3及びMSG4が送受信される段階ではUE 100Aの認証処理が済んでいないため、不適切な通信を行ったUE 100Aを記録に残すことが難しい。

[0044] 本実施形態において、MSG3及びMSG4に関して基地局200に新規な動作を導入することにより、CBRAプロシージャに関するTSの大幅な変更を伴わずに、CBRAプロシージャにおける脆弱性の問題を解決可能とする。

[0045] (基地局の構成)

次に、図8を参照して、本実施形態に係る基地局200の構成について説明する。基地局200は、通信部210と、ネットワークインターフェイス

220と、制御部230とを有する。

[0046] 通信部210は、例えば、UE100からの無線信号を受信し、UE100への無線信号を送信する。通信部210は、無線信号を受信する1つ又は複数の受信機及び無線信号を送信する1つ又は複数の送信機を備えてよい。受信機及び送信機は、アンテナ及びRF (Radio Frequency) 回路を含んで構成されてもよい。アンテナは、信号を電波に変換し、当該電波を空間に放射する。また、アンテナは、空間における電波を受信し、当該電波を信号に変換する。RF回路は、アンテナを介して送受信される信号のアナログ処理を行う。RF回路は、高周波フィルタ、増幅器、変調器及びローパスフィルタ等を含んでもよい。

[0047] ネットワークインターフェイス220は、信号をネットワークと送受信する。ネットワークインターフェイス220は、例えば、基地局間インターフェイスであるXnインターフェイスを介して接続された隣接基地局から信号を受信し、隣接基地局へ信号を送信する。また、ネットワークインターフェイス220は、例えば、NGインターフェイスを介して接続されたコアネットワーク装置300から信号を受信し、コアネットワーク装置300へ信号を送信する。

[0048] 制御部230は、基地局200における各種の制御を行う。制御部230は、例えば、通信部210を介したUE100との通信を制御する。また、制御部230は、例えば、ネットワークインターフェイス220を介したノード（例えば、隣接基地局、コアネットワーク装置300）との通信を制御する。上述及び後述の基地局200の動作は、制御部230の制御による動作であってよい。制御部230は、プログラムを実行可能な少なくとも1つのプロセッサ及びプログラムを記憶するメモリを含んでよい。プロセッサは、プログラムを実行して、制御部230の動作を行ってもよい。制御部230は、アンテナ及びRF回路を介して送受信される信号のデジタル処理を行うデジタル信号プロセッサを含んでもよい。当該デジタル処理は、RANのプロトコルスタックの処理を含む。なお、メモリは、プロセッサにより実行

されるプログラム、当該プログラムに関するパラメータ、及び、当該プログラムに関するデータを記憶する。メモリの全部又は一部は、プロセッサ内に含まれていてよい。

[0049] このように構成された基地局200において、通信部210は、C B R A プロシージャにおいてU E 1 0 0 からU L - S C H 上で送信されるメッセージを受信する。制御部230は、通信部210が受信したメッセージが所定フォーマット（すなわち、T S で規定されたフォーマット）に準拠している場合、通信部210が受信したメッセージをC B R A プロシージャにおける競合解決用の識別データとしてU E 1 0 0 に送り返すエコーバック処理を行う。これに対し、通信部210が受信したメッセージが所定フォーマットに準拠していない場合、制御部230は、エコーバック処理を行わないように制御する。換言すると、制御部230は、通信部210が受信したメッセージが所定フォーマットに準拠している場合に限り、エコーバック処理を伴うM S G 4 送信を行う。

[0050] これにより、図9に示すように、悪意あるU E 1 0 0 A が不正なメッセージをM S G 3 中で送信する場合、このメッセージが所定フォーマットに準拠していないため、エコーバック処理（M S G 4 送信）が行われなくなることになる。その結果、U E 1 0 0 A から基地局200を介してU E 1 0 0 B に不正なメッセージが伝送されること、すなわち、悪意あるU E 間で基地局200を中継ノードとして用いた不正な通信が行われることを防止できる。

[0051] 本実施形態に係る基地局200において、制御部230は、通信部210が受信したメッセージが所定フォーマットに準拠していない場合、エコーバック処理を行わずに、当該メッセージを破棄してもよい。これにより、セキュリティをより一層高めることができる。

[0052] 本実施形態において、C B R A プロシージャは、4つのステップからなる4ステップR A プロシージャである。通信部210がU L - S C H 上でU E 1 0 0 から受信するメッセージは、4つのステップにおける3番目のステップにおいてU E 1 0 0 から基地局200に送信されるM S G 3 である。競合

解決用の識別データは、4つのステップにおける4番目のステップにおいて基地局200からUE100に送信するMSG4である。制御部230は、MSG3が所定フォーマットに準拠している場合、エコーバック処理を伴うMSG4送信を行うように制御する。これに対し、MSG3が所定フォーマットに準拠していない場合、制御部230は、MSG4送信を行わないように制御する。これにより、4ステップCBRAプロシージャにおける脆弱性の問題を解決できる。

[0053] 本実施形態において、所定フォーマットは、移動通信システム1のTS（すなわち、3GPPのTS）で規定されるフォーマットである。例えば、所定フォーマットは、UL CCCH SDUに準拠したフォーマットである。制御部230は、通信部210が受信したメッセージがUL CCCH SDUに準拠したフォーマットであるか否かを確認するフォーマット確認を行う。これにより、基地局200（制御部230）は、TSで規定されるUL CCCH SDUに準拠しないメッセージを不正なメッセージとみなし、当該メッセージのエコーバック処理を避けることができる。このようなフォーマット確認を含む基地局200の制御方法の詳細については後述する。

[0054] （基地局の制御方法）

次に、図10を参照して、本実施形態に係る基地局200の制御方法について説明する。

[0055] ステップS1において、基地局200（通信部210）は、UE100からMSG3を受信する。

[0056] ステップS2において、基地局200（制御部230）は、UE100から受信したMSG3（UL CCCH SDU）にUE contention resolution IDとしてUL-CCCH-Messageが含まれているか否かを判定する。UE100から受信したMSG3（UL CCCH SDU）にUL-CCCH-Messageが含まれていない場合（ステップS2：NO）、ステップS3において、基地局200（制御部230）は、UE100から受信したMSG3（UL CCCH SDU

