(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4900007号
(P4900007)
(45)発行日　平成24年3月21日(2012.3.21)　(24)登録日　平成24年1月13日(2012.1.13)

(51)Int.Cl.　F I
H04W 72/04 (2009.01)　H04Q 7/00 543

請求項の数 6　(全 31 頁)

(21)出願番号　特願2007-104996(P2007-104996)
(22)出願日　平成19年4月12日(2007.4.12)
(65)公開番号　特開2008-263431(P2008-263431A)
(43)公開日　平成20年10月30日(2008.10.30)
審査請求日　平成22年1月19日(2010.1.19)

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100108187
弁理士　横山　淳一
(72)発明者　奥田　將人
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

審査官　角田　慎治

最終頁に続く

(54)【発明の名称】無線基地局、中継局、帯域割当方法

(57)【特許請求の範囲】
【請求項１】
無線端末と無線基地局との間に介在して、データの中継処理を行う中継局において、
該無線端末から受信した、暗号化されたデータを該無線基地局に送信する送信処理部と、該無線基地局の暗号復号化部により得られた該暗号化されたデータの復号結果に基いて生成される該無線端末からの帯域要求情報を受信する受信処理部と、受信した該帯域要求情報に基いて、該無線端末に対して帯域を割当てる帯域割当制御部、を備えたことを特徴とする中継局。
【請求項２】
請求項１に記載の中継局において、
前記無線端末から受信したデータに含まれる帯域要求を取得する受信処理部を備え、
前記帯域割当制御部は、取得した該帯域要求に基いて、該無線端末に対して帯域を割当てることを特徴とする中継局。
【請求項３】
請求項２に記載の中継局において、
前記帯域割当制御部は、前記暗号化されたデータの送信を行った後に、前記無線端末から受信したデータに含まれる帯域要求に基いて帯域割当てを行った場合に、前記無線基地局からの前記帯域要求情報に基く帯域割当てを規制する、ことを特徴とする中継局。
【請求項４】
中継局を介して無線端末と通信する無線基地局において、

該中継局から受信した暗号化されたデータの暗号の復号化処理を行う復号化処理部と、該復号化処理部により得られた、該無線端末からの帯域要求情報を該記中継局に送信する制御を行う制御部、
を備えることを特徴とする無線基地局。
【請求項５】
請求項４に記載の無線基地局において、
前記帯域要求情報は、前記暗号化されたデータの識別情報を含む、ことを特徴とする無線基地局。
【請求項６】
無線端末と無線基地局との間に介在して、データの中継処理を行う中継局における帯域割当て方法において、
該無線端末から受信した、暗号化されたデータを該無線基地局に送信し、該無線基地局の暗号復号化部により得られた該暗号化されたデータの復号結果に基いて生成される該無線端末からの帯域要求情報を受信し、受信した該帯域要求情報に基いて、該無線端末に対して帯域を割当てる、ことを特徴とする中継局における帯域割当て方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、無線通信を利用する無線基地局、中継局、帯域割当方法に関する。本発明は、例えば、ＩＥＥＥ８０２．１６に規定された無線通信システムに中継局を導入して得られる無線通信システムに用いると特に好適である。
【背景技術】
【０００２】
ＷＣＤＭＡ、ＣＤＭＡ２０００等のシステムを代表として現在、無線通信路を介して通信を行う無線通信システムが世界的に普及している。このような無線通信システムにおいては、複数の無線基地局が設置され、無線端末はいずれかの無線基地局を介して他の通信装置（通信端末）との間で通信を行う。無線端末は、通信を開始した無線基地局のサービスエリアのエッジに近づいた場合、隣接する他の無線基地局へハンドオーバすることで通信を継続することができる。
【０００３】
無線方式としては、例えば、符号分割多重、時分割多重、周波数多重、直交周波数分割多重（ＯＦＤＭ、ＯＦＤＭＡ等）の技術が採用され、１つの無線基地局に対して複数の無線端末が同時期に接続可能なことが一般的である。
【０００４】
しかし、無線基地局が無線通信可能なサービスエリア内であっても、エリアの境界に近い場所では、無線環境が良好でないために高速通信が困難であることが多い。また、エリアの内側であったとしても、ビル影等により無線信号の伝播を妨げる要因があり、無線基地局との良好な無線接続が困難なエリア（いわゆる不感地帯）が生じてしまうことがある。
【０００５】
そこで、無線基地局のサービスエリア内に中継局を配置し、無線端末と無線基地局とが中継局を介して無線通信できるようにする案が提案されている。
【０００６】
特に、８０２.１６ｊのタスクグループにおいて、そのような中継局（ＲＳ：Ｒｅｌａｙ　Ｓｔａｔｉｏｎ）の導入について、目下検討されている最中である。
【０００７】
上述した、ＩＥＥＥ８０２.１６に関する事項は、例えば次の非特許文献１、２に開示されている。
【非特許文献１】IEEE Std 802.16-2004
【非特許文献２】IEEE Std 802.16e-2005

【発明の開示】
【発明が解決しようとする課題】
【０００８】
先に説明した背景技術によれば、無線端末は無線基地局と直接又は中継局を介して無線通信を行うとことができることとなるが、無線端末への通信帯域の割当制御をどのように実施するのか検討する必要がある。その際、無線端末と無線基地局との間で暗号化されたデータは、中継局では復号（decipher）できないことも考慮する必要がある。また、不要な帯域割当を行わないように留意する必要がある。
【０００９】
従って、本発明の目的の１つは、中継局に帯域割当機能を付与することである。
【００１０】
また、他の目的の１つは、無線端末と無線基地局との間で暗号化されたデータの内容を中継局で把握可能とすることである。
【００１１】
また、他の目的の１つは、中継局が不要な帯域を行わないようにすることである。
【００１２】
尚、上記目的に限らず、後述する発明を実施するための最良の形態に示す各構成により導かれる効果であって、従来の技術によっては得られない効果を奏することも本発明の他の目的の１つとして位置付けることができる。
【課題を解決するための手段】
【００１３】
（１）本発明では、無線端末と無線基地局との間に介在して、データの中継処理を行う中継局において、該無線端末から受信したデータに含まれる帯域要求を取得する受信処理部と、取得した該帯域要求に基いて、該無線端末に対して帯域を割当てる帯域割当制御部、を備えたことを特徴とする中継局を用いる。
（２）本発明では、無線端末と無線基地局との間に介在して、データの中継処理を行う中継局において、該無線端末から受信した、暗号化されたデータを該無線基地局に送信する送信処理部と、該無線基地局の暗号復号化部により得られた該暗号化されたデータの復号結果に基いて生成される該無線端末からの帯域要求情報を受信する受信処理部と、
受信した該帯域要求情報に基いて、該無線端末に対して帯域を割当てる帯域割当制御部、
を備えたことを特徴とする中継局を用いる。
（３）好ましくは、更に、前記無線端末から受信したデータに含まれる帯域要求を取得する受信処理部を備え、前記帯域割当制御部は、取得した該帯域要求に基いて、該無線端末に対して帯域を割当てる。
（４）好ましくは、前記帯域割当制御部は、前記暗号化されたデータの送信を行った後に、前記無線端末から受信したデータに含まれる帯域要求に基いて帯域割当てを行った場合に、前記無線基地局からの前記帯域要求情報に基く帯域割当てを規制する。
（５）本発明では、中継局を介して無線端末と通信する無線基地局において、
該中継局から受信した暗号化されたデータの暗号の復号化処理を行う復号化処理部と、
該復号化処理部により得られた、該無線端末からの帯域要求情報を該記中継局に送信する制御を行う制御部、を備えることを特徴とする無線基地局を用いる。
（６）好ましくは、前記帯域要求情報は、前記暗号化されたデータの識別情報を含む。
（７）本発明では、無線端末と無線基地局との間に介在して、データの中継処理を行う中継局における帯域割当方法において、該無線端末から受信したデータに含まれる帯域要求を取得し、取得した該帯域要求に基いて、該無線端末に対して帯域を割当てる、ことを特徴とする中継局における帯域割当方法を用いる。
（８）本発明では、無線端末と無線基地局との間に介在して、データの中継処理を行う中継局における帯域割当て方法において、該無線端末から受信した、暗号化されたデータを該無線基地局に送信し、該無線基地局の暗号復号化部により得られた該暗号化されたデー

タの復号結果に基いて生成される該無線端末からの帯域要求情報を受信し、受信した該帯域要求情報に基いて、該無線端末に対して帯域を割当てる、ことを特徴とする中継局における帯域割当て方法を用いる。
（９）本発明では、無線端末と無線基地局との間に介在して、データの中継処理を行う中継局において、該無線端末から受信したデータが特定のコネクションに属しており、該データに含まれるデータ種別が所定の種別に属することを検出した場合に、該無線端末に所定の帯域を割当てる帯域割当制御部、を備えたことを特徴とする中継局を用いる。
（１０）本発明では、無線端末と無線基地局との間に介在して、データの中継処理を行う中継局における帯域割当て方法において、該無線端末から受信したデータが特定のコネクションに属しており、該データに含まれるデータ種別が所定の種別に属することを検出した場合に、該無線端末に所定の帯域を割当てる、を備えたことを特徴とする中継局における帯域割当て方法を用いる。
【発明の効果】
【００１４】
本発明によれば、中継局に帯域割当機能を付与することができる。
【００１５】
また、本発明によれば、無線端末と無線基地局との間で暗号化されたデータの内容を中継局で把握可能とすることができる。
【００１６】
また、本発明によれば、中継局が不要な帯域割当を行わないようにすることができる。
【００１７】
また、本発明によれば、中継局により、適正な帯域割当制御を行うことができる。
【発明を実施するための最良の形態】
【００１８】
以下、図面を用いながら、本発明の実施の形態について説明する。便宜上別個の実施例として説明するが、各実施例を組み合わせることで、組み合わせの効果を得て、更に、有用性を高めることもできることはいうまでもない。
【００１９】
尚、以下、無線通信システムとしてＷｉＭＡＸを例に挙げて説明するが、他の移動無線通信システムにも適用できる。
〔ａ〕第１実施形態の説明
まず、中継局が、単にデータパケットを転送制御する例について説明する。データパケットの暗号化(cipher)、暗号化の復号化(decipher)は無線端末（Ｔ、ＭＳと称することがある）と無線基地局（ＢＳ）間で行うこととする。
【００２０】
図１は、無線基地局、無線端末間で送受信されるデータの例としてのＭＡＣ　ＰＤＵを示す。
【００２１】
IP（Internet Protocol）パケット等のユーザデータは、サブヘッダが付与される。そして、サブヘッダおよびユーザデータ部について暗号化処理が施される。このとき、暗号化の鍵の一部として用いるパケット番号（Packet Number）やデータの完全性を担保するためのICV (Integrity Check Value)が付与される。パケット番号は、例えば無線端末（無線基地局）から送信されるパケットに順に付される番号であり、順に値が増加する。ＩＣＶは、暗号化前のサブヘッダ、ユーザデータに基いて、ハッシュ演算（一方向性関数を用いた演算）を行って得られる演算結果（ハッシュ値）である。データパケットの受信側は、同様に、ハッシュ演算を行って同じハッシュ値が得られるか否かでデータ改ざんの可能性をチェックすることができる。尚、パケット番号は暗号化されないが、ＩＣＶはサブヘッダ、ユーザデータと共に暗号化される。
【００２２】
さて、暗号化されたサブヘッダ、ユーザデータには、更に、MACヘッダおよびCRCが付与

されて、MAC-PDUを構成する。MACヘッダは、コネクションID (CID)や、ペイロード内のサブヘッダの種類を示すTypeビットなどを含む。CRCはMACパケットのＭＡＣヘッダから暗号化されたペイロードを範囲としてＣＲＣ演算を行った結果であり、受信側では、同様にＣＲＣ演算を行い、ビット誤りが発生したか否かを検出することができる。即ちＣＲＣを用いて誤り検出を行うことができる。

【００２３】

なお、暗号化の適用有無は、コネクション毎に設定可能であり、暗号化無しのコネクションの場合、Packet NumberおよびICVは省略される。

【００２４】

図２は、図１におけるＭＡＣヘッダの内容を詳細に示す。

【００２５】

図２において、ＭＡＣヘッダ(Generic MAC Header （GMH）とも呼ぶ)は、ＨＴ、ＥＣ、Ｔｙｐｅ、Ｒｓｖ、ＣＩ、ＥＫＳ、Ｒｓｖ、ＬＥＮ、ＣＩＤ、ＨＣＳフィールドを有する。尚、括弧書きの中は、ビット数の例を示す。

【００２６】

図３に、図２におけるＭＡＣヘッダの各フィールドの説明を示す。

【００２７】

ＨＴ（Header Type）は、ＭＡＣヘッダの種類を示し、０は、Generic MACヘッダであることを示し、１は、帯域（bandwidth）要求ヘッダ（ペイロード無しで、例えば、ＭＡＣヘッダとＣＲＣからなる）を示す。

