(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
2008 年2 月28 日 (28.02.2008)

PCT

(10) 国際公開番号
WO 2008/023781 A1

(51) 国際特許分類:
H04Q 7/38 (2006.01)

(21) 国際出願番号: PCT/JP2007/066416

(22) 国際出願日: 2007 年8 月24 日 (24.08.2007)

(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2006-228348 2006 年8 月24 日 (24.08.2006) JP
特願 2006-294475
2006 年10 月30 日 (30.10.2006) JP
特願2007-009331 2007 年1 月18 日 (18.01.2007) JP

(71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒5718501 大阪府門真市大字門真１００６番地 Osaka (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 森本 哲郎 (MORIMOTO, Tetsuro). 荒牧 隆 (ARAMAKI, Takashi). 江原 宏幸 (EHARA, Hiroyuki).

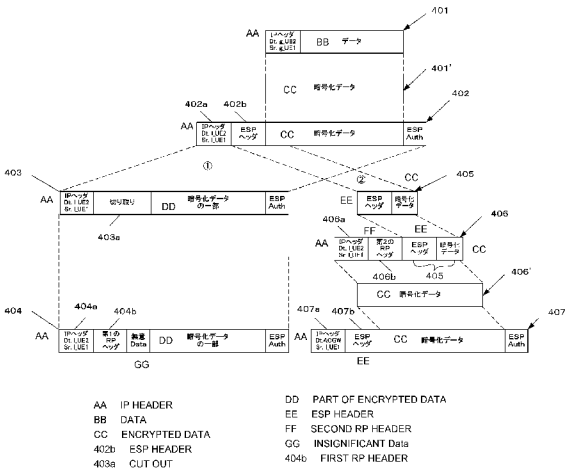
(74) 代理人: 二瓶 正敬 (NIHEI, Masayuki); 〒1600022 東京都新宿区新宿２－８－８ とみん新宿ビル２Ｆ Tokyo (JP).

(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, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM,

[続葉有]

(54) Title: COMMUNICATION SYSTEM, COMMUNICATION METHOD, RADIO TERMINAL, RADIO RELAY DEVICE, AND CONTROL DEVICE

(54) 発明の名称: 通信システム、通信方法、無線端末、無線中継装置及び制御装置



(57) **Abstract:** Disclosed is a technique to effectively use a network resource when a radio terminal of the transmission side and a radio terminal of the reception side are radio-connected to the same radio relay device, to reduce the load on a control device, and to manage communication of the radio terminals by the control device. According to the technique, when the UE (2) of the reception side is connected to the same E-Node B (103), the UE (1) of the transmission side divides the transmission packet destined to the UE (2) into a first packet not to be relayed by an ACGW (105) and a second packet to be relayed by the ACGW (105) and transmits them to the E-Node B (103). The E-Node B (103) transmits the first packet to the UE (2) and transmits the second packet to the ACGW (105).The ACGW (105) receives the second packet and transmits it to the E-Node B (103). The E-Node B (103) receives the second packet transmitted from the ACGW (105) and transmits it to the UE (2). The UE (2) receives the first and the second packet and combines them into the original packet.

(57) 要約: 送信側と受信側の無線端末が同じ無線中継装置に無線接続している場合にネットワークリソースを効率的に使用し、また、制御装置の負荷を軽減し、さらに制御装置が無線端末の通信を管理する技術が開示され、その技術によれば送信側のＵＥ１は受信側のＵＥ２が同一のＥ- ＮｏｄｅＢ１０３に接続されている場合に、ＵＥ２あての送信パケットを、ＡＣＧＷ１０５を介さない第１のパケットとＡＣＧ

[続葉有]

WO 2008/023781 A1

GT, HN, HR, HU, ID, IL, IN, IS, JP, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, 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, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

Ｗ１０５を介する第２のパケットに分割してＥ- ＮｏｄｅＢ１０３に送信し、Ｅ- ＮｏｄｅＢ１０３は第１のパケットをＵＥ２に送信するとともに第２のパケットをＡＣＧＷ１０５に送信し、ＡＣＧＷ１０５は第２のパケットを受信してＥ- ＮｏｄｅＢ１０３に送信し、Ｅ- ＮｏｄｅＢ１０３はＡＣＧＷ１０５から送信された第２のパケットを受信してＵＥ２に送信し、ＵＥ２は第１、第２のパケットを受信して元のパケットに合成する。

明 細 書

通信システム、通信方法、無線端末、無線中継装置及び制御装置

技術分野

[0001] 本発明は、パケット網を利用した通信システム、通信方法、無線端末、無線中継装置及び制御装置に関する。

背景技術

[0002] 下記の非特許文献1、2に示されるように、第3世代携帯電話網(3GPP(登録商標):3rd Generation Partnership Project)の次の世代のネットワーク構成として図15のようなアーキテクチャが考えられている。図15では、無線端末であるユーザ機器(User Equipment、以下、UEと言う。)101とUE102はそれぞれ、基地局であるE－NodeB(Evolved NodeB)103、104に無線電波を用いて接続している。さらに基地局103、104は有線を介して、網側の制御装置であるアクセスゲートウェイ(ACGW: Access Gateway、又はMME／UPE)105と接続される。ACGW105は、ユーザ認証装置106を用いてユーザ認証処理を行ってUE101、102を網に接続させるかどうか判定し、また、課金管理装置107を用いてUE101、102への課金のためにパケット量など使用状況の情報収集を行う(PCRF: Policy Control and Charging Rules Function)。また、ユーザ・プレーン(User Plane)のデータは、ACGW105とUE101、102の間で暗号化される。