) にUE contention resolution IDとしてUL-CCCH-Message 1が含まれているか否かを判定する。UE 100から受信したMSG3 (UL-CCCH-SDU) にUL-CCCH-Message及びUL-CCCH-Message 1のいずれも含まれていない場合 (ステップS3: NO)、ステップS4において、基地局200 (制御部230) は、受信したMSG3 (UL-CCCH-SDU) のエコーバック処理を行うことなく、受信したMSG3 (UL-CCCH-SDU) を破棄する。

[0057] UE 100から受信したMSG3 (UL-CCCH-SDU) にUE contention resolution IDとしてUL-CCCH-Messageが含まれている場合 (ステップS2: YES)、ステップS5において、基地局200 (制御部230) は、当該UL-CCCH-Messageのメッセージタイプ (UL-CCCH-MessageType) が次のいずれかであるか否かを判定する:

- rrcSetupRequest;
- rrcResumeRequest;
- rrcReestablishmentRequest;
- rrcSystemInfoRequest。

[0058] ステップS5で「NO」である場合、ステップS6において、基地局200 (制御部230) は、受信したMSG3 (UL-CCCH-SDU) のエコーバック処理を行うことなく、受信したMSG3 (UL-CCCH-SDU) を破棄する。他方、ステップS5で「YES」である場合、ステップS7において、基地局200 (制御部230) は、受信したMSG3 (UL-CCCH-SDU) 中のUL-CCCH-Messageが、対応するメッセージタイプのTS (具体的には、RRCのTSであるTS38.331) で規定されるメッセージフォーマットに準拠しているか否かを判定する。例えば、基地局200 (制御部230) は、必須のフィールド (Mandatory field) が抜けている場合、TSで規定されるメッセージフォ

フォーマットに準拠していないと判定する。また、例えば、基地局200（制御部230）は、フィールド長がTSで規定されている長さと異なっている場合、TSで規定されるメッセージフォーマットに準拠していないと判定する。また、例えば、基地局200（制御部230）は、TSで規定されていないフィールドがある場合、TSで規定されるメッセージフォーマットに準拠していないと判定する。TSで規定されるメッセージフォーマットに準拠していないと判定された場合（ステップS7：NO）、ステップS6において、基地局200（制御部230）は、受信したMSG3（UL CCCH SDU）のエコーバック処理を行うことなく、受信したMSG3（UL CCCH SDU）を破棄する。これに対し、TSで規定されるメッセージフォーマットに準拠していると判定された場合（ステップS7：YES）、ステップS8において、基地局200（制御部230）は、受信したMSG3（UL CCCH SDU）のエコーバック処理を伴うMSG4（UE contention resolution MAC CE）送信を行う。具体的には、基地局200（通信部210）は、受信したMSG3（UL CCCH SDU）を含むMSG4（UE contention resolution MAC CE）を送信する。

[0059] UE100から受信したMSG3（UL CCCH SDU）にUE contention resolution IDとしてUL-CCCH-Message1が含まれている場合（ステップS3：YES）、ステップS9において、基地局200（制御部230）は、当該UL-CCCH-Message1のメッセージタイプ（UL-CCCH-MessageType1）がrrcResumeRequest1であるか否かを判定する。ステップS9で「NO」である場合、ステップS4において、基地局200（制御部230）は、受信したMSG3（UL CCCH SDU）のエコーバック処理を行うことなく、受信したMSG3（UL CCCH SDU）を破棄する。他方、ステップS9で「YES」である場合、ステップS10において、基地局200（制御部230）は、受信したMSG3（UL

CCCH SDU) 中のUL-CCCH-Message 1が、対応するメッセージタイプのTS (具体的には、RRCのTSであるTS 38.331) で規定されるメッセージフォーマットに準拠しているか否かを判定する。例えば、基地局200 (制御部230) は、必須のフィールド (Mandatory field) が抜けている場合、TSで規定されるメッセージフォーマットに準拠していないと判定する。また、例えば、基地局200 (制御部230) は、フィールド長がTSで規定されている長さと異なっている場合、TSで規定されるメッセージフォーマットに準拠していないと判定する。また、例えば、基地局200 (制御部230) は、TSで規定されていないフィールドがある場合、TSで規定されるメッセージフォーマットに準拠していないと判定する。TSで規定されるメッセージフォーマットに準拠していないと判定された場合 (ステップS9: NO)、ステップS4において、基地局200 (制御部230) は、受信したMSG3 (UL-CCCH SDU) のエコーバック処理を行うことなく、受信したMSG3 (UL-CCCH SDU) を破棄する。これに対し、TSで規定されるメッセージフォーマットに準拠していると判定された場合 (ステップS9: YES)、ステップS10において、基地局200 (制御部230) は、受信したMSG3 (UL-CCCH SDU) のエコーバック処理を伴うMSG4 (UE contention resolution MAC CE) 送信を行う。具体的には、基地局200 (通信部210) は、受信したMSG3 (UL-CCCH SDU) を含むMSG4 (UE contention resolution MAC CE) を送信する。

[0060] なお、図10に示す制御方法は一例に過ぎないものであって、MSG3中のUL-CCCH SDUとして、UL-CCCH-Message及びUL-CCCH-Message 1以外のメッセージがTSにおいて新たに導入された場合、当該新たに導入されたメッセージはエコーバック対象として扱われる。同様に、UL-CCCH-MessageTypeとして、rrcSetupRequest、rrcResumeRequest、rrc

Reestablishment Request、及びrrcSystemInfoRequest以外のメッセージがTSにおいて新たに導入された場合、当該新たに導入されたメッセージはエコーバック対象として扱われる。同様に、UL-CCCH-MessageType1として、rrcResumeRequest1以外のメッセージがTSにおいて新たに導入された場合、当該新たに導入されたメッセージはエコーバック対象として扱われる。

[0061] (その他の実施形態)