【００２８】

ＥＣ（Encryption control）は、ペイロード（サブヘッダ、ユーザデータ等）についての暗号化制御（暗号化有り、無し）を示し、０は、ペイロードを暗号化していないこと、１は、ペイロードを暗号化していることを示す。

【００２９】

ＣＩは、ＣＲＣインジケータ（ＣＲＣの有無）を示し、１は、ＣＲＣを含み、０は、ＣＲＣを含まないことを示す。

【００３０】

ＥＫＳは、暗号鍵シーケンス（Encryption Key Sequence）を示し、トラフィック暗号鍵（ＴＥＫ）の識別情報（インデックス）を示す。尚、このフィールドは、ＥＣ＝１である場合に有効となる。基地局および無線端末は、セキュリティ強度を維持するために、ＴＥＫに有効期限を設け、有効期限前に新しいＴＥＫの交換をする。そのため、基地局および無線端末は、同時に新旧２つのＴＥＫを共有することがある。ＥＫＳはペイロードの暗号化に使用しているＴＥＫの識別情報である。

【００３１】

ＬＥＮは、ＰＤＵ長（Generic MAC Header、ＣＲＣ含む）を示す。

【００３２】

ＣＩＤは、接続識別子（Connection ID）を示し、無線端末と基地局との間の通信接続の識別のために用いられる。

【００３３】

ＨＣＳは、ヘッダチェックシーケンス（Header Check Sequence）を示し、ヘッダのエラー検出に用いられる。すなわち、ＨＣＳを除く５バイトを生成多項式(D^8+D^2+D+1)で除算した結果をＨＣＳとしてヘッダに挿入する。受信側では、ＨＣＳを含むヘッダ全体を上記生成多項式で除算し、あまりが０以外の場合、ヘッダ中にビット誤りが存在することを検出することができる。

【００３４】

Ｔｙｐｅは、サブヘッダ種別を示し、＃５は、メッシュサブヘッダ(Mesh Subheader)、＃４は、再送制御に関するフィードバックであることを示すＡＲＱフィードバックサブヘッダ、＃３は、拡張タイプ(Extended type)、＃２は、断片化サブヘッダ(Fragmentation Subheader)、＃１は、パッキングサブヘッダ(Packing Su

bheader)、＃０は、ＤＬの場合は、無線端末からの高速なフィードバック情報であることを示す高速フィードバックサブヘッダ(Fast Feedback Subdeader)、ＵＬの場合は、許可管理サブヘッダ(Grant Management Subheader)をそれぞれ示す。

【００３５】

メッシュサブヘッダは、基地局と無線端末が1対多で接続する木構造の接続形態ではなく、各端末が相互に接続可能な接続形態で通信するときに用いられるサブヘッダである。

【００３６】

断片化サブヘッダは、ＩＰパケット等のユーザデータを分割し、複数のＭＡＣ－ＰＤＵで転送するときに各ＭＡＣ－ＰＤＵに付与するサブヘッダで、シーケンス番号等を含み、受信側で元のユーザデータを再構成できるようにするために用いられる。

【００３７】

パッキングサブヘッダは、ＩＰパケット等のユーザデータを複数結合し、１つのＭＡＣ－ＰＤＵで転送するときに、各ユーザデータに付与するサブヘッダで、シーケンス番号を含む。

【００３８】

拡張タイプは、上記断片化サブヘッダやパッキングサブヘッダに含まれるシーケンス番号のビット数を規定する。すなわち、本ビットがセットされていると、１１ビットのシーケンス番号、セットされていなければ、３ビットのシーケンス番号が使われることを示す。

【００３９】

ここで、許可管理サブヘッダ(Grant Management Subheader)について更に詳しく説明しておく。

【００４０】

許可管理サブヘッダは、ＣＩＤの品質クラス（QoSクラス）により意味が異なる。ＣＩＤは、ＭＡＣヘッダに格納されたＣＩＤにより判別可能である。

【００４１】

尚、品質クラス（QOS）は、無線端末、又は無線基地局が通信接続を形成する際に定まる。例えば、通信接続を形成する際に送信されるＤＳＡ－ＲＥＱ又はＤＳＡ－ＲＳＰにおいて、ＣＩＤとともにＱＯＳクラスを指定することで、その通信接続がどのＱＯＳクラスに属するか定まる。従って、ＣＩＤとＱＯＳクラスの対応づけが以降可能となる。

【００４２】

ＱＯＳクラスの例

・UGS (Unsolicited Grant Service)コネクション

このQoSクラスに属する通信接続に対しては、無線端末が帯域要求をしなくとも、所定（固定）の帯域幅が定期的に割当てられる。このＱｏＳクラスは、一定量の帯域が定期的に割当てられるので、音声等の固定レートの通信に適している。なお、無線端末は、必要に応じて、帯域を要求しても良い。

・ertPS (Extended Real-Time Polling Service)コネクション

このQoSクラスに属する通信接続に対しても、無線端末が帯域要求をしなくとも、定期的に帯域が割当てられるが、割当てられる帯域量は、無線端末からのExtended Piggyback Requestにより変更可能である。このＱｏＳクラスは、帯域が割り当てられる周期は一定だが、一度に割り当てられる帯域量は可変にできる。従って、無音圧縮などをサポートする音声通話等に適している。

・Others (rtPS/nrtPS/BE)コネクション

他のQoSクラスである。

【００４３】

rtPS (Real-Time Polling Service)に属する通信接続に対して、基地局は、比較的短い周期でポーリング(後述する帯域要求ヘッダを送信できるだけの帯域の割り当て)を行う。nrtPS (Non-real-time Polling Service)に属する通信接続に対しても、rtPSと同様に、基地局がポーリングを行うが、その周期はrtPSよりも長くてよい。

【００４４】
図４は、許可管理サブヘッダ(Grant Management Subheader)のフォーマットの詳細を示す。
【００４５】
ＵＧＳ(Unsolicited Grant Service)コネクションの場合は、許可管理サブヘッダは、ＳＩ、ＰＭ、ＦＬＩ、ＦＬ、Ｒｓｖｄを含む。尚、括弧内の数字は、ビット数を示す。
【００４６】
ｅｒｔＰＳ（Extended Real-Time Polling Serveice）コネクションの場合は、許可管理サブヘッダは、拡張ピギーバック要求（Extended Piggyback Request）、ＦＬＩ、ＦＬを含む。
【００４７】
他のコネクション(rtPS/nrtPS/BE)コネクションの場合は、ピギーバック要求を含む。
【００４８】
図５に、許可管理サブヘッダのフィールドの詳細な説明を示す。
【００４９】
ＳＩは、スリップインジケータ（Slip Indicator）を示し、０は、アクション無し、１は、ＵＧＳクラスの送信キューが閾値を越えたことを示す。ＵＧＳクラスは固定レートのサービスであるが、同レートはＤＳＡ－ＲＥＱ／ＲＳＰを用いたコネクション設定時に基地局と無線端末で共有する。しかしながら、例えば、100kbpsと設定しても、無線端末と基地局のクロック精度のズレから無線端末に送信すべきデータがキューに蓄積していくことがある。そのような場合に、このＳＩビットを用いて、無線端末は基地局に多めの帯域を割当てることを要求することができる。
【００５０】
ＰＭは、ポーリング要求(Poll me)を示し、０でアクション無し、１で、他のＣＩＤのための帯域問い合わせを要求するものである。例えば、ＵＧＳクラスのコネクションとＢＥクラスのコネクションを設定しているとき、ＢＥクラスの送信データが発生したときに、ＰＭビットをセットすることにより、無線端末は帯域要求ヘッダを送信するための帯域の割当（ポーリング）を要求することができる。
【００５１】
ＦＬＩは、フレーム待ち時間（Frame Latency）を示し、現在のフレームに先行するフレームで、データ送信ができたフレームの数、待ち時間が１５より大きい場合はＦＬ＝１５とされる。例えば、ＶｏＩＰ(Voice over IP)トラフィックの場合、20ms毎にデータが発生する。ＶｏＩＰデータの発生タイミングとＵＧＳ用の帯域割当のタイミングにずれがあると、送信待ち遅延が大きくなってしまう。そこで、ＶｏＩＰトラフィックの発生直後にＵＧＳデータ用帯域割当があるように、ＦＬＩ／ＦＬで基地局に要求することができる。
【００５２】
ピギーバック要求は、無線端末による上り帯域幅（バイト数）要求。帯域幅の増加要求を示す。
【００５３】
一方、無線端末が帯域を要求する方法として、ペイロードを持たない帯域要求ヘッダ（Bandwidth Request Header）を用いることもできる。
【００５４】
図６は、帯域要求ヘッダを示す。
【００５５】
図のように、帯域要求ヘッダは、ＨＴ、ＥＣ、Ｔｙｐｅ、ＢＲ、ＣＩＤ、ＨＣＳを含む。ＨＴに１が設定され、ＥＣは０（暗号化無し）に設定されている点が特徴である。即ち、帯域要求ヘッダは、暗号化されていない。尚、この帯域要求ヘッダには、図１のＭＡＣＰＤＵに含まれていたペイロードは付加されない。

【００５６】
図７は、帯域要求ヘッダの各フィールドの説明を示す。
【００５７】
Ｔｙｐｅは、帯域要求の形式（種別）を示し、０００は、ＢＲにより要求する帯域幅が、増加を求める帯域幅(Incremental Bandwidth)であることを示し、００１は、ＢＲにより要求する帯域幅が、使用を求める総帯域幅（Aggregate Bandwidth）であることを示す。
【００５８】
ＢＲは、帯域要求(Bandwidth Request)であり、無線端末が要求する帯域幅のﾊﾞｲﾄ数を示す。尚、その際ＰＨＹのオーバヘッドを含めない。すなわち、誤り訂正符号のレートによって実際に送信されるビット数は異なり、また、使用する誤り訂正符号化レートは基地局が決定するため、無線端末はＰＨＹオーバーヘッドを含まないバイト数を要求する。
【００５９】
ＣＩＤは、接続識別子（Connection ID）であり、要求接続ＩＤを示す。
【００６０】
ＨＣＳは、ヘッダチェックシーケンス(Header Check Sequence)であり、ヘッダのエラー検出に使用される。
【００６１】
上述のように、無線端末から帯域の要求を行う場合に、ユーザデータと一緒に送ることができる許可管理サブヘッダ（第１の帯域要求）を送信する (Piggyback Bandwidth Request (PB-BR)と呼ぶ)方法と、ペイロード不要の帯域要求ヘッダ(Bandwidth Request Header)（第２の帯域要求）を送信する方法があることとなる。尚、帯域要求ヘッダは暗号化されずに送信され、許可管理サブヘッダは、ＭＡＣヘッダのＥＣの０、１に応じて、暗号化されていない許可管理サブヘッダを有するコネクションと、暗号化された許可管理サブヘッダを有するコネクションとが混在しうる状況となっている。
「システム構成」
このような帯域要求形態を１例として採用し、本実施例において用いるシステム構成、装置構成、処理手順等を図面を用いながら説明する。
【００６２】
図８は、第１実施例における無線通信システムの構成を示す。図において、１はルーティング装置、２は無線基地局（ＢＳ）、３は中継局（ＲＳ）、４は無線端末（Ｔ、ＭＳと記載することもある）をそれぞれ示す。尚、無線端末４としては、移動した利用に適したいわゆるＭＳ（Ｍｏｂｉｌｅ　Ｓｔａｔｉｏｎ）、固定的な利用に適した無線装置のいずれを用いることもできる。
【００６３】
無線端末４は、Ｔ４－１のように、無線基地局２－１のエリア内で無線基地局２－１と直接（中継局を介さずに）無線通信を行ったり、Ｔ４－２のように中継局３を介して無線基地局２－１と無線通信を行うことができる。
【００６４】
尚、通信経路に着目し、Ｔ４－１をＢＳ配下の無線端末、Ｔ４－２をＲＳ配下の無線端末と称することとする。
【００６５】
中継局３は、無線基地局２のサービスエリア内に１又はそれ以上設けられる。
【００６６】
無線基地局２は、ルーティング装置１と接続される。無線基地局２は、無線端末４からのデータを受信し、ルーティング装置１にそのデータを送出するとともに、逆に、ルーティング装置１から受信したデータを無線端末４に対して送信する制御を行う。ルーティング装置１は、複数の無線基地局と接続され、無線基地局２から受信したデータを他のルーティング装置又は他の無線基地局に送出することで、送信宛先にデータが到達するように

ルーティングを行う。

【００６７】

好ましくは、無線基地局２は、データをパケット形式に変換してからルーティング装置に転送する。尚、ルーティング装置１からアクセス可能となるように、無線端末の位置登録エリア（複数の無線基地局で構成されるエリア毎における無線端末の在圏情報）、サービス形態等を記憶したデータベースを配置し、ルーティングの際に必要に応じてルーティング装置１がこれらの情報を取得可能とすることが望ましい。