[0003] まず、UE101、102間でのパケットの流れについて説明する。送信側のUE101は受信側のUE102に向けてパケットを生成し、この生成したパケットをACGW105あてに暗号化し、暗号化したパケットをACGW105に送信する。送信側UE101が暗号化パケットを送信すると、基地局103はUE101からの暗号化パケットを受信し、ACGW105に転送する。ACGW105はUE101からの暗号化されたパケットを受信し、そのパケットを復号化する。さらにACGW105は、パケットのあて先であるUE102あてに暗号化し、暗号化したパケットを送信する。基地局104はACGW105から暗号化パケットを受信し、受信側のUE102に転送する。受信側のUE102はACGW105から暗号化パケットを受信して復号化し、送信側UE101からのパケットを受信処

理する。以上が、UE－UE間のパケットの流れである。

また、データ分割の従来技術として、非特許文献3、特許文献1に示すように音声信号を帯域分割して各帯域を別々に符号化するスケーラブル音声符号化が知られている。

非特許文献1:3GPP(登録商標) Technical Report 23.882 draft V1.1.0 (2006-04)

非特許文献2:3GPP(登録商標) Technical Report 25.813 V0.9.2 (2006-05)

非特許文献3:「高パケットロス耐性を有する広帯域音声符号化法」、森岳至他、電子情報通信学会論文誌 2005/7 Vol. J88-DII No.7, P.1103-1113

特許文献1:特開2003－241799号公報(要約書)

[0004] しかしながら、上記のUE－UE間のパケットの流れでは、図1に示すようにUE101(UE1)とUE102(UE2)が同じ基地局103に無線接続している場合には、UE101が送信したパケットは、UE101→基地局103→ACGW105→基地局103→UE102(ルート(2)図1中は丸囲み数字2で表す(以下同様))と流れる。すなわち、ルート(2)ではACGW105と基地局103を折り返してデータが流れている。このように、従来の方法では、パケット通信を行っているUE101とUE102が同じ基地局103に無線接続している場合に、基地局103－ACGW105間のネットワークリソースを無駄に使用し、効率的に使用できないという課題があった。また、ACGW105は多数のUEと通信し、UEからのパケットを復号化する処理及びUEに転送するパケットを暗号化する処理があり、ACGW105に処理負荷が集中するという課題があった。

[0005] ところで、図1に示すようにUE101とUE102が同じ基地局103に無線接続している場合には、基地局103で折り返すことによりACGW105を経由しない方法(ルート(1))が考えられるが、ユーザデータを盗聴などの攻撃から保護するためにE－Node Bより網側の装置、すなわちUE－ACGW間で暗号化する必要があることや、網側でユーザデータの通信管理、例えば課金などの目的のために、パケット数のカウントを網側の装置で行いたいというオペレータの要望があることや、また必要がある場合にはユーザデータを監視(Lawful Interception)できるようにしたいという要望を満たすことは、この方法では困難である。

発明の開示

[0006] 本発明は上記従来技術の問題点に鑑み、送信側と受信側の無線端末が同じ無線中継装置に無線接続している場合にネットワークリソースを効率的に使用することができ、また、制御装置の負荷を軽減することができるとともに、制御装置が無線端末の通信を管理することができる通信システム、通信方法、無線端末、無線中継装置及び制御装置を提供することを目的とする。

[0007] 本発明は上記目的を達成するために、無線端末と相互に無線通信を行う無線中継装置と、前記無線中継装置との間でパケット転送を行うとともに前記無線端末及び無線中継装置間の無線通信を管理する制御装置とを備えた通信システムにおいて、

送信側の無線端末は、受信側の無線端末が同一の無線中継装置に接続されている場合に、前記受信側の無線端末あての送信パケットを、前記制御装置を介さない第1のパケットと前記制御装置を介する第2のパケットに分割して前記無線中継装置に送信し、

前記無線中継装置は、前記送信側の無線端末から送信された前記第1及び前記第2のパケットを受信して、前記第1のパケットを前記受信側の無線端末に送信するとともに前記第2のパケットを前記制御装置に送信し、

前記制御装置は、前記無線中継装置から送信された前記第2のパケットを受信して前記無線中継装置に送信し、

前記無線中継装置は、前記制御装置から送信された前記第2のパケットを受信して前記受信側の無線端末に送信し、

前記受信側の無線端末は、前記無線中継装置から送信された前記第1及び前記第2のパケットを受信して元のパケットを復元する構成とした。

上記構成により、送信側と受信側の無線端末が同じ無線中継装置に無線接続している場合に、受信側の無線端末あての送信パケットを、制御装置を介さない第1のパケットと制御装置を介する第2のパケットに分割するので、ネットワークリソースを効率的に使用することができ、また、制御装置の負荷を軽減することができるとともに、制御装置が無線端末の通信を管理することができる。