上述の実施形態において、4ステップのCBRAプロシーダを想定しているが、図11に示すように、2ステップのCBRAプロシーダを想定してもよい。2ステップのCBRAプロシーダにおいて、UE100は、MSG1及びMSG3をまとめてMSG_Aとして基地局200に送信し、基地局200は、MSG2及びMSG4をまとめてMSG_BとしてUE100に送信する。2ステップのCBRAプロシーダにおいて、基地局200は、MSG_Aで送られたUE_contention_resolution_ID (UL-CCCH-SDU)をMSG_Bでエコーバックする。そのため、基地局200 (通信部210)がUL-SCH上でUE100から受信するメッセージは、UE100から基地局200に送信されるMSG_A、具体的には、MSG_A中のUE_contention_resolution_ID (UL-CCCH-SDU)に相当する。エコーバックされる競合解決用の識別データは、基地局200からUE100に送信するMSG_B、具体的には、MSG_B中のUE_contention_resolution_MAC_CEに相当する。基地局200 (制御部230)は、MSG_A中のメッセージが所定フォーマットに準拠している場合、当該メッセージのエコーバック処理を伴うMSG_B送信を行う。これに対し、MSG_A中のメッセージが所定フォーマットに準拠していない場合、基地局200 (制御部230)は、MSG_B送信を行わないように制御する。これにより、2ステップCBRAプロシーダにおける脆弱性の問題を解決できる。

- [0062] 上述の実施形態におけるステップは、必ずしもフロー図又はシーケンス図に記載された順序に沿って時系列に実行されなくてよい。例えば、動作におけるステップは、フロー図又はシーケンス図として記載した順序と異なる順序で実行されても、並列的に実行されてもよい。また、動作におけるステップの一部が削除されてもよく、さらなるステップが処理に追加されてもよい。さらに、上述の各動作フローは、別個独立に実施する場合に限らず、2以上の動作フローを組み合わせることで実施可能である。例えば、1つの動作フローの一部のステップを他の動作フローに追加してもよいし、1つの動作フローの一部のステップを他の動作フローの一部のステップと置換してもよい。
- [0063] 上述の実施形態において、基地局200は、複数のユニットを含んでもよい。複数のユニットは、プロトコルスタックに含まれる上位レイヤ（higher layer）をホストする第1のユニットと、プロトコルスタックに含まれる下位レイヤ（lower layer）をホストする第2のユニットとを含んでよい。上位レイヤは、RRCレイヤ、SDAPレイヤ及びPDCPレイヤを含んでよく、下位レイヤは、RLCレイヤ、MACレイヤ及びPHYレイヤを含んでよい。第1のユニットは、CU（central unit）であってよく、第2のユニットは、DU（Distributed Unit）であってよい。複数のユニットは、PHYレイヤの下位の処理を行う第3のユニットを含んでよい。第2のユニットは、PHYレイヤの上位の処理を行ってよい。第3のユニットは、RU（Radio Unit）であってよい。基地局200は、複数のユニットのうちの1つであってよく、複数のユニットのうちの他のユニットと接続されていてよい。また、基地局200は、IAB（Integrated Access and Backhaul）ドナー又はIABノードであってよい。
- [0064] 上述の実施形態において、移動通信システム1としてNRに基づく移動通信システムを例に挙げて説明した。しかしながら、移動通信システム1は、この例に限定されない。移動通信システム1は、LTE（Long Term Evolution）又は3GPP規格の他の世代システム（例えば、

第6世代)のいずれかのTSに準拠したシステムであってよい。基地局200は、LTEにおいてUE100へ向けたE-UTRA (Evolved Universal Terrestrial Radio Access) ユーザプレーン及び制御プレーンプロトコル終端を提供するeNBであってよい。移動通信システム1は、3GPP規格以外の規格のTSに準拠したシステムであってよい。

[0065] UE100又は基地局200が行う各処理をコンピュータに実行させるプログラムが提供されてもよい。プログラムは、コンピュータ読取り可能媒体に記録されていてもよい。コンピュータ読取り可能媒体を用いれば、コンピュータにプログラムをインストールすることが可能である。ここで、プログラムが記録されたコンピュータ読取り可能媒体は、非一過性の記録媒体であってもよい。非一過性の記録媒体は、特に限定されるものではないが、例えば、CD-ROMやDVD-ROM等の記録媒体であってもよい。また、UE100又は基地局200が行う各処理を実行する回路を集積化し、UE100又は基地局200の少なくとも一部を半導体集積回路(チップセット、SoC)として構成してもよい。

[0066] 上述の実施形態において、「送信する(transmit)」は、送信に使用されるプロトコルスタック内の少なくとも1つのレイヤの処理を行うことを意味してもよく、又は、無線又は有線で信号を物理的に送信することを意味してもよい。或いは、「送信する」は、上記少なくとも1つのレイヤの処理を行うことと、無線又は有線で信号を物理的に送信することとの組合せを意味してもよい。同様に、「受信する(receive)」は、受信に使用されるプロトコルスタック内の少なくとも1つのレイヤの処理を行うことを意味してもよく、又は、無線又は有線で信号を物理的に受信することを意味してもよい。或いは、「受信する」は、上記少なくとも1つのレイヤの処理を行うことと、無線又は有線で信号を物理的に受信することとの組合せを意味してもよい。同様に、「取得する(obtain/acquire)」は、記憶されている情報の中から情報を取得することを意味してもよく、他

のノードから受信した情報の中から情報を取得することを意味してもよく、又は、情報を生成することにより当該情報を取得することを意味してもよい。同様に、「～を含む (include)」及び「～を備える (comprise)」は、列挙する項目のみを含むことを意味せず、列挙する項目のみを含んでもよいし、列挙する項目に加えてさらなる項目を含んでもよいことを意味する。同様に、本開示において、「又は (or)」は、排他的論理和を意味せず、論理和を意味する。

[0067] 本開示は、実施例に準拠して記述されたが、本開示は当該実施例や構造に限定されるものではないと理解される。本開示は、様々な変形例や均等範囲内の変形をも包含する。加えて、様々な組み合わせや形態、さらには、それらに一要素のみ、それ以上、あるいはそれ以下、を含む他の組み合わせや形態をも、本開示の範疇や思想範囲に入るものである。