「無線フレームフォーマット」

次に、無線基地局２－１、無線端末４－１、中継局３、無線端末４－２との間の無線フォーマットの例について説明することとする。

【００６８】

図９は、無線フレームフォーマットの例を示す。尚、ここでは、ＩＥＥＥ　Ｓｔｄ８０２．１６ｄ、ｅに対応した無線フレームフォーマットを例としてあげるが、これに限定されるものではない。

【００６９】

図において、Ｔｘ、Ｒｘはそれぞれ送信、受信を意味する。従って、ＢＳ２はプリアンブル（Ｐ）をフレームの先頭として、ＤＬ／ＵＬ　ＭＡＰ、下りバーストＴ４－１（無線端末４－１への送信データ）を順に送信し，さらにＲＳ３向けのＤＬ／ＵＬ　ＭＡＰ、ＭＭＲバースト１（無線基地局２から中継局３への送信データ）をさらに送信している。ここで、ＭＳ向けとは別にＲＳ３向けにＭＡＰを送信しているのは、ＲＳ３もＢＳ２と同じタイミングでプリアンブル信号、ＤＬ／ＵＬ　ＭＡＰ、下りバーストＴ４－２をＴ４－２向けに送信しているため、ＢＳ３からの信号を同時に受信できないためである。

【００７０】

プリアンブルは、無線端末４が無線基地局２あるいは中継局３に同期することを可能とするために、無線基地局２あるいは中継局３のエリア内に送信される同期信号である。なお、中継局３の無線基地局２との同期を維持するために、無線基地局２は、中継局３向けのＭＡＰの前に、別の信号(図示していない)を送信しても良い。プリアンブル信号は、所定の既知パターンとして一定周期で送信される。尚、図において、ＵＰ　Ｌｉｎｋ　Ｓｕｂ－ｆｒａｍｅが終わると再び、プリアンブルの送信が送信され、Ｄｏｗｎ　Ｌｉｎｋ　Ｓｕｂ－ｆｒａｍｅの送信が開始する。

【００７１】

無線端末は、予め複数種類のプリアンブル信号のパターンを記憶しておき、各パターンのうち最も受信品質（例えば受信レベル）が良好なパターンに対応する無線基地局を通信先の無線基地局として選択することができる。

【００７２】

無線方式として、例えば、ＯＦＤＭ（ＯＦＤＭＡ含む）を利用する場合には、無線基地局は送信データを各サブキャリアに割り振って、複数のサブキャリアを用いて送信を行うが、プリアンブルを所定のパターンで各サブキャリアに割り振り送信することができる。無線端末は、その所定のサブキャリアの組み合わせを受信して既知のプリアンブル信号とのマッチングをとって、最も良好なプリアンブルを送信する無線基地局に対して同期をとることができる。

【００７３】

プリアンブルの送信に続くのは、ＤＬ／ＵＬ　ＭＡＰであり、無線端末４（４－１）に対して送信受信タイミング、送受信チャネル、無線通信方式（変調方式、符号化方式、符号化レート等）等の送受信動作を制御するための通信パラメータを通知するための制御データ（ＭＡＰデータ）を格納する領域である。中継局に対しては、プレアンブル直後のＤＬ／ＵＬ ＭＡＰとは異なるＭＡＰで同様の情報を通知する。

【００７４】

ＭＡＰデータは、ＤＬ　ＭＡＰデータと、ＵＬ　ＭＡＰデータを含み、ＤＬ　ＭＡＰデータは、下りサブフレームの構造を定義し、ＵＬ　ＭＡＰデータは上りサブレームの構造

を定義していると言える。

【００７５】

ＤＬ　ＭＡＰデータは、中継局３に対する送信データであるＭＭＲ１の領域（送信タイミング、送信チャネル（受信装置にとっての受信タイミング、受信チャネル））や無線通信方式を通知するための中継局用ＭＡＰデータ（ＲＢ）や、無線端末４－１に対する送信データであるＴ４－１の領域（送信タイミング、送信チャネル（受信装置にとっての受信タイミング、受信チャネル））や無線通信方式を通知するための無線端末用ＭＡＰデータ（Ｂ）を含む。尚、ＲＢ、Ｂはそれぞれ送信対象としての中継局、無線端末の識別情報（ＣＩＤ等）も含む。

【００７６】

一方、ＵＬ　ＭＡＰデータは、無線端末４－１からのバーストデータ、ＲＮＧ（Ｒａｎｇｉｎｇ信号）やＣＱＩを受信する領域（受信タイミング、受信チャネル（送信装置にとっての送信タイミング、送信チャネル）や無線通信方式を通知するためのＭＡＰデータ（Ｂ）や、中継局３からのＭＭＲ１を受信する領域（受信タイミング、受信チャネル（送信装置にとっての送信タイミング、送信チャネル）や無線通信方式を通知するためのＭＡＰデータ（ＲＢ）を含む。

【００７７】

ＲＮＧの領域で送信可能なＲａｎｇｉｎｇ信号は、複数パターン存在する。状況に対応するパターンのレンジング信号を用いて、状況に応じたレンジング処理を行う。

・初期用レンジング信号

網に帰属しようとする際に送信される信号で、この成功により無線端末は網に帰属することとなる。尚、この信号を受信した無線基地局２は、受信処理部において、受信タイミングずれ（位相ずれ）、受信周波数ずれ、必要な送信電力の増減情報を求め、Ａｄｊｕｓｔｍｅｎｔ情報（ＲＮＧ－ＲＳＰ（レンジング応答））として無線端末に送信する。

・定期用レンジング信号

網に帰属している無線端末が網に対して定期的に送信する信号である。

・帯域幅要求用レンジング信号

ＵＬの帯域幅要求を行う際に送信される信号であり、初期レンジングを完了させた無線端末等が、データの送信を希望する際に送信し、送信帯域を獲得する。即ち、帯域要求用のＲａｎｇｉｎｇ信号を送信し、帯域要求を行うための送信領域をＵＬ　ＭＡＰデータにより割り当てを受け、その送信領域で帯域要求ヘッダを送信する。そして、要求した帯域幅に見合った送信領域をＵＬ　ＭＡＰデータにより指定された無線端末４は、その指定領域で、データ送信を行う（図１０参照）。

・ハンドオーバ用レンジング信号

ハンドオーバ先の無線基地局に対して送信する信号であり、初期レンジング信号と同様の処理を行う。

【００７８】

ＣＱＩは、プリアンブル又はパイロット信号（下りバーストデータ等に含まれる既知信号）等の既知信号について無線端末が受信品質の測定を行った結果を報告するための送信期間を示し、無線基地局２は、ＢＳ配下の無線端末４－１から受信したＣＱＩに基づいて送信処理部を制御して変調方式（６４ＱＡＭ、１６ＱＡＭ等）、符号化方式（畳み込み符号化、ターボ符号化等）、符号化レート（１／２、１／３等）等の送信パラメータを変更する。即ち、受信品質が良好な場合は、伝送速度を上げる方向の制御を行い、受信品質が劣化した場合は、伝送速度を下げる方向の制御を行う。

【００７９】

また、中継局３も、無線基地局２と同様に、プリアンブル、ＤＬ／ＵＬ　ＭＡＰデータ及び配下の無線端末Ｔ４－２へのバーストデータの送信を行う。

【００８０】

ここで、中継局３が送信するＤＬ／ＵＬ　ＭＡＰは、中継局３が生成、制御できることとする。

【００８１】
中継局３配下の無線端末４－２は、中継局３から送信されるプリアンブルを用いて中継局３に同期をとる処理を行い、中継局３から送信されたＭＡＰデータを受信し、送受信タイミングを認識し、割り当てられた送受信タイミングで送受信を行う。また、ＵＬ　ＭＡＰデータで指定されたＲＮＧ、ＣＱＩの送信領域でＲａｎｇｉｎｇ信号、ＣＱＩの送信を行う。
【００８２】
即ち、状況に対応するパターンのＲａｎｇｉｇ信号を送信し、また、中継局３から受信したプリアンブル又はパイロット信号（下りバーストデータ等に含まれる既知信号）等の既知信号について受信品質の測定を行い、中継局３又は無線基地局２にＣＱＩとして報告する。報告された測定結果は、中継局３において、送信処理部の制御に用いられ、変調方式、符号化方式、符号化レート等の送信パラメータが同様に変更される。
【００８３】
尚、このフレーム構成例においては、ＢＳ２又はＲＳ３から、Ｔに対して送信が行われる期間、ＢＳ２からＲＳ３に対して送信が行われる期間は時間的に分離されている。
【００８４】
中継局３は、無線端末４－２から受信したデータを、ＭＭＲリンクを介して無線基地局２に送信し、逆に、ＭＭＲリンクを介して無線基地局２から受信したデータを無線端末４４－２に送信する。
「装置構成」
次に、無線基地局２の構成について図１１を用いて詳細に説明する。
【００８５】
図１１は無線基地局２の構成を示す図である。
【００８６】
図において、１０は中継局３、無線端末４との間で無線信号を送受信するためのアンテナ、１１はアンテナ１０を送受信系で共用するためのデュプレクサ、１２は受信部、１３は受信信号を復調する復調部、１４は復調した受信信号を復号する復号化部、１５は、無線端末４において暗号化されたデータ部分に対して暗号の復号化（decipher）処理を施して、復号結果を制御データ抽出部１６に与える復号化部(decipher unit)を示す。
【００８７】
制御データ抽出部１６は、制御データを抽出し帯域割り当てに関するデータを帯域割当制御部２０、制御部２７に与えるとともに、ユーザデータ等の他のデータをパケット生成部１７に転送する制御データ抽出部、１７は制御データ抽出部から転送されたデータをパケット化してＮＷインタフェース部１８に引き渡すパケット生成部を示す。
【００８８】
１８はルーティング装置１との間のインタフェース（ここではパケット通信を行うこととする）を形成するインタフェース部であり、１９はＮＷインタフェース部１８から受信したパケットデータに含まれるＩＰアドレスを識別し、ＩＰアドレスデータに基づき宛先無線端末４を特定（例えば、ＩＰアドレスデータとＣＩＤの対応を記憶しておき、対応するＣＩＤを取得）するとともに、ＣＩＤに対応するＱＯＳ（同様にＣＩＤに対応させて記憶しておく）情報を取得し、帯域割当制御部２０にＣＩＤ、ＱＯＳ情報を与えて帯域割り当て要求を行い、ＮＷインタフェース部１８から渡されたパケットデータをパケットバッファ部２１に格納する。
【００８９】
２０は、帯域割当制御部２０を示し、パケット識別部１９からの帯域割り当て要求、制御データ抽出部から取得した帯域割り当て要求（中継局３を介さずに無線端末４－１から受信した帯域割り当て要求）に基いて、ＭＡＰデータを生成してパケットバッファ部２１に与えることで、ＭＡＰデータの送信を実行させる。
【００９０】
２２はＰＤＵ生成部を示し、同期信号（プリアンブル）を基準として形成される無線フ

レームの各領域にＭＡＰデータ、送信データ（ＭＡＣ　ＰＤＵ）が格納されるよう生成し、暗号化部２３に送出する。即ち、ＰＤＵ生成部２２は、ユーザデータに対して、必要なＭＡＣヘッダ、パケット番号、サブヘッダ、ＩＣＶ、CRC等を付加して出力する。

【００９１】

暗号化部２３は、ＭＡＣヘッダのＥＣが１の場合に、ペイロード（サブヘッダ、ユーザデータ、ＩＣＶ）部分に暗号化処理を施し、その結果を符号化部２４に与える。尚、暗号化処理は、ＰＤＵ生成部２２が行うものとして、ヘッダ等を付加する前に実施することもできる。

【００９２】

２４は符号化部、２５は変調部、２６送信部をそれぞれ示し、順にＰＤＵデータを誤り訂正符号化等の符号化処理を施してから変調し、送信部２６からアンテナ１０を介して無線信号として送信する。

【００９３】

２７は制御部を示し、送信処理部、受信処理部を制御して送受信動作を制御する。

【００９４】

尚、制御部２７は、ＭＭＲリンクを介して中継局３に送信を希望するデータがある場合には、帯域割当制御部２０にＭＭＲリンクのバースト領域の確保を依頼するとともに、送信データ（制御データ等）をＰＤＵ生成部２２に与えることでＭＭＲリンクを介して送信させる。