前記制御装置を介さない第1のパケットは、音声信号の帯域を分割した低域側の基本音声データと高域側の拡張音声データのうち前記拡張音声データを含み、前記

制御装置を介する第2のパケットは前記基本音声データを含む。また、前記制御装置を介さない第1のパケットは、画像信号を画面内でのみ符号化した画面内符号化データと、画面間差分を予測符号化した画面間差分予測符号化データのうち前記画面間差分予測符号化データを含み、前記制御装置を介する第2のパケットは前記画面内符号化データを含む。

[0008] また、前記送信側の無線端末は、前記受信側の無線端末あての送信データを暗号化して、前記暗号化データを前記受信側の無線端末側で復号するための識別データを取り除いた前記第1のパケットを生成するとともに、前記識別データを含む前記第2のパケットを生成し、

前記受信側の無線端末は、前記第2のパケット内の前記識別データを、前記第1のパケット内の前記識別データが切り取られた部分にセットして前記第1のパケット内の前記暗号化データを復号する構成とした。

また、前記送信側の無線端末は、前記受信側の無線端末あての送信データを暗号化して、前記暗号化データを前記受信側の無線端末側で復号するための識別データ及び前記暗号化データの一部を取り除いた前記第1のパケットを生成するとともに、前記識別データ及び前記暗号化データの一部を含む前記第2のパケットを生成し、

前記受信側の無線端末は、前記第2のパケット内の前記識別データ及び前記暗号化データの一部を、前記第1のパケット内の前記識別データ及び前記暗号化データの一部が切り取られた部分にセットして前記第1のパケット内の前記暗号化データを復号する構成とした。

また、前記送信側の無線端末は、前記受信側の無線端末あての送信データを暗号化して、前記暗号化データを前記受信側の無線端末側で復号するために必要なデータの一部を取り除いた前記第1のパケットを生成するとともに、前記復号するために必要なデータの一部を含む前記第2のパケットを生成し、

前記受信側の無線端末は、前記第2のパケット内の前記復号するために必要なデータの一部を、前記第1のパケット内の前記復号するために必要なデータの一部が切り取られた部分にセットして前記第1のパケット内の前記暗号化データを復号する

構成とした。

上記構成により、第1のパケットが制御装置を介さなくても通信のセキュリティを維持することができ、また、受信側の無線端末では第1、第2のパケットの両方が到着しなければ元のデータを復元できないので、システム側すなわち網側がユーザ機器間の直接通信を管理することができる。

[0009] また、本発明は上記目的を達成するために、無線端末と無線中継装置との間で相互に無線通信を行い、制御装置が前記無線中継装置との間でパケット転送を行うとともに前記無線端末及び無線中継装置間の無線通信を管理する通信方法において、

送信側の無線端末及び受信側の無線端末が同一の前記無線中継装置に接続されている場合に、前記送信側の無線端末が、受信側の無線端末あての送信パケットを、前記制御装置を介さない第1のパケットと前記制御装置を介する第2のパケットに分割して前記無線中継装置に送信するステップと、

前記無線中継装置が、前記送信側の無線端末から送信された前記第1及び前記第2のパケットを受信して、前記第1のパケットを前記受信側の無線端末に送信するとともに前記第2のパケットを前記制御装置に送信するステップと、

前記制御装置が、前記無線中継装置から送信された前記第2のパケットを受信して前記無線中継装置に送信するステップと、

前記無線中継装置が、前記制御装置から送信された前記第2のパケットを受信して前記受信側の無線端末に送信するステップと、

前記受信側の無線端末が、前記無線中継装置から送信された前記第1及び前記第2のパケットを受信して元のパケットに復元するステップとを、

有するようにした。

[0010] また、本発明は上記目的を達成するために、無線端末と相互に無線通信を行う無線中継装置と、前記無線中継装置との間でパケット転送を行うとともに前記無線端末及び無線中継装置間の無線通信を管理する制御装置とを備えた通信システムにおける送信側の前記無線端末において、

自己及び受信側の無線端末が同一の前記無線中継装置に接続されている場合に

、前記受信側の無線端末あての送信パケットを、前記制御装置を介さない第1のパケットと前記制御装置を介する第2のパケットに分割して前記無線中継装置に送信する手段を備え、

前記無線中継装置が、前記送信側の無線端末から送信された前記第1及び前記第2のパケットを受信して、前記第1のパケットを前記受信側の無線端末に送信するとともに前記第2のパケットを前記制御装置に送信し、

前記制御装置が、前記無線中継装置から送信された前記第2のパケットを受信して前記無線中継装置に送信し、

前記無線中継装置が、前記制御装置から送信された前記第2のパケットを受信して前記受信側の無線端末に送信し、

前記受信側の無線端末が、前記無線中継装置から送信された前記第1及び前記第2のパケットを受信して元のパケットに復元するようにした。

[0011] また、本発明は上記目的を達成するために、無線端末と相互に無線通信を行う無線中継装置と、前記無線中継装置との間でパケット転送を行うとともに前記無線端末及び無線中継装置間の無線通信を管理する制御装置とを備えた通信システムにおける前記無線中継装置において、

送信側の無線端末及び受信側の無線端末が自己に接続されている場合に、前記送信側の無線端末が、前記受信側の無線端末あての送信パケットを、前記制御装置を介さない第1のパケットと前記制御装置を介する第2のパケットに分割して自己に送信したとき、前記送信側の無線端末から送信された前記第1及び前記第2のパケットを受信して、前記第1のパケットを前記受信側の無線端末に送信するとともに前記第2のパケットを前記制御装置に送信する手段と、