請求の範囲

- [請求項1] 移動通信システム（１）で用いる基地局（２００）であって、
競合ベースランダムアクセスプロシージャにおいてユーザ装置（１００）から上りリンク共有チャネル上で送信されるメッセージを受信する通信部（２１０）と、
前記受信したメッセージが所定フォーマットに準拠している場合、前記受信したメッセージを前記競合ベースランダムアクセスプロシージャにおける競合解決用の識別データとして前記ユーザ装置（１００）に送り返すエコーバック処理を行う制御部（２３０）と、を備え、
前記制御部（２３０）は、前記受信したメッセージが前記所定フォーマットに準拠していない場合、前記エコーバック処理を行わないように制御する、基地局（２００）。
- [請求項2] 前記制御部（２３０）は、前記受信したメッセージが前記所定フォーマットに準拠していない場合、前記エコーバック処理を行わずに、前記受信したメッセージを破棄する、請求項１に記載の基地局（２００）。
- [請求項3] 前記競合ベースランダムアクセスプロシージャは、４つのステップからなる４ステップランダムアクセスプロシージャであり、
前記メッセージは、前記４つのステップにおける３番目のステップにおいて前記ユーザ装置（１００）から前記基地局（２００）に送信されるMSG3であり、
前記競合解決用の識別データは、前記４つのステップにおける４番目のステップにおいて前記基地局（２００）から前記ユーザ装置（１００）に送信するMSG4である、請求項１又は２に記載の基地局（２００）。
- [請求項4] 前記制御部（２３０）は、
前記MSG3が前記所定フォーマットに準拠している場合、前記エコーバック処理を伴うMSG4送信を行うように制御し、

前記MSG3が前記所定フォーマットに準拠していない場合、前記MSG4送信を行わないように制御する、請求項3に記載の基地局(200)。

[請求項5] 前記競合ベースランダムアクセスプロシージャは、2つのステップからなる2ステップランダムアクセスプロシージャであり、

前記メッセージは、前記2つのステップにおける1番目のステップにおいて前記ユーザ装置(100)から前記基地局(200)に送信されるMSG Aであり、

前記競合解決用の識別データは、前記2つのステップにおける2番目のステップにおいて前記基地局(200)から前記ユーザ装置(100)に送信するMSG Bである、請求項1又は2に記載の基地局(200)。

[請求項6] 前記制御部(230)は、

前記MSG Aが前記所定フォーマットに準拠している場合、前記エコーバック処理を伴うMSG B送信を行うように制御し、

前記MSG Aが前記所定フォーマットに準拠していない場合、前記MSG B送信を行わないように制御する、請求項5に記載の基地局(200)。

[請求項7] 前記所定フォーマットは、前記移動通信システムの技術仕様において規定されたフォーマットである、請求項1乃至6のいずれか1項に記載の基地局(200)。

[請求項8] 前記所定フォーマットは、上りリンクの論理チャネルの一種である上りリンク共通制御チャネル(UL CCH)のサービスデータユニット(SDU)に準拠したフォーマットであり、

前記制御部(230)は、前記受信したメッセージが前記UL CCH SDUに準拠したフォーマットであるか否かを確認するフォーマット確認を行う、請求項1乃至7のいずれか1項に記載の基地局(200)。

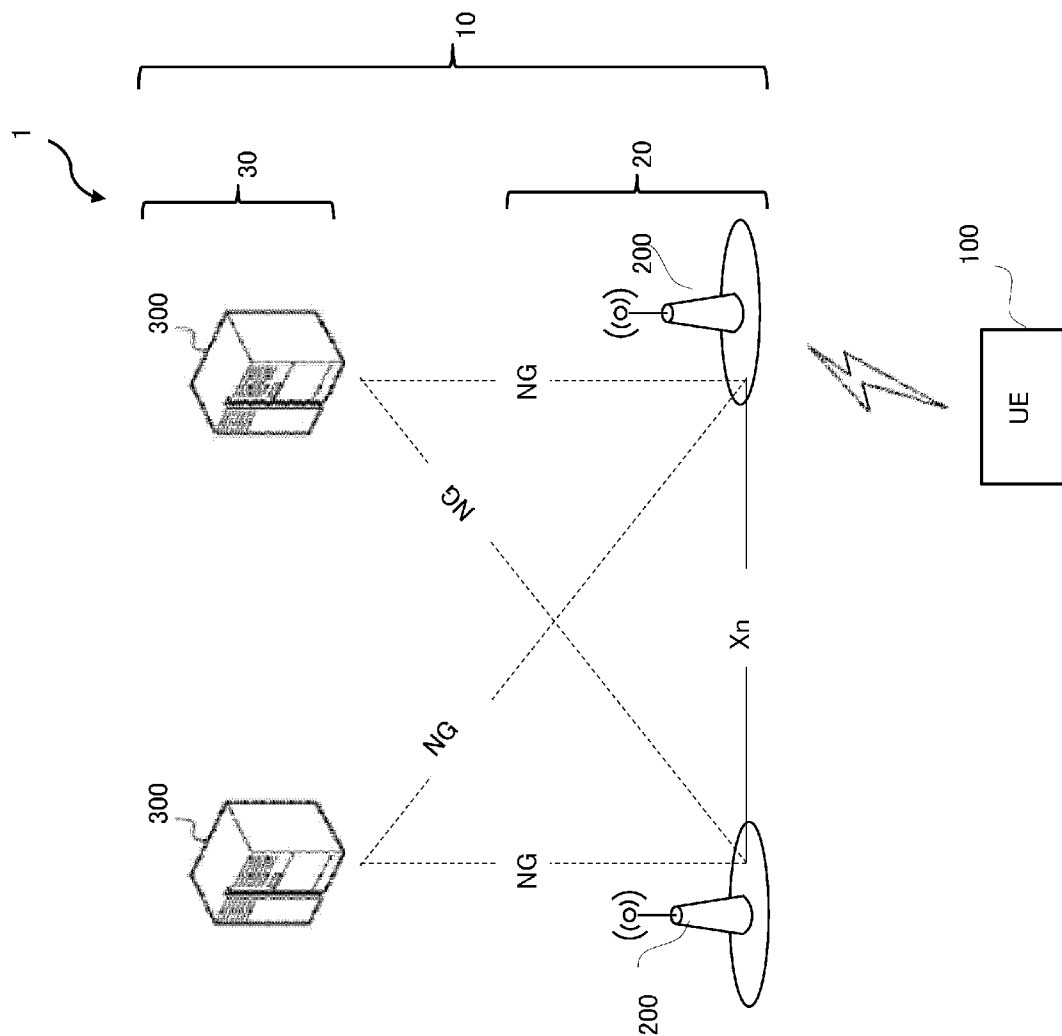
[請求項9] 移動通信システム（１）で用いる基地局（２００）における制御方法であって、