【００９５】

一方、ＭＭＲリンクにより中継局３から送信されたデータ（制御データ等）を制御データ抽出部１６から取得し、その内容を解読し、必要な処理を行う。

【００９６】

また、制御部２７は、中継局３から暗号化されたデータ（例えば、ＭＡＣヘッダのＨＴが０、ＥＣが１に設定され、タイプフィールドに＃０が設定された場合の、サブヘッダ等）を受信する。そして、暗号復号化部１５がそのデータ（サブヘッダ）の暗号の復号化を行った結果を制御部２７は取得し、無線端末４からの帯域要求情報を生成する。無線端末４からの帯域要求情報は、無線端末４が帯域を求めるために要求した帯域（帯域幅）についての情報である。従って、無線基地局２は、中継局３に対して暗号の復号結果である無線端末４の帯域要求情報をＰＤＵ生成部２２に与えることで、ＭＭＲリンクを介して中継局３に送信する。その際、制御部２７は、帯域割当制御部２０に対して、データ送信領域の確保を依頼する。

【００９７】

図１２は中継局３の構成を示す図である。

【００９８】

図において、３０は無線基地局２、無線端末４との間で無線信号を送受信するためのアンテナ、３１はアンテナ１０を送受信で共用するためのデュプレクサ、３２は受信部、３３は受信信号を復調する復調部、３４は復調した受信信号を復号（誤り訂正復号化）する復号化部、３５は無線基地局２、無線端末から受信したデータのうち非暗号化データを抽出する抽出部を示す。

【００９９】

非暗号化データ抽出部３５は、例えば、無線端末から受信した暗号化されていないＭＡＣ　ＰＤＵ、暗号化されていないＭＡＣヘッダ（帯域要求ヘッダ（ＨＴ＝１、ＥＣ＝０））を抽出して帯域割当制御部３６に与える。尚、非暗号化データ抽出部３５は、暗号化されているか否かにかかわらず、受信データを制御部４１に与える（ＭＡＰデータ、無線端末から受信した暗号化されたＭＡＣ　ＰＤＵ、その他受信した制御データ、暗号化されていないＭＡＣ　ＰＤＵ、暗号化されていないＭＡＣヘッダ等）。

【０１００】

制御部４１は、無線端末から受信した暗号化されたＭＡＣ　ＰＤＵ、その他受信した制御データ、暗号化されていないＭＡＣ　ＰＤＵ、暗号化されていないＭＡＣヘッダを無

線基地局２に対して送信するようにバッファ部３７に与える。その際、無線端末４－２から帯域割り当て要求があったが、帯域割当制御部３６によって帯域の割り当て制御が可能な場合は、その割り当て要求については無線基地局２に送信しないように制御（例えばバッファ部３７にその要求を示すデータを与えない）したり、また、その要求は無効である旨無線基地局２に通知してもよい。

【０１０１】

帯域割当制御部３６は、暗号化されておらず、解析可能なＭＡＣ　ＰＤＵ、ＭＡＣヘッダ（帯域要求ヘッダ）を解析して、要求された帯域幅を確保したアップリンクＭＡＰデータを生成してバッファ３７に与えることで、そのＭＡＰデータを無線端末４に向けて送信させる。また、制御部４１から無線端末４に送信するＭＡＣ　ＰＤＵの情報を取得し、ダウンリンクＭＡＰデータを生成してバッファ３７に与え、そのＭＡＰデータおよびＭＡＣ　ＰＤＵを無線端末４に送信させる。

【０１０２】

３７はバッファ部を示し、制御部４１から与えられる送信データを格納し、帯域割当制御部３６から与えられるＭＡＰデータで定義された送信タイミングで、対応する送信データが送信されるように、格納した送信データを符号化部３８に出力する。尚、無線端末４－２に向けて送信する際には、プリアンブル、帯域割当制御部３６からのＭＡＰデータも送信データに加えて符号化部３８に与える。

【０１０３】

尚、無線端末４宛のデータは、無線基地局２と中継局３との間で形成された通信リンク（ＭＭＲリンク）を介して受信される。

【０１０４】

３８は符号化部、３９は変調部をそれぞれ示し、バッファ部３７からの送信データを符号化し、帯域割当制御部で取得した送信タイミング、チャネルでユーザデータの送信を行うように変調処理を施してから送信部４０に引き渡す。

【０１０５】

４０は送信部を示し、送信信号をアンテナ３０を介して無線端末４、無線基地局２宛に無線信号として送信する。

【０１０６】

４１は制御部を示し、無線基地局２から受信したＭＡＰデータを解析し取得した送受タイミング、チャネル、無線通信方式で無線基地局２との送受信を行うように、送信処理部、受信処理部を制御する。尚、無線端末４への下りバーストを送信する際には、帯域割当制御部３６で定義されたダウンリンクＭＡＰデータに従って、送信処理部を制御し、無線端末４からの上りバーストを受信する際には、帯域割当制御部３６で定義されたアップリンクＭＡＰデータに従って、受信処理部を制御する。

【０１０７】

図１３は無線端末４の構成を示す図である。

【０１０８】

図において、５０は中継局３、無線基地局２との間で無線信号を送受信するためのアンテナ、５１はアンテナ５０を送受信で共用するためのデュプレクサ、５２は受信部、５３は受信信号を復調する復調部、５４は復調した受信信号を復号する復号部、５５は、復号されたデータのうち、暗号化されたデータについて暗号の復号化処理を施す暗号復号化部を示す。

【０１０９】

制御データ抽出部５６は、制御データを抽出し、ＭＡＰデータであればＭＡＰ情報解析部６３に与え、他の制御データは、制御部６４へ引き渡し、ユーザデータ等はデータ処理部５７へ引き渡す。

【０１１０】

６３はＭＡＰ情報解析部を示し、無線基地局２又は中継局３から受信したＭＡＰデータ（下り通信パラメータ（Ｂ））を解析し、解析結果を制御部６４に与える。即ち、各種デ

ータの送受信タイミングを制御部６４に通知する。

【０１１１】

５７はデータ処理部を示し、受信データに含まれる各種データの表示処理、音声出力処理等を行う。また、データ処理部５７は、通信先の装置に対して送信を希望するユーザデータは、ＰＤＵバッファ部５８に与える。

【０１１２】

５８はＰＤＵバッファ部を示し、データ処理部５７からの送信データをＭＡＰデータ（通信パラメータ（Ｂ））により指定された送信タイミング、送信チャネル、無線通信方式で送信可能とすべく、格納したデータを暗号化部５９側に出力する。

【０１１３】

暗号化部５９は、サブヘッダ、ユーザデータ等のＭＡＣ　ＰＤＵのペイロード部分等に対して暗号化処理を施し、その結果を符号化部６０に与える。無線基地局２同様、ＰＤＵバッファ部５８が暗号化機能を備えることとし、暗号化してからＭＡＣヘッダ等を付加するようにしてもよい。

【０１１４】

６０は符号化部、６１は変調部を示し、ＰＤＵバッファ部５８からの送信データをＭＡＰ情報で指定された送信タイミング、送信チャネルで送信するように制御部６４の制御の下、送信データについて符号化、変調処理を実行する。

【０１１５】

送信部６２は、アンテナ５０を介して無線信号を送信する。

【０１１６】

制御部６４は、ＭＡＰデータに基づいて送信処理部、受信処理部の動作を制御する。

「帯域（幅）要求」

次に、無線端末４から上り送信帯域を要求する場合の処理について、上述したシステムをベースとして説明する。

【０１１７】

ここでは、中継局３は、無線端末４から帯域要求を受信した場合、中継局３の帯域割当制御部３６により帯域割り当て制御を実行する。例えば、中継局３から無線端末４－２へのＵＬ　ＭＡＰデータにより、無線端末４のデータ送信用の送信領域を定義して送信を許容する。これにより、無線基地局３に問い合わせずとも無線端末４の帯域割り当て要求に応じることができるため処理の遅延が抑制される。

【０１１８】

また、中継局３の帯域割当制御部３６は、無線端末４からの帯域割り当て要求が無線基地局２に問い合わせずに解析可能である場合は、帯域割り当て制御部３６により無線基地局２に問い合わせずに帯域割り当てを行う。

【０１１９】

しかし、中継局３の帯域割当制御部３６は、無線端末４からの帯域割り当て要求が無線基地局２に問い合わせずに解析可能でない場合（例えば、無線基地局２と無線端末４との間の暗号化通信により、帯域割り当て制御に必要とされるデータが暗号化されている場合）には、無線基地局２にその暗号化されたデータを転送し、無線基地局２によって暗号化の復号化行われることで得られた帯域割り当て制御に必要とされるデータ（無線端末４からの帯域要求情報）を、その無線基地局２から取得し、取得したデータに基いて、帯域割り当て制御部３６は、無線端末４に対して帯域割り当てを行う。

【０１２０】

これにより、無線基地局２と無線端末４との間の暗号化通信が行われ、中継局３独自では、暗号化の復号ができない場合でも復号結果を取得することができ、復号結果に基いて無線端末との間の無線通信の制御を行うことができる。

【０１２１】

図面を用いて更に詳細に説明する。

【０１２２】

図１４は、無線端末４からの帯域要求として、帯域要求ヘッダが用いられる場合のシーケンスを示す。

【０１２３】

先に説明したように、図６に示す帯域要求ヘッダは、暗号化されておらず、ペイロードも含まない簡素なメッセージとなっている。この帯域要求ヘッダは、例えば、初期レンジングを完了し、網にエントリした無線端末４がデータの送信を希望する場合に送信される。

【０１２４】

図１４に示すように、無線端末４（ＭＳ）は、帯域要求（帯域要求ヘッダ）を送信する。

【０１２５】

尚、この送信に先立って、帯域幅要求用レンジング信号を送信し、この帯域要求ヘッダの送信領域を確保することができる。即ち、中継局３は、帯域幅要求用レンジング信号の受信により、所定の帯域幅を確保すべくＵＬ　ＭＡＰデータを帯域割当制御部３６により生成して無線端末４（４－２）に送信するのである。

【０１２６】

但し、帯域幅要求用レンジング信号の送信は必須ではなく、ＱｏＳの種別によっては、無線端末４に対して、帯域要求（帯域要求ヘッダ）の送信を許容する送信領域を定期的に割り当てるため、その送信領域を用いて帯域要求（帯域要求ヘッダ）を送信すればよい。

【０１２７】

中継局３（RS）が無線端末４から帯域要求ヘッダを受信すると、中継局３の非暗号化データ抽出部３５は、ＥＣ＝０により暗号化対象外と認識し、帯域割当制御部３６に帯域要求ヘッダを与える。

【０１２８】

帯域割当制御部３６は、帯域要求ヘッダに含まれる情報（帯域要求種別（Ｔｙｐｅ）及び要求帯域幅（ＢＲ））を元に、無線端末４に対して割り当てるべき帯域を求め、その帯域を割り当てるべくＭＡＰデータを生成して、ＰＤＵバッファ部３７に与えて送信させる。ここで、無線端末４に対して割り当てる最大帯域は、例えば、既に要求されていた帯域がＡであって、帯域要求ヘッダのＴｙｐｅが０００（増加）で、ＢＲが、Ｂである場合、Ａ＋Ｂとする。また、無線端末４に対して割り当てる最大帯域は、例えば、既に要求されていた帯域がＡであって、帯域要求ヘッダのＴｙｐｅが００１（総帯域）で、ＢＲが、Ｂである場合、Ｂとする。

【０１２９】

中継局３は、無線端末４に割り当てる帯域幅以上の帯域（Ｘ）（好ましくは同じ帯域幅）を上りＭＭＲリンクに割り当てるように要求してもよい。例えば、制御部４１は、その帯域（Ｘ）の割り当てを要求する制御データを生成し、それを無線基地局２に対して送信するようにＰＤＵバッファ部３７に与えることとしてもよい。

【０１３０】

さて、無線端末４のＭＡＰ情報解析部６３は、中継局３から送信されるＭＡＰデータにより、ユーザデータの送信が許容された送信領域（送信タイミング、送信領域）を取得し、制御部６４に与える。

【０１３１】

制御部６４は、その送信領域で、ユーザデータ等の送信を行うように送信処理部を制御する。

【０１３２】

中継局３の制御部４１は、帯域割当制御部３６で、無線端末４に割り当てた送信領域を認識しているため、受信処理部を制御して、ユーザデータ等の送信データを受信する。

【０１３３】

中継局３の制御部４１は、受信したユーザデータをＰＤＵバッファ部３７に与えて、ＭＭＲリンクを介して送信させることで、無線基地局２にユーザデータを転送することがで

きる。

【０１３４】

尚、先に説明したように、ユーザデータの転送に必要とされる送信領域を確保するように無線基地局２に要求しておくことで、迅速にユーザデータの転送を行うことが可能となる。

【０１３５】

もちろん、制御部４１は、無線端末４からユーザデータを受信してから、上りＭＭＲリンクにおける送信領域を確保するように、無線基地局２に対する制御信号を生成し、送信する制御を行ってもよい。

【０１３６】

次に、無線端末４の暗号化部５９によって暗号化されることもあるサブヘッダを用いて、無線端末４から帯域要求を行う例について図１５を用いて説明する。尚、このサブヘッダは、図４に示したいずれかのサブヘッダであり、ＭＡＣヘッダのＴｙｐｅにおいて＃０が設定されたものである。但し、ＭＡＣヘッダのＥＣは０に設定され、サブヘッダは暗号化されていない。ＭＡＣ　ＰＤＵ全体は、図１に示したとおりである（ペイロードは、暗号化はされていない）。