前記制御装置が、自己から送信された前記第2のパケットを受信して自己に送信したとき、前記制御装置から送信された前記第2のパケットを受信して前記受信側の無線端末に送信する手段とを備え、

前記受信側の無線端末が、自己から送信された前記第1及び前記第2のパケットを受信して元のパケットに復元するようにした。

[0012] また、本発明は上記目的を達成するために、無線端末と相互に無線通信を行う無

線中継装置と、前記無線中継装置との間でパケット転送を行うとともに前記無線端末及び無線中継装置間の無線通信を管理する制御装置とを備えた通信システムにおける前記制御装置において、

送信側の無線端末が、受信側の無線端末が同一の無線中継装置に接続されている場合に、前記受信側の無線端末あての送信パケットを、自己を介さない第1のパケットと自己を介する第2のパケットに分割して前記無線中継装置に送信し、前記無線中継装置が、前記送信側の無線端末から送信された前記第1及び前記第2のパケットを受信して、前記第1のパケットを前記受信側の無線端末に送信するとともに前記第2のパケットを自己あてに送信したとき、前記無線中継装置から送信された前記第2のパケットを受信して前記無線中継装置に送信する手段と、

前記第2のパケットに基づいて前記無線端末及び無線中継装置間の無線通信を管理する手段とを備え、

前記無線中継装置が、自己から送信された前記第2のパケットを受信して前記受信側の無線端末に送信し、

前記受信側の無線端末が、前記無線中継装置から送信された前記第1及び前記第2のパケットを受信して元のパケットに復元するようにした。

[0013] また、本発明は上記目的を達成するために、無線端末と相互に無線通信を行う無線中継装置と、前記無線中継装置との間でパケット転送を行うとともに前記無線端末及び無線中継装置間の無線通信を管理する制御装置とを備えた通信システムにおける受信側の前記無線端末において、

送信側の無線端末及び自己が同一の無線中継装置に接続されている場合に、前記送信側の無線端末が自己あての送信パケットを、前記制御装置を介さない第1のパケットと前記制御装置を介する第2のパケットに分割して前記無線中継装置に送信し、前記無線中継装置が、前記送信側の無線端末から送信された前記第1及び前記第2のパケットを受信して、前記第1のパケットを前記受信側の無線端末に送信するとともに前記第2のパケットを前記制御装置に送信し、前記制御装置が、前記無線中継装置から送信された前記第2のパケットを受信して前記無線中継装置に送信し、前記無線中継装置が、前記制御装置から送信された前記第2のパケットを受信して

自己に送信したとき、前記無線中継装置から送信された前記第1及び前記第2のパケットを受信して元のパケットに復元する手段を、

備えた構成とした。

[0014] また、本発明は上記目的を達成するために、無線端末と相互に無線通信を行う無線中継装置と、前記無線中継装置との間でパケット転送を行うとともに前記無線端末及び無線中継装置間の無線通信を管理する制御装置とを備えた通信システムにおいて、

送信側の無線端末は、受信側の無線端末が同一の無線中継装置に接続されている場合に、前記受信側の無線端末あての送信データを暗号化した後にパケット化し、このパケットを前記制御装置を介さない前記受信側の無線端末あての第1のパケットとして前記無線中継装置に送信するとともに、前記暗号化されたデータを復号するための鍵データをパケット化し、このパケットを前記制御装置を介する前記受信側の無線端末あての第2のパケットとして前記無線中継装置に送信し、

前記無線中継装置は、前記送信側の無線端末から送信された前記第1及び前記第2のパケットを受信して、前記第1のパケットを前記受信側の無線端末に転送するとともに前記第2のパケットを前記制御装置に転送し、さらに複数の前記第1のパケットの内の一部のパケットを定期的にコピーしてこのパケットを第3のパケットとして前記制御装置に送信し、

前記制御装置は、前記無線中継装置から転送された前記第2のパケットを受信して内部の鍵データを確認して前記第2のパケットを前記無線中継装置に転送するとともに、前記無線中継装置から送信された前記第3のパケットに基づいて前記第1のパケットの管理情報を取得し、

前記無線中継装置は、前記制御装置から転送された前記第2のパケットを受信して前記受信側の無線端末に転送し、

前記受信側の無線端末は、前記無線中継装置から転送された前記第1及び前記第2のパケットを受信して、前記暗号化されたデータを前記鍵データにより復号する構成とした。

[0015] 上記構成により、送信側と受信側の無線端末が同じ無線中継装置に無線接続して

いる場合に、受信側の無線端末あての送信パケットを、制御装置を介さない第1のパケットとして受信側の無線端末に転送するとともに、第1のパケット内の暗号化データを復号する鍵データを制御装置を介する第2のパケットとして受信側の無線端末に転送するので、ネットワークリソースを効率的に使用することができ、また、制御装置の負荷を軽減することができるとともに、制御装置が無線端末の通信を管理することができる。また、制御装置を介さなくても第1のパケットの通信のセキュリティを維持することができ、また、受信側の無線端末では第1、第2のパケットの両方が到着しなければ元のデータを復元できないので、システム側、すなわち網側がユーザ機器間の直接通信を管理することができる。