 競合ベースランダムアクセスプロシージャにおいてユーザ装置（１００）から上りリンク共有チャネル上で送信されるメッセージを受信するステップと、

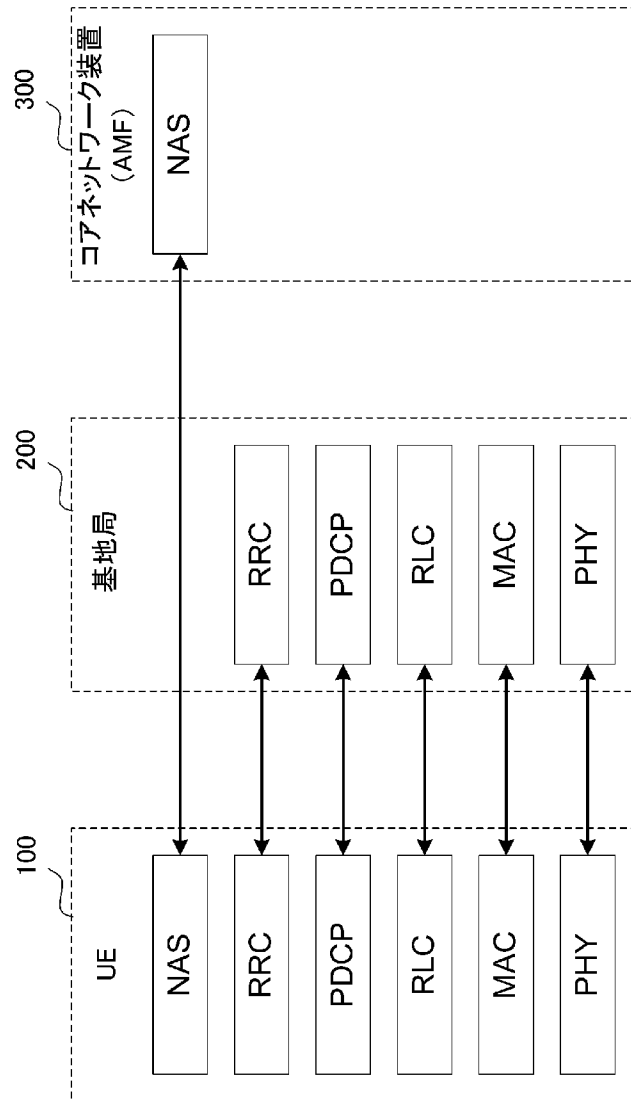
 前記受信したメッセージが所定フォーマットに準拠している場合、前記受信したメッセージを前記競合ベースランダムアクセスプロシージャにおける競合解決用の識別データとして前記ユーザ装置（１００）に送り返すエコーバック処理を行うステップと、

 前記受信したメッセージが前記所定フォーマットに準拠していない場合、前記エコーバック処理を行わないように制御するステップと、を有する制御方法。

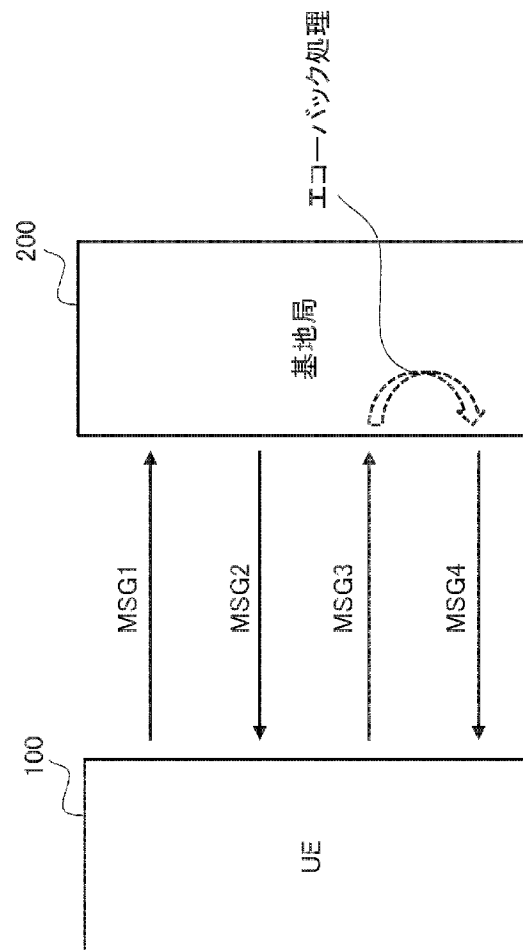
[図1]



[図2]



[図3]



[図4]

```
-- ASN1START
-- TAG-UL-CCCH-MESSAGE-START

UL-CCCH-Message ::=
    message
    {
        SEQUENCE {
            UL-CCCH-MessageType
        }

        UL-CCCH-MessageType ::=
            CHOICE {
                c1 CHOICE {
                    rrcSetupRequest      RRCSetupRequest,
                    rrcResumeRequest      RRCResumeRequest,
                    rrcReestablishmentRequest RRCReestablishmentRequest,
                    rrcSystemInfoRequest  RRCSystemInfoRequest
                },
                messageClassExtension    SEQUENCE {}
            }
    }

-- TAG-UL-CCCH-MESSAGE-STOP
-- ASN1STOP
```