【０１３７】

さて、無線端末４は、中継局３が解読できない暗号化処理が施されていないユーザデータ（省略してもよい）、中継局３が解読できない暗号化処理が施されていないサブヘッダ（図４の上から２番目、３番目のピギーバック帯域要求を含むサブヘッダ又は図４の一番上のサブヘッダ）を含むＭＡＣ　ＰＤＵを制御部６４の制御により送信する。このＭＡＣ　ＰＤＵの送信帯域は、定期的に割り当てられることもできるし、また、帯域幅要求用レンジング信号の送信により獲得してもよい。

【０１３８】

さて、中継局３の非暗号化処理部３５は、ＭＡＣヘッダ、サブヘッダ等を帯域割当制御部３６に与える。

【０１３９】

帯域割当制御部３６は、ＭＡＣヘッダで通知されたＣＩＤについて、サブヘッダのピギーバック帯域要求から求まる総帯域幅（好ましくは総帯域幅と同じ帯域幅、それ以上の帯域幅であってもよい）を算出し、その算出値を上限として対応する送信領域を無線端末４に割り当てる。即ち、帯域割当制御部３６はその送信帯域を定義したＵＬ　ＭＡＰデータを生成してバッファ部３７に与える。このとき、先と同様に、無線基地局２に対して後に転送すべきユーザデータの送信領域の要求を制御信号の送信により行ってもよい。

【０１４０】

さて、中継局３からＵＬ　ＭＡＰデータを受信した無線端末４は、指定された送信領域でユーザデータ等の送信を行うように、制御部６４は送信処理部を制御する。

【０１４１】

中継局３は、無線端末４から受信したユーザデータを先の説明同様、無線基地局２に転送する。

【０１４２】

無線端末４の暗号化部５９によって暗号化されたサブヘッダを用いて、無線端末４から帯域要求を行う例について図１６を用いて説明する。尚、このサブヘッダは、図４に示したいずれかのサブヘッダであり、ＭＡＣヘッダのＴｙｐｅにおいて＃０が設定されたものである。但し、ＭＡＣヘッダのＥＣは１に設定され、サブヘッダは暗号化されている。ＭＡＣ　ＰＤＵ全体は、図１に示したとおりである（ペイロードは、暗号化はされている）。

【０１４３】

さて、無線端末４は、中継局３が解読できない暗号化処理が施されたユーザデータ（省略してもよい）、サブヘッダ（図４の上から２番目、３番目のピギーバック帯域要求を含むサブヘッダ又は図４の一番上のサブヘッダ）を含むＭＡＣ　ＰＤＵを制御部６４の

制御により送信する。このＭＡＣ　ＰＤＵの送信帯域は、定期的に割り当てられることもできるし、また、帯域幅要求用レンジング信号の送信により獲得してもよい。

【０１４４】

さて、中継局３の非暗号化処理部３５は、ＥＣ＝１により、ペイロードが暗号化されているため、受信したＭＡＣ　ＰＤＵを制御部４１に与える。従って、この場合、帯域割当制御部３６は、無線基地局２に問い合わせることなく、帯域割り当て制御を実行するといった制御は行わない。

【０１４５】

中継局３は、暗号化されたペイロードを含むＭＡＣ　ＰＤＵをバッファ部３７に与え、上りＭＭＲリンクを介して無線基地局２に送信する。その際、無線基地局２に対して、ペイロードの暗号化の復号処理を行った結果（特に帯域要求に関するデータ）である無線端末４からの帯域要求情報を中継局３に対して返送するように要求するデータを付加して送信してもよい。

【０１４６】

無線基地局２は、暗号化されたペイロードを含むＭＡＣ　ＰＤＵを暗号復号化部１５で復号し、その復号結果を制御部２７に与える。無線基地局２は、受信タイミング（CID等）からＭＭＲリンクを介してＭＡＣ　ＰＤＵを受信したことから、直接受信したＭＡＣ　ＰＤＵでないことを識別することができる。尚、直接受信したＭＡＣ　ＰＤＵは、帯域割当制御部２０に与えることができる。

【０１４７】

さて、制御部２０は、暗号化の復号化処理が完了したＭＡＣ　ＰＤＵを取得するので、中継局３における帯域割り当て制御に必要なデータである無線端末４からの帯域要求情報を中継局３にＭＭＲリンクを介して返送する。ＭＡＣヘッダ内のＣＩＤ、暗号化を解いたサブヘッダを返送してもよいし、無線端末４により要求されている帯域幅（例えば、総帯域幅、増加帯域幅）を無線端末４からの帯域要求情報として返送してもよい。１例を図２１に示している。図２１の例では、Ｇｅｎｅｒｉｃ　ＭＡＣヘッダ、メッセージ種別（帯域幅が増加帯域幅か、総帯域幅かを示す）、ＣＩＤ、要求している帯域幅（帯域要求）を含むデータを返送することとなる。

【０１４８】

さて、ＭＭＲリンクを介して無線端末４からの帯域要求情報を取得した中継局３の制御部４１は、帯域割当制御部３６に対して無線端末４に対して割り当てるべき帯域幅とＣＩＤ等の帯域割り当てに必要とされる情報を与える。

【０１４９】

従って、帯域割当制御部３６は、与えられた情報に基いて、ＭＡＰデータを生成して、無線端末４に送信する。

【０１５０】

このとき、先と同様に、無線基地局２に対して後に転送すべきユーザデータの送信領域の要求を制御信号の送信により行ってもよい。

【０１５１】

さて、中継局３からＵＬ　ＭＡＰデータを受信した無線端末４は、指定された送信領域でユーザデータ等の送信を行うように、制御部６４は送信処理部を制御する。

【０１５２】

中継局３は、無線端末４から受信したユーザデータを先の説明同様、無線基地局２に転送する。

【０１５３】

図１７に、無線端末４からのＭＡＣ　ＰＤＵ、帯域要求ヘッダを受信した場合における中継局３の処理フローを示す。

【０１５４】

まず、中継局３は、無線端末４からデータを受信したか否か判定する。ここでＮｏであれば、最初の判定に戻る。

【０１５５】
一方Ｙｅｓの場合、ペイロードがあるか否か判定する。ここでＹｅｓであれば、帯域要求情報にピギーバック帯域要求が含まれるか否か判定する。ピギーバック帯域要求があるか否かの判定で、Ｎｏであれば受信データを無線基地局２に転送し、最初の判定に戻る。
【０１５６】
ピギーバック帯域要求があるか否かの判定で、Ｙｅｓであれば、ピギーバック帯域要求が暗号化されているかどうか判定する。
【０１５７】
暗号化されている場合、受信データを無線基地局２に転送する。
【０１５８】
一方、暗号化されていない場合は、帯域割当制御部３６は、ＣＩＤごとに管理して（記憶部に記憶）いる帯域要求管理テーブルの要求帯域値の更新（加算（Incrementalの場合、記憶値に要求帯域を加算して更新）、総計(Aggregate)の場合、記憶値を要求帯域におきかえて更新）を行う。尚、記憶部に記憶される帯域要求管理テーブルの例は、図２０に示している。無線端末４との接続の識別のためのＣＩＤに対応させて、要求帯域が管理されている（例えばﾊﾞｲﾄ単位）。
【０１５９】
要求帯域値の更新がなされた後、受信データは、無線基地局２に転送される。
【０１６０】
さて、ペイロードがあるかどうかの判定で、Ｎｏとなった場合は、帯域要求情報が有るがどうか判定する。ここでＮｏの場合は、受信データを無線基地局２に転送する。
【０１６１】
一方、Ｙｅｓの場合は、帯域要求ヘッダのＴｙｐｅが、総計(Aggregate)であるか否か判定する。
【０１６２】
Ｔｙｐｅが、総計(Aggregate)の場合は、帯域割当制御部３６は、ＣＩＤごとに管理して（記憶部に記憶）いる帯域要求管理テーブルの要求帯域値の更新（記憶値を要求帯域におきかえて更新）を行って、受信データを破棄する。ペイロードがないため、無線基地局２に対してユーザデータの転送を行う必要がないためである。
【０１６３】
Ｔｙｐｅが、加算（Incremental）の場合は、ＣＩＤごとに管理して（記憶部に記憶）いる帯域要求管理テーブルの要求帯域値の更新（記憶値に要求帯域を加算して更新）して受信データを破棄する。
【０１６４】
ここで、中継局３は、帯域要求管理テーブルの更新後、帯域要求ヘッダは廃棄するとしているが、別途無線基地局２にユーザデータ等の転送用の送信帯域を要求する。もちろん、無線端末４から受信した帯域要求ヘッダを無線基地局２に転送して、ＭＭＲの上り送信帯域を確保することもできる。
【０１６５】
ここでは、帯域要求を受信した場合の帯域要求管理テーブルの要求帯域値の更新について示しているが、中継局３が無線端末４に帯域を割当てた場合、対象ＣＩＤの帯域要求値は割り当てた分だけ減算される。
【０１６６】
図１８は、無線基地局２が中継局３からＭＡＣ　ＰＤＵを受信した場合の処理フローを示す。
【０１６７】
まず、中継局３からデータを受信したかどうか判定する。ここでＮｏの場合、最初の判定に戻る。
【０１６８】
一方Ｙｅｓの場合、受信したデータに帯域要求（ピギーバック帯域要求）が有るかどう

か判定する。

【０１６９】

ここで、有りと判定すると、帯域要求（ピギーバック帯域要求）が暗号化されているか否か判定し、暗号化されていない場合は、受信データのルーティング装置１への転送処理を行う。一方、暗号化されている場合は、暗号化された帯域要求（ピギーバック帯域要求）について施した暗号の復号化処理結果を無線端末４からの帯域要求情報として中継局３に返送する。

【０１７０】

図２１は、無線基地局２から中継局３に送信される無線端末による帯域要求情報の例を示している。Generic ＭＡＣヘッダに続き、メッセージ種別、帯域割当が必要なコネクションを表すCID、帯域要求量Bandwidth Request (バイト単位)が含まれる。

【０１７１】

メッセージ種別として、帯域増加として、帯域要求量を無線端末４が希望する帯域増加量とすることができる。また、メッセージ種別として、総帯域として、帯域要求量を無線端末４が希望する総帯域とすることができる。

【０１７２】

無線端末４による帯域要求情報を中継局３に送信すると、無線基地局２は、受信データをルーティング装置１へ転送する。

【０１７３】

図１９は、中継局３が無線基地局２から無線端末４の帯域要求情報（図２１）を受信した場合の処理フローをそれぞれ示す。

【０１７４】

中継局３は、無線基地局から無線端末４の帯域要求情報を受信すると、その情報に従って記憶部に記憶している帯域管理テーブル（図２０）を更新する。

【０１７５】

中継局３は、帯域要求管理テーブルで更新されて結果の値に基づいて、無線端末４に対して帯域の割当てをおこなう。即ち、更新値に対応する送信領域を定義したＵＬ　ＭＡＰを生成して、送信する。

〔ｂ〕第２実施形態の説明

次に、無線端末４が、ユーザデータ等の送信を行うための帯域を獲得するために、帯域要求（例えば、ピギーバック帯域要求(暗号化有り)の送信の後（直後）に帯域要求（帯域要求ヘッダ (Aggregate)）を送信した場合について説明する。

【０１７６】

中継局３は、無線端末４からピギーバック帯域要求(暗号化有り)により帯域の増加を要求された場合、その暗号を解くことができないので、無線基地局２に対してピギーバック帯域要求(暗号化有り)を転送する。

【０１７７】

その後、無線端末４は、帯域要求ヘッダの送信により総帯域を指定した帯域要求ヘッダの送信を行う。この送信は、定期的な帯域要求の送信タイミングであるために行われる場合や、送信したピギーバック帯域要求に対する応答がないために、再度送信帯域の獲得を求めるために行われることがあり得る。

【０１７８】

帯域要求ヘッダ（総帯域指定）は、暗号化されていないため、中継局３の帯域割当制御部３６は、無線端末４により要求された総帯域を解釈し、帯域要求ヘッダに含まれるＣＩＤに対応する帯域要求管理テーブルの帯域を総帯域値に更新し、無線端末４にその帯域を割り当てる。即ち、ＵＬ　ＭＡＰデータにより送信帯域を割り当てる。