さらに、無線中継装置が、第1のパケットの内の一部のパケットを定期的にコピーしてこのパケットを第3のパケットとして制御装置に送信するので、制御装置が第3のパケットに基づいて第1のパケットの管理情報を取得することができる。また、送信側の無線端末が第1のパケットの各パケット内にそれぞれシーケンス番号をセットすることにより、制御装置が第3のパケット内のシーケンス番号に基づいて第1のパケットの転送パケット数を管理することができる。

[0016] また、本発明は上記目的を達成するために、無線端末と無線中継装置との間で相互に無線通信を行い、制御装置が前記無線中継装置との間でパケット転送を行うとともに前記無線端末及び無線中継装置間の無線通信を管理する通信方法において、

送信側の無線端末が、受信側の無線端末が同一の無線中継装置に接続されている場合に、前記受信側の無線端末あての送信データを暗号化した後にパケット化し、このパケットを前記制御装置を介さない前記受信側の無線端末あての第1のパケットとして前記無線中継装置に送信するとともに、前記暗号化されたデータを復号するための鍵データをパケット化し、このパケットを前記制御装置を介する前記受信側の無線端末あての第2のパケットとして前記無線中継装置に送信するステップと、

前記無線中継装置が、前記送信側の無線端末から送信された前記第1及び前記第2のパケットを受信して、前記第1のパケットを前記受信側の無線端末に転送するとともに前記第2のパケットを前記制御装置に転送し、さらに複数の前記第1のパケット

の内の一部のパケットを定期的にコピーしてこのパケットを第3のパケットとして前記制御装置に送信するステップと、

前記制御装置が、前記無線中継装置から転送された前記第2のパケットを受信して内部の鍵データを確認して前記第2のパケットを前記無線中継装置に転送するとともに、前記無線中継装置から送信された前記第3のパケットに基づいて前記第1のパケットの管理情報を取得するステップと、

前記無線中継装置が、前記制御装置から転送された前記第2のパケットを受信して前記受信側の無線端末に転送するステップと、

前記受信側の無線端末は、前記無線中継装置から転送された前記第1及び前記第2のパケットを受信して、前記暗号化されたデータを前記鍵データにより復号するステップとを、

有する構成とした。

[0017] また、本発明は上記目的を達成するために、無線端末と相互に無線通信を行う無線中継装置と、前記無線中継装置との間でパケット転送を行うとともに前記無線端末及び無線中継装置間の無線通信を管理する制御装置とを備えた通信システムにおける送信側の前記無線端末において、

自身と受信側の無線端末が同一の無線中継装置に接続されている場合に、前記受信側の無線端末あての送信データを暗号化した後にパケット化し、このパケットを前記制御装置を介さない前記受信側の無線端末あての第1のパケットとして前記無線中継装置に送信するとともに、前記暗号化されたデータを復号するための鍵データをパケット化し、このパケットを前記制御装置を介する前記受信側の無線端末あての第2のパケットとして前記無線中継装置に送信する手段を備え、

前記無線中継装置が、前記送信側の無線端末自身から送信された前記第1及び前記第2のパケットを受信して、前記第1のパケットを前記受信側の無線端末に転送するとともに前記第2のパケットを前記制御装置に転送し、さらに複数の前記第1のパケットの内の一部のパケットを定期的にコピーしてこのパケットを第3のパケットとして前記制御装置に送信し、

前記制御装置が、前記無線中継装置から転送された前記第2のパケットを受信して

内部の鍵データを確認して前記第2のパケットを前記無線中継装置に転送するとともに、前記無線中継装置から送信された前記第3のパケットに基づいて前記第1のパケットの管理情報を取得し、

前記無線中継装置が、前記制御装置から転送された前記第2のパケットを受信して前記受信側の無線端末に転送し、

前記受信側の無線端末が、前記無線中継装置から転送された前記第1及び前記第2のパケットを受信して、前記暗号化されたデータを前記鍵データにより復号する構成とした。

[0018] また、本発明は上記目的を達成するために、無線端末と相互に無線通信を行う無線中継装置と、前記無線中継装置との間でパケット転送を行うとともに前記無線端末及び無線中継装置間の無線通信を管理する制御装置とを備えた通信システムにおける前記無線中継装置において、

送信側の無線端末が、受信側の無線端末が同一の無線中継装置に接続されている場合に、前記受信側の無線端末あての送信データを暗号化した後にパケット化し、このパケットを前記制御装置を介さない前記受信側の無線端末あての第1のパケットとして前記無線中継装置自身に送信するとともに、前記暗号化されたデータを復号するための鍵データをパケット化し、このパケットを前記制御装置を介する前記受信側の無線端末あての第2のパケットとして前記無線中継装置自身に送信した場合に、前記送信側の無線端末から送信された前記第1及び前記第2のパケットを受信して、前記第1のパケットを前記受信側の無線端末に転送するとともに前記第2のパケットを前記制御装置に転送し、さらに複数の前記第1のパケットの内の一部のパケットを定期的にコピーしてこのパケットを第3のパケットとして前記制御装置に送信する手段と、