[図5]

```
-- ASN1START
-- TAG-UL-CCCH1-MESSAGE-START

UL-CCCH1-Message ::=
    message
    {
        SEQUENCE {
            UL-CCCH1-MessageType
        }
    }

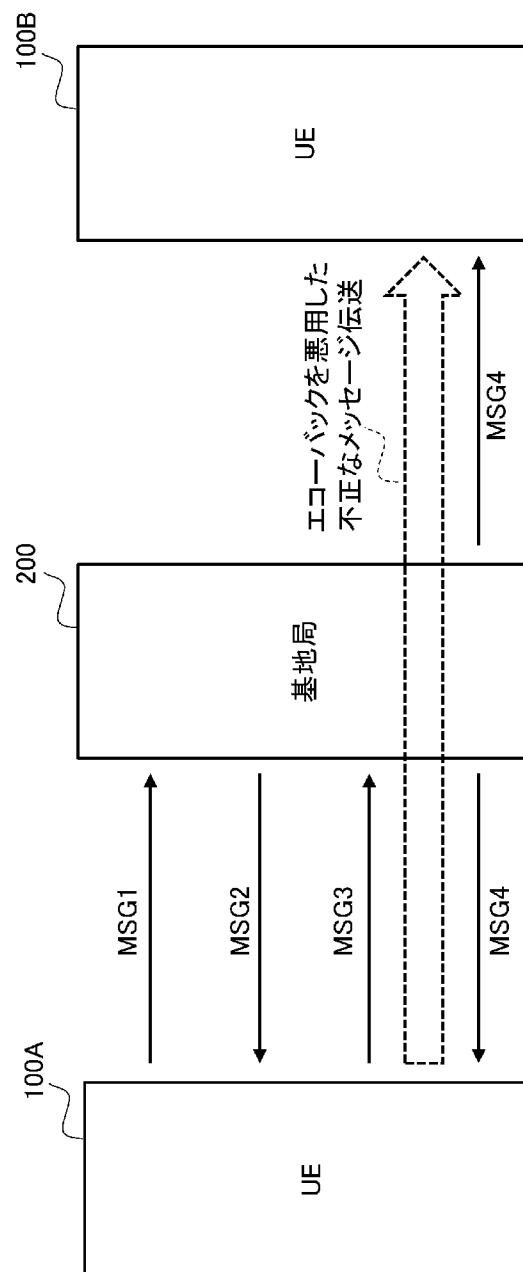
UL-CCCH1-MessageType ::=
    c1
    {
        rrcResumeRequest1
        spare3 NULL,
        spare2 NULL,
        spare1 NULL
    }
    },
    messageClassExtension SEQUENCE {}
}

-- TAG-UL-CCCH1-MESSAGE-STOP
-- ASN1STOP
```

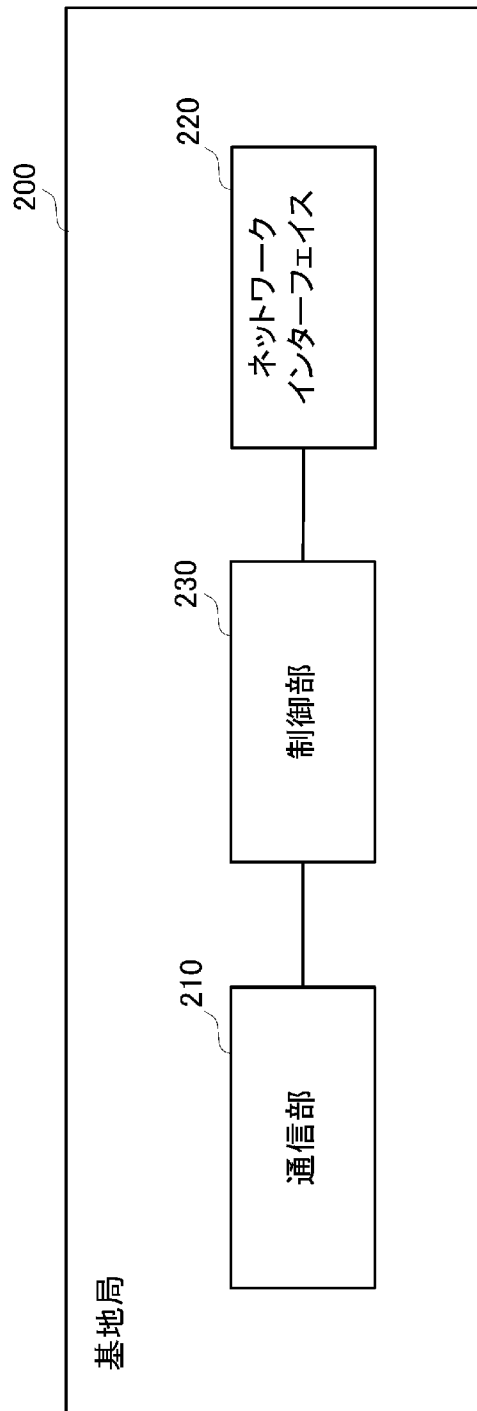
[図6]

	Oct 1
UE Contention Resolution Identity	
UE Contention Resolution Identity	Oct 2
UE Contention Resolution Identity	Oct 3
UE Contention Resolution Identity	Oct 4
UE Contention Resolution Identity	Oct 5
UE Contention Resolution Identity	Oct 6