【０１７９】

従って、無線端末４は、ＵＬ　ＭＡＰデータにより指定された送信帯域を用いてユーザデータを含むＭＡＣ　ＰＤＵを送信する。

【０１８０】
一方、ピギーバック帯域要求(暗号化有り)を受信した無線基地局２は、その暗号の復号化処理を復号化部１５で行い、その結果を制御部２７が取得する。
【０１８１】
制御部２７は、ピギーバック帯域要求に基づいて、無線端末４から要求されている帯域の増加量を検出し、帯域増加量を無線端末４の帯域要求情報として中継局３に送信する。即ち、帯域要求情報を下りＭＭＲリンクを介して中継局３に送信する。
【０１８２】
中継局３は、同様に帯域要求管理テーブルの帯域を増加量だけ加算することで更新し、更新後の帯域を無線端末４に割り当てる。
【０１８３】
しかし、無線端末４は、既に送信帯域を割り当てられ、ユーザデータ等を送信してしまっているため、この割り当ては無駄となることがある。
そこで、中継局３における処理フローを工夫する。フローは、図２３に示してあり、図１７に類似するため、相異点を説明する。
【０１８４】
図１７において、帯域要求にピギーバック帯域要求が有りと判断され、その要求が暗号化されていると判定した場合の処理が図２３では変更されている。
【０１８５】
即ち、帯域要求管理テーブルのパケット番号を受信したＭＡＣ　ＰＤＵのパケット番号に更新するとともに、未知帯域要求フラグを１にセットしてから受信データの転送を行う点が変更されている。未知帯域要求フラグ＝1は、中継局２が認識していない帯域要求を無線端末４が行っていることを表し、無線基地局２から無線端末４の帯域要求情報が転送されることを意味する。
【０１８６】
また、受信データに、ペイロードがなく、帯域要求ヘッダが総帯域を指定している場合に、帯域要求管理テーブルの要求帯域値を総帯域で置きかえるとともに、未知帯域フラグを０にセットする点が相異する。ここで、未知帯域要求フラグ＝０は、要求帯域が最新の値にセットされていることを表す。
【０１８７】
帯域要求管理テーブルの例は、図２５に示されており、未知帯域要求フラグとパケット番号との列が付加されている。
【０１８８】
無線基地局２が、中継局３からデータを受信したときの処理フローは、図１８と同様である。ただし、無線基地局２が中継局３に送信する無線端末４の帯域要求情報には、暗号化されたＭＡＣ　ＰＤＵに含まれるパケット番号が追加される（図２６参照）。
【０１８９】
図２４は、中継局３が、無線基地局２から無線端末４の帯域要求情報を受信した際の動作を示したフローである。
【０１９０】
中継局３は、無線基地局２から無線端末４からの帯域要求情報を受信したかどうか判定する。ここのＮｏの場合は、最初の判定に戻る。
【０１９１】
一方、Ｙｅｓの場合は、対応するＣＩＤのレコードにおいて、未知帯域要求フラグが０にセットされているか否か判定する。
【０１９２】
ここで、フラグが０であれば、既に、最新の無線端末４の要求帯域に応じて帯域割り当てを行っているため、無線端末４の帯域要求情報を破棄して最初の判定に戻る。
【０１９３】
一方、フラグが１であれば、帯域要求管理テーブルの要求帯域値の更新を行う。

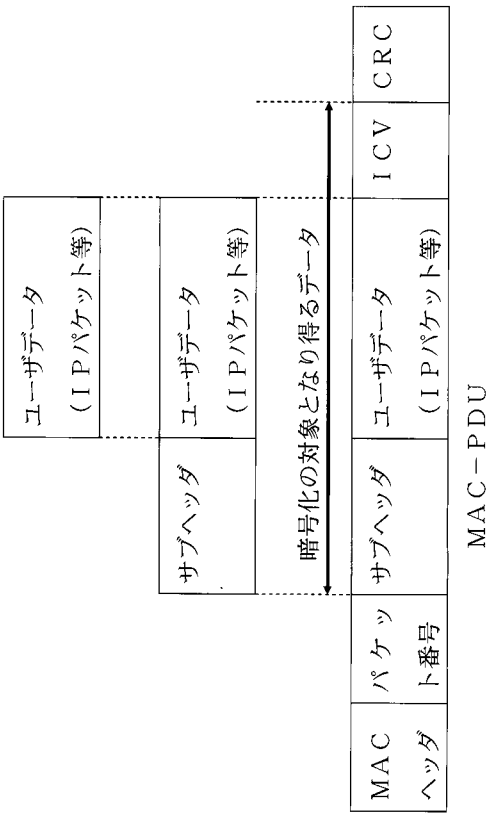
【０１９４】
そして、未知帯域要求フラグの設定値を維持するか、更新するかの処理を分けるべく、帯域要求管理テーブルのパケット番号が、無線基地局２から通知されたパケット番号より大きいかどうかを判定する。
【０１９５】
ここで、Ｙｅｓの場合は、未知帯域要求フラグをそのまま維持し、Ｎｏの場合は、帯域要求管理テーブルの未知帯域要求フラグを０に更新して、無線端末４の帯域要求情報を破棄する。尚、この例では、パケット番号を用いているが、その他の情報を用いることもできる。例えば、フレーム番号等の帯域要求が送信された順序関係の判定を可能とする情報を使用することもできる。

〔ｃ〕第３実施形態の説明
ＣＩＤがＵＧＳクラスのコネクションの場合、許可管理サブヘッダには、ピギーバック帯域要求は含まれず、ポーリング要求（Poll-Me Bit（ＰＭビット））が含まれる。ＰＭビットが含まれている場合、無線端末４が、帯域要求ヘッダを送信できるだけの帯域を割り当てればよい。
【０１９６】
この実施例では、中継局３の帯域割当制御部３６は、無線端末４に割り当てられたコネクション（ＣＩＤ）がどのＱＯＳクラスに属するか（UGSコネクションか他のコネクションか）を管理する。尚、コネクションがどのＱＯＳクラスに属するかは、無線端末４と無線基地局２との間で送受信されるデータを監視することにより取得することもできる。例えば、無線基地局２がＣＩＤと、対応するＱＯＳクラスを中継局３経由で無線端末４に通知する際に中継局３はその通知を取得し、ＣＩＤとＱＯＳクラスの対応テーブルを記憶部に記憶する。
【０１９７】
従って、図２７に示すように、中継局３は、無線端末４からデータを受信したかどうか判定し、Ｎｏの場合は最初の判定に戻る。
【０１９８】
一方、Ｙｅｓの場合は、ＣＩＤがＵＧＳクラスに該当するか否か判定する。この判定の際には、記憶部に記憶したＣＩＤとＱＯＳクラスの対応テーブルを参照し、無線端末４からの受信データに含まれるＣＩＤに対応するＱＯＳクラスを検索する。
【０１９９】
検索の結果、ＵＧＳクラスでなければ、受信データを無線基地局２に転送する。
【０２００】
検索の結果、ＵＧＳクラスであれば、中継局３において解読ができない暗号化処理が施されていないＭＡＣヘッダのＴｙｐｅフィールドを解析し、＃０であるか否かを判定する。即ち、サブヘッダの種別が、許可管理サブヘッダであるか否か判定する。
【０２０１】
ここで、Ｎｏの場合は、受信データを無線基地局２に転送する。
【０２０２】
一方、Ｙｅｓの場合は、無線端末４に、帯域要求ヘッダを送信できるだけの所定の帯域を割り当て、受信データを無線基地局に転送する。
【０２０３】
これにより、サブヘッダ自体は、暗号化されており、解読できないかもしれないが、ＣＩＤによる品質クラスの検出及びＭＡＣヘッダのサブヘッダの種類情報により、無線端末４が所定の帯域を要求していることを検出することができ、より早く（無線基地局２に問い合わせることなく）送信帯域を無線端末４に割り当てることができる。
【図面の簡単な説明】
【０２０４】
【図１】ＭＡＣ　ＰＤＵのフォーマットを示す。

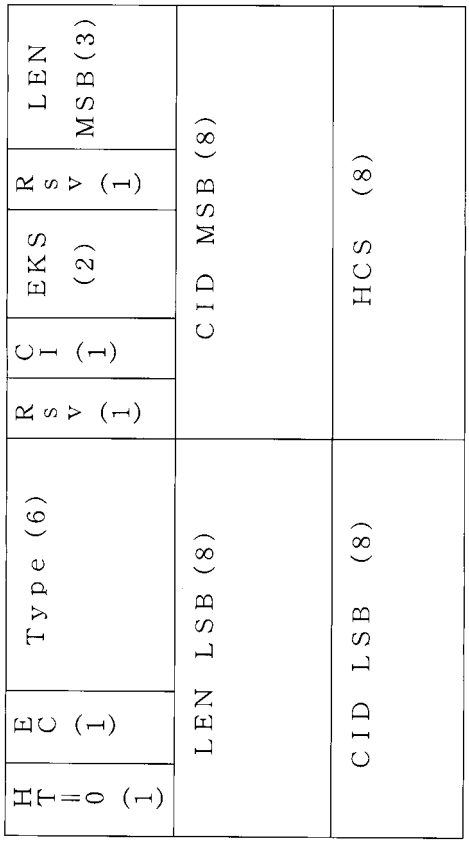
【図２】ＭＡＣヘッダを示す。
【図３】ＭＡＣヘッダ内のフィールドの説明示す。
【図４】許可管理サブヘッダ（ＵＬ）の種類を示す。
【図５】許可管理サブヘッダのフィールドの説明を示す。
【図６】帯域要求ヘッダのフォーマットを示す。
【図７】帯域要求ヘッダのフィールドの説明を示す。
【図８】無線通信システムを示す。
【図９】無線フレームフォーマットを示す。
【図１０】帯域割り当てシーケンスを示す。
【図１１】無線基地局２を示す。
【図１２】中継局３を示す。
【図１３】無線端末４を示す。
【図１４】帯域要求ヘッダに基く帯域割り当てシーケンスを示す。
【図１５】ピギーバック帯域要求（非暗号化）に基く帯域割り当てシーケンスを示す。
【図１６】ピギーバック帯域要求（暗号化）に基く帯域割り当てシーケンスを示す。
【図１７】中継局３の動作を示す。
【図１８】無線基地局２の動作を示す。
【図１９】中継局３の動作を示す。
【図２０】帯域要求管理テーブルを示す。
【図２１】無線端末４の帯域要求情報を示す。
【図２２】帯域要求（暗号化有り）の場合のシーケンスを示す。
【図２３】中継局３の動作を示す。
【図２４】中継局３の動作を示す。
【図２５】帯域要求管理テーブルを示す。
【図２６】無線端末４の帯域要求情報を示す。
【図２７】中継局３の動作を示す。
【符号の説明】
【０２０５】
１　ルーティング装置
２　無線基地局
３　中継局
４　無線端末
１０　アンテナ
１１　デュプレクサ
１２　受信部
１３　復調部
１４　復号化部
１５　暗号復号化部
１６　制御データ抽出部
１７　パケット生成部
１８　ＮＷインタフェース部
１９　パケット識別部
２０　帯域割当制御部
２１　パケットバッファ部
２２　ＰＤＵ生成部
２３　暗号化部
２４　符号化部
２５　変調部
２６　送信部
２７　制御部

３０
３１　デュプレクサ
３２　受信部
３３　復調部
３４　復号化部
３５　非暗号化データ抽出部
３６　帯域割当制御部
３７　バッファ部
３８　符号化部
３９　変調部
４０　送信部
４１　制御部
５０　アンテナ
５１　デュプレクサ
５２　受信部
５３　復調部
５４　復号化部
５５　暗号復号化部
５６　制御データ抽出部
５７　データ処理部
５８　ＰＤＵバッファ部
５９　暗号化部
６０　符号化部
６１　変調部
６２　送信部
６３　ＭＡＰ情報解析部
６４　制御部