前記制御装置が、前記無線中継装置自身から転送された前記第2のパケットを受信して内部の鍵データを確認して前記第2のパケットを前記無線中継装置自身に転送するとともに、自身から送信された前記第3のパケットに基づいて前記第1のパケットの管理情報を取得した場合に、前記制御装置から転送された前記第2のパケットを受信して前記受信側の無線端末に転送する手段とを備え、

前記受信側の無線端末が、前記無線中継装置自身から転送された前記第1及び前記第2のパケットを受信して、前記暗号化されたデータを前記鍵データにより復号する構成とした。

[0019] また、本発明は上記目的を達成するために、無線端末と相互に無線通信を行う無線中継装置と、前記無線中継装置との間でパケット転送を行うとともに前記無線端末及び無線中継装置間の無線通信を管理する制御装置とを備えた通信システムにおける前記制御装置において、

送信側の無線端末が、受信側の無線端末が同一の無線中継装置に接続されている場合に、前記受信側の無線端末あての送信データを暗号化した後にパケット化し、このパケットを自身を介さない前記受信側の無線端末あての第1のパケットとして前記無線中継装置に送信するとともに、前記暗号化されたデータを復号するための鍵データをパケット化し、このパケットを自身を介する前記受信側の無線端末あての第2のパケットとして前記無線中継装置に送信し、前記無線中継装置が、前記送信側の無線端末から送信された前記第1及び前記第2のパケットを受信して、前記第1のパケットを前記受信側の無線端末に転送するとともに前記第2のパケットを自身に転送し、さらに複数の前記第1のパケットの内の一部のパケットを定期的にコピーしてこのパケットを第3のパケットとして自身に送信した場合、前記無線中継装置から転送された前記第2のパケットを受信して内部の鍵データを確認して前記第2のパケットを前記無線中継装置に転送するとともに、前記無線中継装置から送信された前記第3のパケットに基づいて前記第1のパケットの管理情報を取得する手段を備え、

前記無線中継装置が、前記制御装置自身から転送された前記第2のパケットを受信して前記受信側の無線端末に転送し、

前記受信側の無線端末が、前記無線中継装置から転送された前記第1及び前記第2のパケットを受信して、前記暗号化されたデータを前記鍵データにより復号する構成とした。

[0020] また、本発明は上記目的を達成するために、無線端末と相互に無線通信を行う無線中継装置と、前記無線中継装置との間でパケット転送を行うとともに前記無線端末及び無線中継装置間の無線通信を管理する制御装置とを備えた通信システムにお

ける受信側の前記無線端末において、

送信側の無線端末が、受信側の無線端末が同一の無線中継装置に接続されている場合に、前記受信側の無線端末自身あての送信データを暗号化した後にパケット化し、このパケットを前記制御装置を介さない前記受信側の無線端末自身あての第1のパケットとして前記無線中継装置に送信するとともに、前記暗号化されたデータを復号するための鍵データをパケット化し、このパケットを前記制御装置を介する自身あての第2のパケットとして前記無線中継装置に送信し、前記無線中継装置が、前記送信側の無線端末から送信された前記第1及び前記第2のパケットを受信して、前記第1のパケットを前記受信側の無線端末自身に転送するとともに前記第2のパケットを前記制御装置に転送し、さらに複数の前記第1のパケットの内の一部のパケットを定期的にコピーしてこのパケットを第3のパケットとして前記制御装置に送信し、前記制御装置が、前記無線中継装置から転送された前記第2のパケットを受信して内部の鍵データを確認して前記第2のパケットを前記無線中継装置に転送するとともに、前記無線中継装置から送信された前記第3のパケットに基づいて前記第1のパケットの管理情報を取得し、前記無線中継装置が、前記制御装置から転送された前記第2のパケットを受信して前記受信側の無線端末自身に転送した場合に、前記無線中継装置から転送された前記第1及び前記第2のパケットを受信して、前記暗号化されたデータを前記鍵データにより復号する手段を、

備えた構成とした。

[0021] 本発明によれば、送信側の無線端末から送信されたパケットをすべて無線中継装置と制御装置の間で折り返す必要がなく、一部の小さなデータだけで十分であり、無線中継装置と制御装置のネットワークリソースを効率的に使用できるという効果がある。また、制御装置は、送信側の無線端末が受信側の無線端末に送信するパケットの全データに対して復号化処理及び暗号化処理を行うのではなく、一部のデータのみ復号化処理及び暗号化処理を行うため、処理負荷を軽減できるという効果がある。

図面の簡単な説明

[0022] [図1]従来の技術及び本発明の実施の形態において送信側UEと受信側UEが同一のE-NodeBに接続する場合のシステム構成図

[図2]本発明の実施の形態におけるUE－UE直接通信を開始するときの処理を示すフローチャート

[図3A]本発明の実施の形態におけるUE－UE直接通信を開始するときのUE-ACGW間のメッセージシーケンスを示す説明図であって図1のUE1、UE2がともに「UE－UE直接通信」に対応している場合の説明図

[図3B]本発明の実施の形態におけるUE－UE直接通信を開始するときのUE-ACGW間のメッセージシーケンスを示す説明図であって図1のUEが「UE－UE直接通信」に対応していない場合（UE2が非対応）の説明図