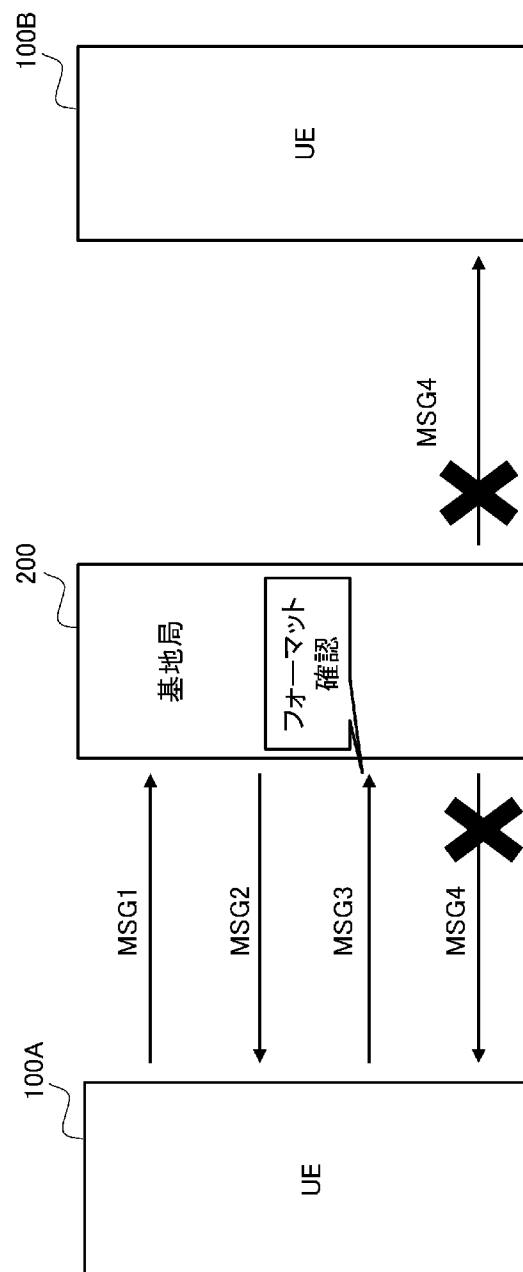
[図7]



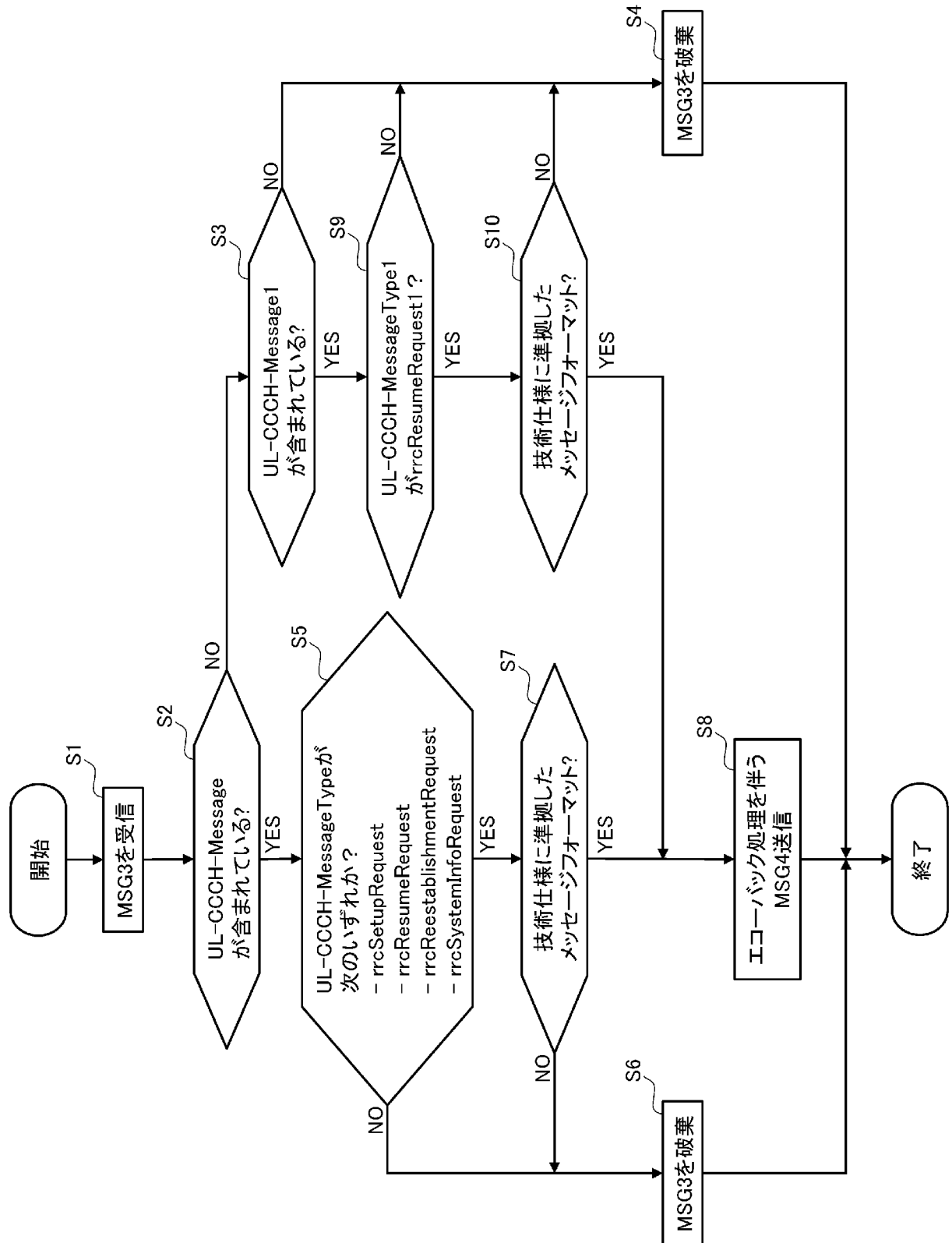
[図8]