【図１】



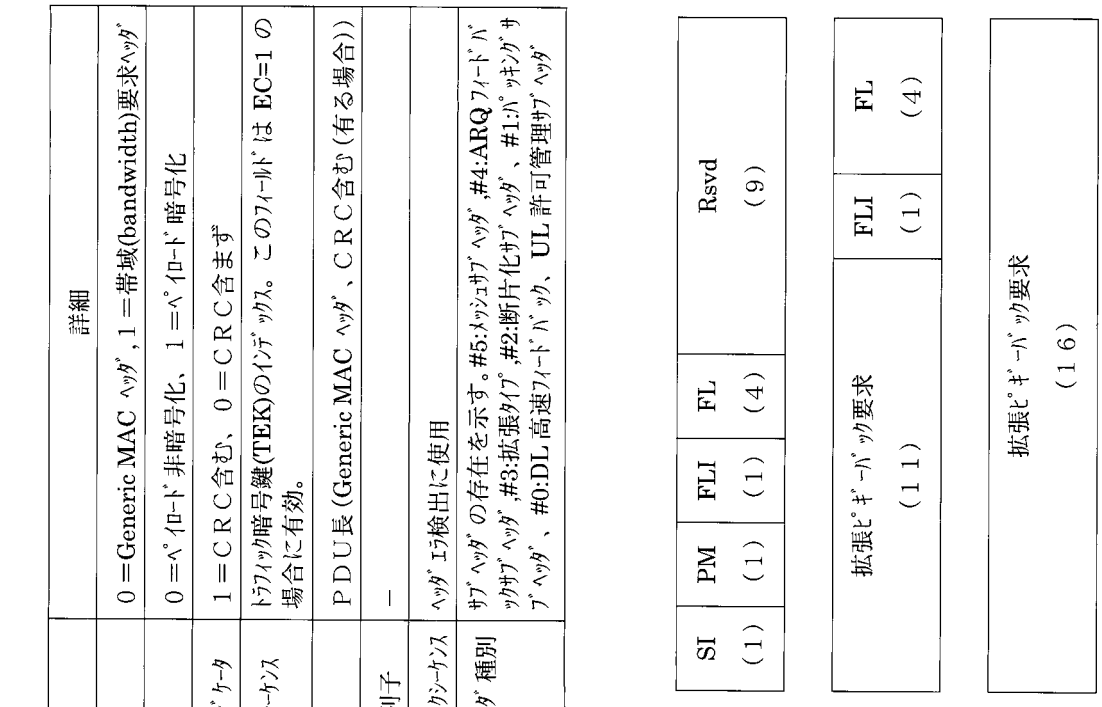
【図２】



【図３】

フィールド名	詳細
ＨＴ：ﾍｯﾀﾞﾀｲﾌﾟ	０＝Generic MAC ﾍｯﾀﾞ，１＝帯域(bandwidth)要求ﾍｯﾀﾞ
ＥＣ：暗号制御	０＝ﾍﾟｲﾛｰﾄﾞ非暗号化、１＝ﾍﾟｲﾛｰﾄﾞ暗号化
ＣＩ：ＣＲＣｲﾝｼﾞｹｰﾀ	１＝ＣＲＣ含む、０＝ＣＲＣ含まず
ＥＫＳ：暗号鍵ｼｰｹﾝｽ	ﾄﾗﾌｨｯｸ暗号鍵(TEK)のｲﾝﾃﾞｯｸｽ。このﾌｨｰﾙﾄﾞは EC=1 の場合に有効。
ＬＥＮ：長さ	ＰＤＵ長 (Generic MAC ﾍｯﾀﾞ，ＣＲＣ含む (有る場合))
ＣＩＤ：接続識別子	－
ＨＣＳ：ﾍｯﾀﾞﾁｪｯｸｼｰｹﾝｽ	ﾍｯﾀﾞｴﾗｰ検出に使用
Ｔｙｐｅ：ｻﾌﾞﾍｯﾀﾞ種別	ｻﾌﾞﾍｯﾀﾞの存在を示す。#5:ﾒｯｼｭｻﾌﾞﾍｯﾀﾞ,#4:ARQ ﾌｨｰﾄﾞﾊﾞｯｸｻﾌﾞﾍｯﾀﾞ,#3:拡張ﾀｲﾌﾟｻﾌﾞﾍｯﾀﾞ,#2:断片化ｻﾌﾞﾍｯﾀﾞ、#1:ﾊﾟｯｷﾝｸﾞｻﾌﾞﾍｯﾀﾞ、#0:DL 高速ﾌｨｰﾄﾞﾊﾞｯｸ，UL 許可管理ｻﾌﾞﾍｯﾀﾞ

【図４】



【図５】

フィールド名	詳細
ＳＩ：ｽﾘｯﾌﾟ識別子	0=ｱｸｼｮﾝ無し,1=送信ｷｭｰが閾値越えたらＭＳが送信
PM(問い合わせ要求)	0=ｱｸｼｮﾝ無し,1=他の CID のための帯域問い合わせ要求
ＦＬＩ：	0=FL はこの許可では無効、1=FL はこの許可で有効
ＦＬ：ﾌﾚｰﾑ待ち時間	現在のﾌﾚｰﾑに先行するﾌﾚｰﾑで、ﾃﾞｰﾀ送信ができたﾌﾚｰﾑの数。待ち時間が 15 より大きい場合 FL=15。
ﾋﾟｷﾞｰﾊﾞｯｸ要求	ＭＳによる上り帯域（ﾊﾞｲﾄ数）要求。増加要求

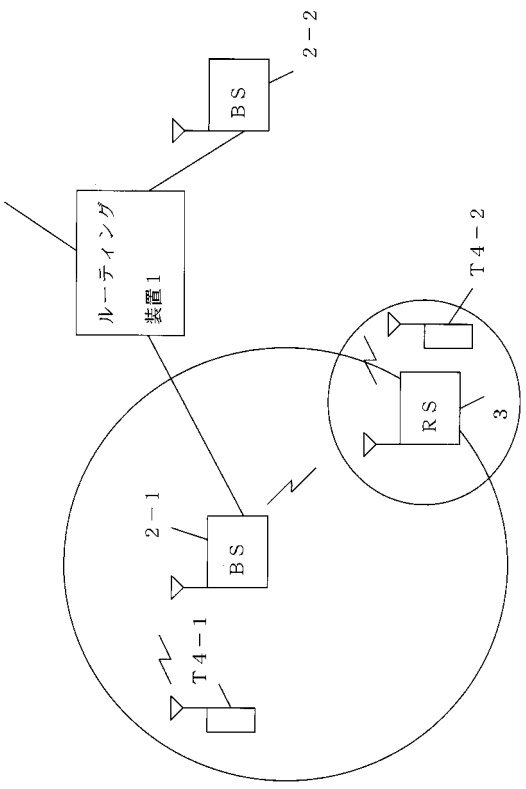
【図６】

ＨＴ＝１（１）	ＥＣ＝０（１）	Ｔｙｐｅ（３）	ＢＲ ＭＳＢ（１１）
ＢＲ ＬＳＢ（８）			ＣＩＤ ＭＳＢ（８）
ＣＩＤ ＬＳＢ （８）			ＨＣＳ （８）

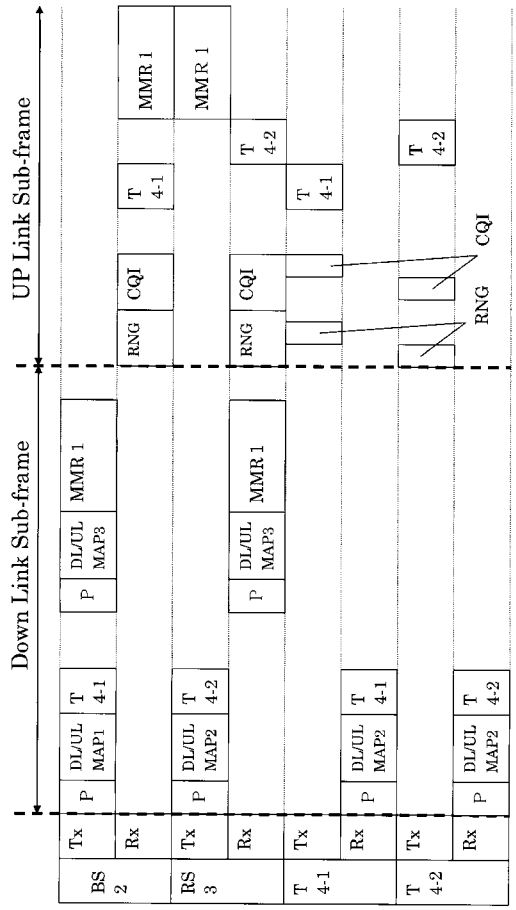
【図７】

フィールド名	詳細
ＨＴ：ﾍｯﾀﾞﾀｲﾌﾟ	1=帯域(bandwidth)要求ﾍｯﾀﾞ
ＥＣ：暗号制御	０＝ﾍﾟｲﾛｰﾄﾞ非暗号化
Type：帯域要求ﾀｲﾌﾟ	000=増加(帯域)、001=総計(帯域)
ＢＲ：帯域要求	ＭＳが要求する上り帯域幅のﾊﾞｲﾄ数。その要求は、ＰＨＹｵｰﾊﾞｰﾍｯﾄﾞを含んではいけない。
ＣＩＤ：接続識別子	要求接続ＩＤ
ＨＣＳ：ﾍｯﾀﾞﾁｪｯｸｼｰｹﾝｽ	ﾍｯﾀﾞｴﾗｰの検出に使用