[図4]図1の送信側UEのパケット分割処理を示す説明図

[図5A]図4のRPヘッダのフォーマットを示す説明図であって図4の第1のRPヘッダのフォーマットを示す説明図

[図5B]図4のRPヘッダのフォーマットを示す説明図であって図4の第2のRPヘッダのフォーマットを示す説明図

[図6]図1のUEのパケット送信部を示すブロック図

[図7]図1のUEのパケット送信処理を示すフローチャート

[図8]図1のE-NodeBを示すブロック図

[図9]図1のE-NodeBのパケット受信処理を示すフローチャート

[図10]図1のACGWのパケット受信送信処理を示す説明図

[図11]図1のACGWを示すブロック図

[図12]図1のACGWのパケット受信処理を示すフローチャート

[図13]図1の受信側UEのパケット合成処理を示す説明図

[図14]図1のUEのパケット受信部を示すブロック図

[図15]送信側UEと受信側UEが異なるE-NodeBに接続する場合のシステム構成図

[図16]送信側UEが受信側UEあてパケットをACGW経由で送るパケットの構成を示す説明図

[図17]UE－UE直接通信のパケットの構成を示す説明図

[図18]図16、図17のパケットの構成を詳しく示す説明図

[図19]第2の実施の形態においてUE－UE直接通信時にE-NodeBがACGWに送

るパケットの構成を示す説明図

[図20]第2の実施の形態のUEのパケット送信部を示すブロック図

[図21]第2の実施の形態のUEのパケット受信部を示すブロック図

[図22]第2の実施の形態のE-NodeBを示すブロック図

[図23]第2の実施の形態のACGWを示すブロック図

[図24]第2の実施の形態におけるUE－UE直接通信の場合の各パケットの構成を示す説明図

[図25]第2の実施の形態におけるUE－UE直接通信でない場合の各パケットの構成を示す説明図

[図26]第2の実施の形態におけるシーケンス番号を入れる場合のパケットの構成を示す説明図

[図27]第2の実施の形態における総データバイト数を入れる場合のパケットの構成を示す説明図

[図28]第2の実施の形態におけるUE－UE直接通信時の鍵データ送信パケットの構成を示す説明図

[図29]第2の実施の形態におけるUE－UE直接通信時の鍵データ送信パケットの構成を示す説明図

[図30]第1の実施の形態の具体例、第1、第2の実施の形態の変形例におけるスケーラブル音声符号化装置及び復号装置を示すブロック図

[図31]第1の実施の形態の具体例におけるパケットの構成を示す説明図

[図32]第1、第2の実施の形態の変形例におけるパケットの構成を示す説明図

発明を実施するための最良の形態

[0023] ＜第1の実施の形態＞

以下、図面を参照して本発明の実施の形態について説明する。図1はUE101とUE102が同じ基地局103（以下、E-NodeBと言う。）に無線接続している状態を示す。なお、この状態は、通信開始時からこの状態が継続している場合の他に、図15の状態からUE101又はUE102が移動した場合などが考えられる。この状態では、UE101からUE102に送信を行う場合には、以下に詳しく示す「UE－UE直接通信」に

よりUE101において送信パケットを分割し、ACGW105を経由しない直接ルート(1)とACGW105を経由するACGW経由ルート(2)に分けて転送する。なお、以下では、直接ルート(1)側を経由するパケットを第1のパケット、ACGW経由ルート(2)側を経由するパケットを第2のパケットと呼ぶことにする。

[0024] ＜UE－UE間の通信開始状態＞

UE101－UE102間の通信が開始した最初の状態では、従来どおりにACGW105経由の通信から始まる。送信側UE101は受信側UE102に向けてパケットを生成し、この生成したパケットをACGW105あてに暗号化し、送信する。UE102の送信した暗号化パケットをE-NodeB103が受信し、ACGW105に転送する。ACGW105は受信した暗号化パケットを復号化し、復号化したパケットのあて先からルーティング先を判定する。ACGW105は、UE102あてにパケットを暗号化し、送信する。ACGW105が送信した暗号化パケットをE-NodeB103が受信し、UE102に転送する。受信側UE102は暗号化パケットを受信して復号化し、送信側UE101からのパケットを取得する。本実施の形態では、パケットを暗号化・復号化する方法としてIPsec ESP (Encapsulating Security Payload)のトンネルモードを用いた場合を想定して説明するが、本発明はIPsec ESP方式に限定するものではない。

[0025] ＜UE－UE直接通信開始＞

「UE－UE直接通信」は、ACGW105が送信側UE101と受信側UE102が同一のE-NodeB103に接続していることを検出したときに開始する。この場合、ACGW105はパケットを受信したときの転送元のE-NodeBと転送する先のE-NodeBが同一であることをルーティング処理の際に検出するか、又は、ACGW105が管理するUE101、UE102の情報から検出することなどによって、送信側UE101と受信側UE102が同一のE-NodeB103に接続していることを検出する。ACGW105は、送信側UE101と受信側UE102が同一のE-NodeB103に接続していることを検出した後、それぞれのUE101、102に「UE－UE直接通信」が可能かどうかの問合せを送信する。両方の又はどちらか一方のUEが「UE－UE直接通信機能」に対応していない場合には、「UE－UE直接通信」を行うことができない。両方のUEが「UE－UE直接通信機能」に対応している場合には、それぞれのUE101、102に「UE－UE直接通