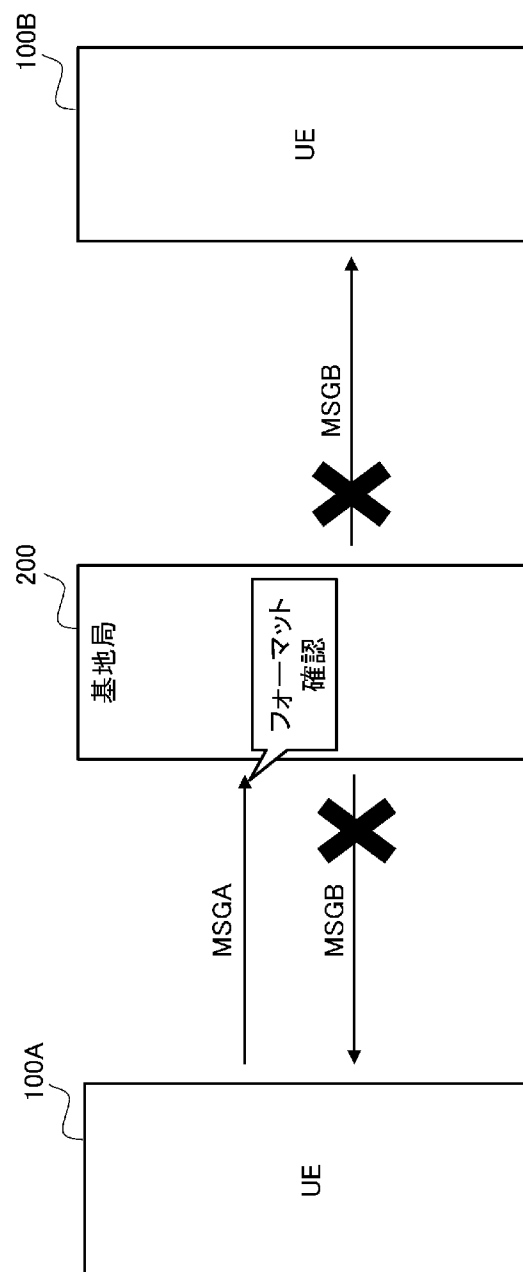
[図9]



[図10]



[図11]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2022/019896

A. CLASSIFICATION OF SUBJECT MATTER**H04W 74/08**(2009.01)i; **H04W 12/122**(2021.01)i

FI: H04W12/122; H04W74/08

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

Published examined utility model applications of Japan 1922-1996

Published unexamined utility model applications of Japan 1971-2022

Registered utility model specifications of Japan 1996-2022

Published registered utility model applications of Japan 1994-2022

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	GSMA. Stealth Pirating Attack by RACH Rebroadcast Overwriting (SPARROW) [online]. 3GPP TSG RAN WG2 #114-e R2-2106454. 12 May 2021, Internet <URL: https://www.3gpp.org/ftp/tsg_ran/WG2_RL2/TSGR2_114-e/Docs/R2-2106454.zip > particularly, section 2, fig. 1	1-9
Y	JP 2017-147610 A (AUTO NETWORK GIJUTSU KENKYUSHO KK) 24 August 2017 (2017-08-24) paragraphs [0003], [0007], [0059]-[0063]	1-9



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 July 2022

Date of mailing of the international search report

26 July 2022

Name and mailing address of the ISA/JP

Japan Patent Office (ISA/JP)

3-4-3 Kasumigaseki, Chiyoda-ku, Tokyo 100-8915

Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/JP2022/019896

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
JP 2017-147610 A	24 August 2017	(Family: none)	

A. 発明の属する分野の分類（国際特許分類（IPC）） H04W 74/08(2009.01)i; H04W 12/122(2021.01)i FI: H04W12/122; H04W74/08														
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（IPC）） 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														
<table border="0"> <tr> <td>日本国実用新案公報</td> <td>1922-1996年</td> </tr> <tr> <td>日本国公開実用新案公報</td> <td>1971-2022年</td> </tr> <tr> <td>日本国実用新案登録公報</td> <td>1996-2022年</td> </tr> <tr> <td>日本国登録実用新案公報</td> <td>1994-2022年</td> </tr> </table>			日本国実用新案公報	1922-1996年	日本国公開実用新案公報	1971-2022年	日本国実用新案登録公報	1996-2022年	日本国登録実用新案公報	1994-2022年				
日本国実用新案公報	1922-1996年													
日本国公開実用新案公報	1971-2022年													
日本国実用新案登録公報	1996-2022年													
日本国登録実用新案公報	1994-2022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	GSMA, Stealth Pirating Attack by RACH Rebroadcast Overwriting (SPARROW)[online], 3GPP TSG RAN WG2 #114-e R2-2106454, 2021.05.12, Internet<URL:https://www.3gpp.org/ftp/tsg_ran/WG2_RL2/TSGR2_114-e/Docs/R2-2106454.zip> 特に2節, 図1	1-9												
Y	JP 2017-147610 A (株式会社オートネットワーク技術研究所) 24.08.2017 (2017 - 08 - 24) 段落[0003], [0007], [0059]-[0063]	1-9												
☐ 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。														
<table border="0"> <tr> <td>* 引用文献のカテゴリー</td> <td>“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抵触するものではなく、発明の原理又は理論の理解のために引用するもの</td> </tr> <tr> <td>“A” 特に関連のある文献ではなく、一般的技术水準を示すもの</td> <td>“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</td> </tr> <tr> <td>“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</td> <td>“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</td> </tr> <tr> <td>“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）</td> <td>“&” 同一パテントファミリー文献</td> </tr> <tr> <td>“O” 口頭による開示、使用、展示等に言及する文献</td> <td></td> </tr> <tr> <td>“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</td> <td></td> </tr> </table>			* 引用文献のカテゴリー	“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抵触するものではなく、発明の原理又は理論の理解のために引用するもの	“A” 特に関連のある文献ではなく、一般的技术水準を示すもの	“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	“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	“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	“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）	“&” 同一パテントファミリー文献	“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	
* 引用文献のカテゴリー	“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抵触するものではなく、発明の原理又は理論の理解のために引用するもの													
“A” 特に関連のある文献ではなく、一般的技术水準を示すもの	“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													
“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	“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													
“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）	“&” 同一パテントファミリー文献													
“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														
国際調査を完了した日 12.07.2022	国際調査報告の発送日 26.07.2022													
名称及びあて先 日本国特許庁(ISA/JP) 〒100-8915 日本国 東京都千代田区霞が関三丁目4番3号	権限のある職員（特許庁審査官） 三枝 保裕 5J 6305 電話番号 03-3581-1101 内線 3534													

国際調査報告
パテントファミリーに関する情報

国際出願番号

PCT/JP2022/019896

引用文献	公表日	パテントファミリー文献	公表日
JP 2017-147610 A	24.08.2017	(ファミリーなし)	