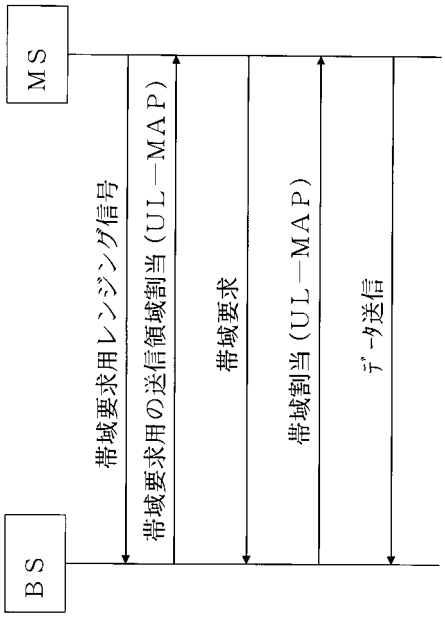
【図８】



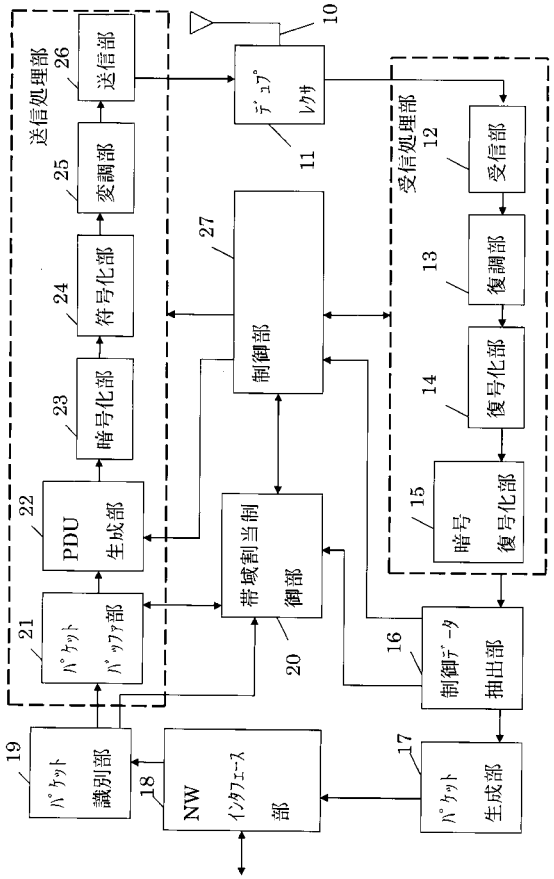
【図９】



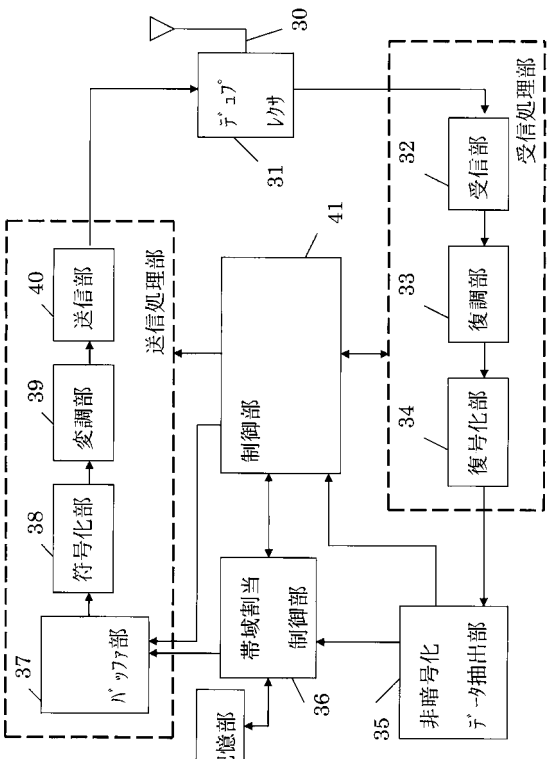
【図１０】



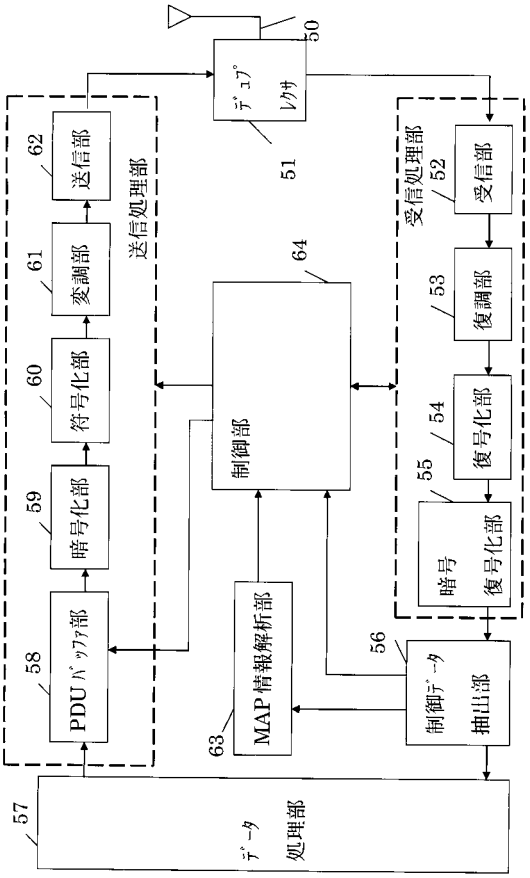
【図１１】



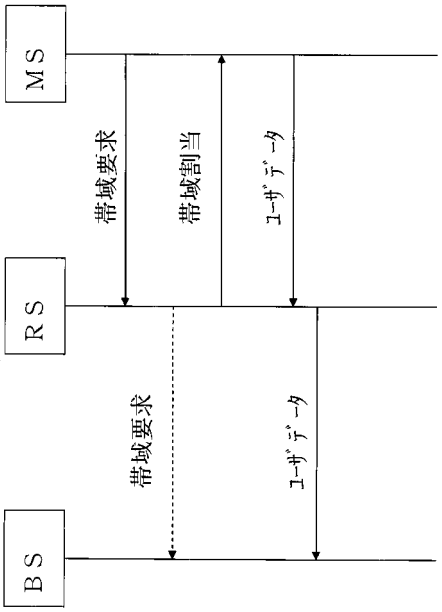
【図１２】



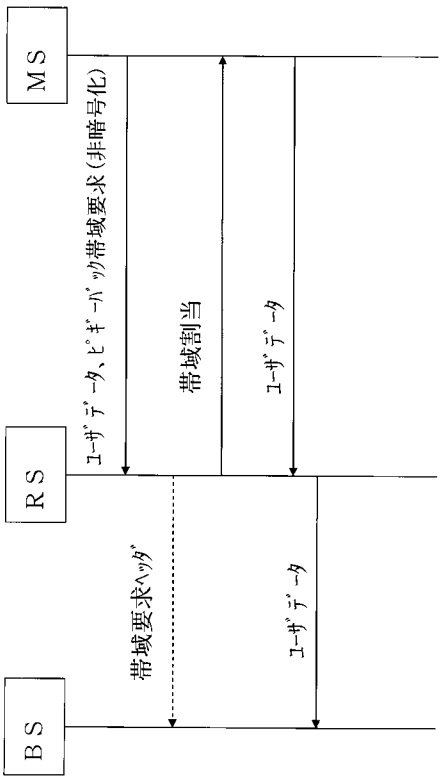
【図１３】



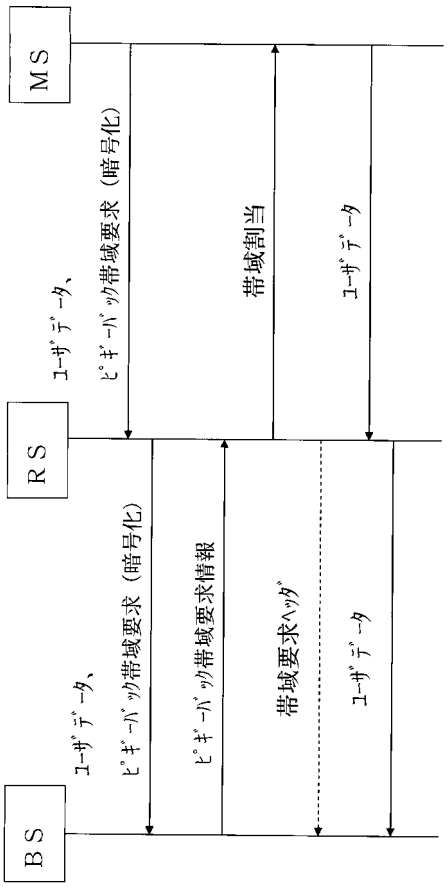
【図１４】



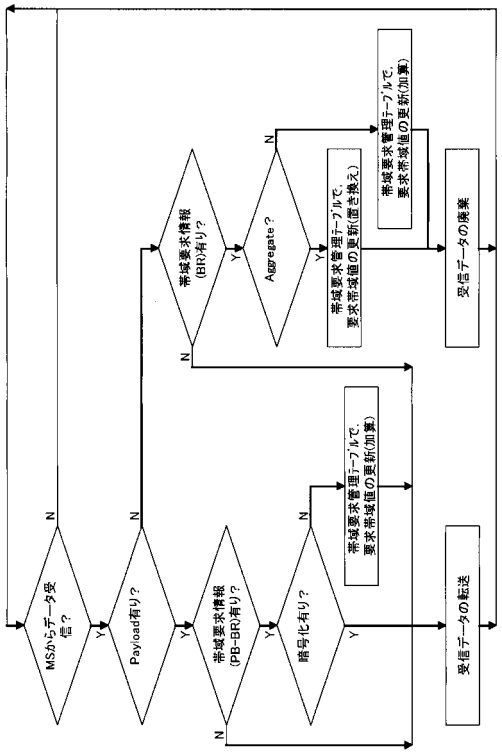
【図１５】



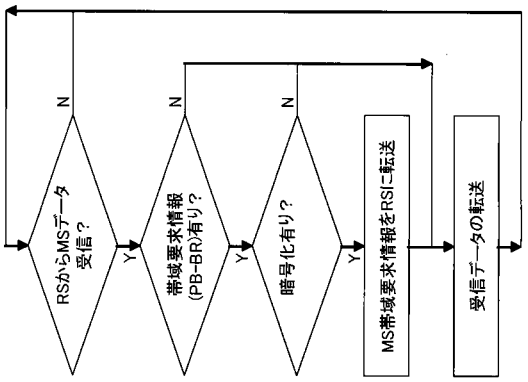
【図１６】



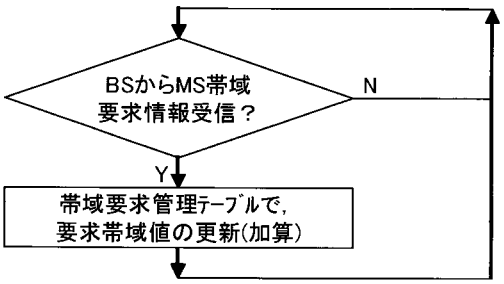
【図１７】



【図１８】



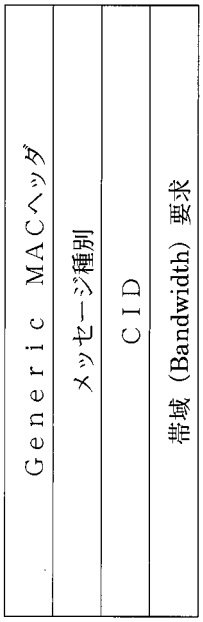
【図１９】



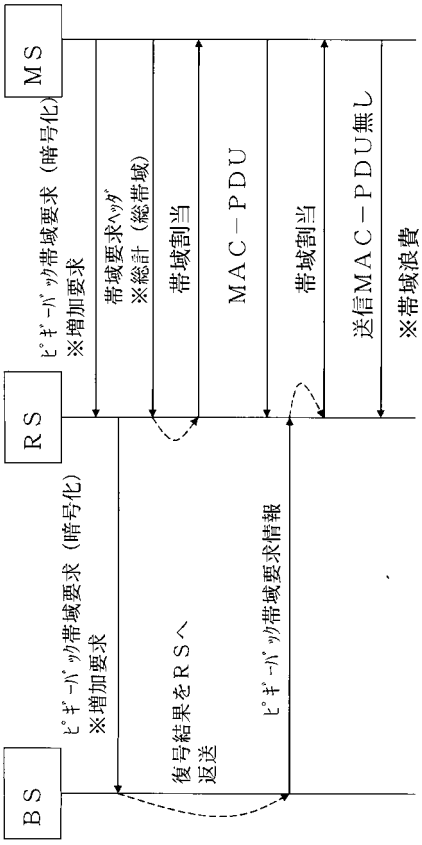
【図２０】

ＣＩＤ	要求帯域（バイト）
＃１	1000
＃２	2000
…	…

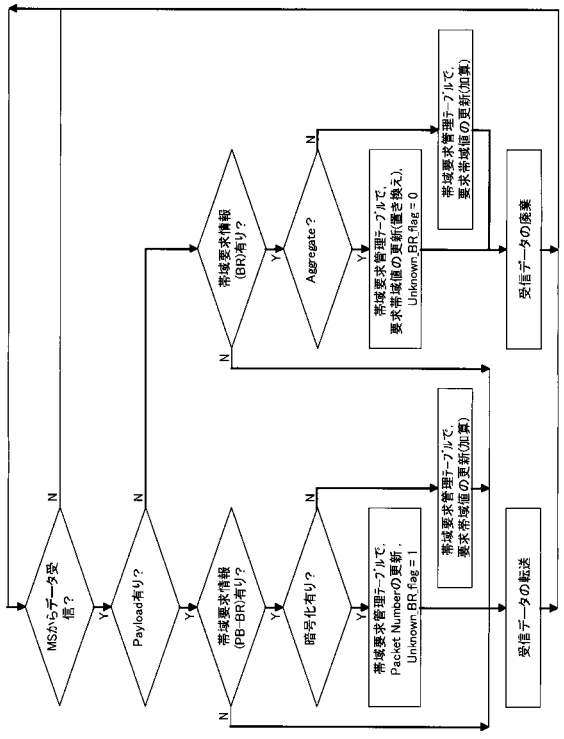
【図２１】



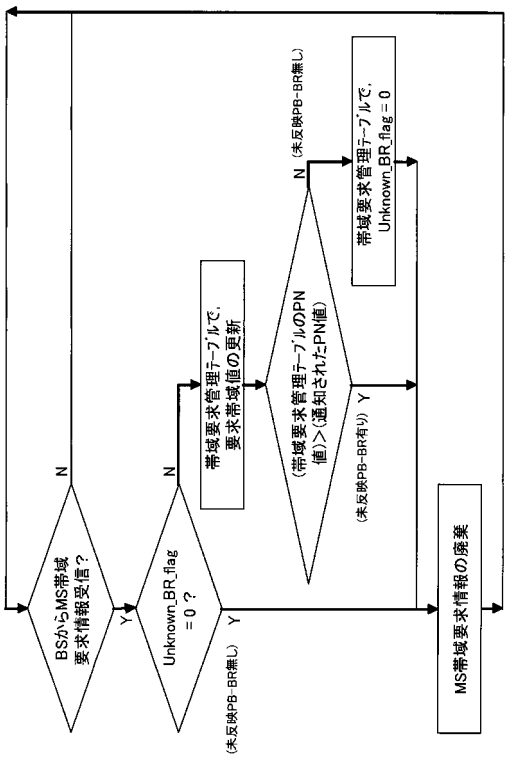
【図２２】



【図２３】



【図２４】



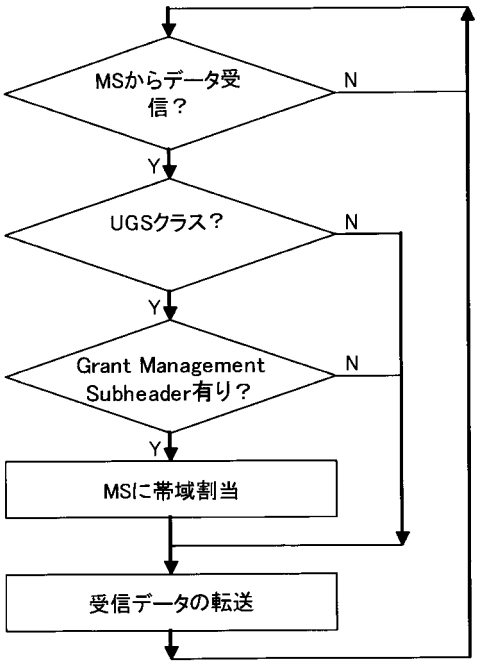
【図２５】

ＣＩＤ	要求帯域（バイト）	未知帯域要求ﾌﾗｸﾞ	パケット番号
＃１	1000	0	３５６
＃２	2000	1	２３８
…	…	…	…

【図２６】

Ｇｅｎｅｒｉｃ　ＭＡＣヘッダ
メッセージ種別
ＣＩＤ
帯域（Bandwidth）要求
パケット番号

【図２７】



フロントページの続き

(56)参考文献 特開２００６－３５２３３８（ＪＰ，Ａ）
国際公開第２００８／０４４３１７（WO，Ａ１）
特開平０６－０９７８８１（ＪＰ，Ａ）
特開平１０－０６５６０１（ＪＰ，Ａ）
特開２００２－０２６７９８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｂ　　７／２４－７／２６
Ｈ０４Ｗ　　４／００－９９／００