信」の通信路設定を指示する。またACGW105はE-NodeB103に対して、UE101、102の間でのパケットの転送を許可するように指示する。

[0026] ＜UE－UE直接通信中＞

送信側UE101はACGW105から「UE－UE直接通信」の指示を受け、受信側UE102あてにパケットを生成した際は、まずUE102あてにパケットを暗号化する。そして、その暗号化したパケットの一部を切り出し、切り出したデータをACGW105あてに暗号化する。送信側UE101は、第1のパケットをUE102あてに(直接ルート(1))、第2のパケットをACGW105あて(ACGW経由ルート(2))に送信する。E-NodeB103は、送信側UE101からの第1、第2のパケットを受信し、UE102あての第1のパケットをUE102あてに、ACGW105あての第2のパケットをACGW105あてに転送する。ACGW105は、E-NodeB103から転送された第2のパケットを受信し、復号処理し、UE102あてに暗号処理し、UE102に転送する。

[0027] 受信側UE102は、UE101から第1のパケットのみを受信した場合、この第1のパケットだけでは意味のあるデータとならないため、受信した第1のパケットを保持して第2のパケットが到着するのを待つ。また逆にACGW105から第2のパケットだけを受信した場合には第1のパケットが到着するのを待つ。受信側UE102は、第1のパケットと第2のパケットを合成して、送信側UE101が生成した元のパケットを復元し、そのパケットを受信処理する。

[0028] ＜UE－UE直接通信終了＞

「UE－UE直接通信」を行うUE101、102が移動するなどによって同一のE-NodeB103に接続している状態ではなくなった場合には、ACGW105はそれぞれのUE101、102に「UE－UE直接通信」の終了を指示する。またE-NodeB103にも通知し、UE101、102との間で直接にパケットの転送を行わないように指示する。

[0029] 以下では、各処理について詳細に説明する。

＜UE－UE直接通信開始＞

UE－UE直接通信を開始する処理に関して、図2、図3A及び図3Bを用いて説明する。最初は、送信側のUE101と受信側のUE102は、ACGW105を経由してパケットを送受信している。送信側UE101は、受信側UE102に向けてパケットを生成し

、生成したパケットをACGW105あてに暗号化し、送信する。送信された暗号化パケットをE-NodeB103が受信し、ACGW105に転送する。ACGW105は受信した暗号化パケットを復号化し、復号化したパケットのあて先からルーティング先を判定する。ACGW105はUE102あてにパケットを暗号化し、送信する。送信されたパケットをE-NodeB103が受信し、UE102に転送する。受信側UE102は暗号化パケットを受信して復号化し、送信側UE101からのパケットを取得する。これがUE－UE直接通信を開始する前の状態である。

[0030] 図2において、ACGW105は、送信側UE101と受信側UE102が同一のE-NodeB103に接続していることを検出する(ステップS21)。例えばACGW105は、パケットを受信したときの転送元のE-NodeBと転送する先のE-NodeBが同一であることから、ルーティング処理の際に検出する。又は、ACGW105が管理するUEの情報から接続しているE-NodeBを調べ、同一のE-NodeBに接続していることを検出する。次に、ACGW105は、送信側UE101と受信側UE102が同一のE-NodeB103に接続していることを検出した後、それぞれのUE101、102に「UE－UE直接通信」が可能か否かの問合せを送信する(ステップS22)。

[0031] この問合せの際のメッセージシーケンスを図3A及び図3Bに示す。図3Aでは、ACGW105がUE1(UE101)とUE2(UE102)に問合せメッセージ(Req)を送信している(ステップS31)。ACGW105は問合せを送信した後、UE101、UE102からの応答を待つ(図2のステップS23)。UE101、UE102は「UE－UE直接通信機能」に対応している場合には、対応していること(OK)と、SPI(SecurityParameters Index)の値(UE101からの応答の場合には、SPI(UE1)、UE102からの応答の場合はSPI(UE2))と、UE101、UE102が対応可能な暗号方式のそれぞれの候補をACGW105に応答として返す(図2のステップS24、図3Aのステップ S32)。

[0032] ACGW105はUE101及びUE102の両方から対応していることを示す応答が返ってきたならば、UE101、UE102にそれぞれ通信相手(UE102、UE101)のローカルアドレス(local address)を通知する(図2のステップS25、図3Aのステップ S33)。この「local address」は、網内のトランスポート用のアドレスである。また、UE101、UE102にそれぞれ通信相手側の指定したSPIの値SPI(UE2)、SPI(UE1)を通知する

(図2のステップS25、図3Aのステップ S33)。この値をつけて暗号化したパケットを送信することによって、受信側はどの条件で復号化処理すればよいのか判別することができる。また、UE101、UE102がそれぞれ提示した暗号方式の候補の中からACGW105が1つを選択し、その暗号方式をそれぞれUE102、UE101に通知する(図3AのステップS33)。共通して使用できる暗号方式が存在しない場合には、「UE－UE直接通信」を開始することはできない。また、UE101、UE102にそれぞれ暗号・復号処理用の共通鍵を通知する。これらのUE101、UE102とACGW105の通信は、UE101－ACGW105間、UE102－ACGW105間の暗号化された通信路を用いて行う。

[0033] 以上は、UE101、UE102の両方が「UE－UE直接通信機能」に対応している場合について説明した。もし、一方でも対応していない場合には、「UE－UE直接通信」を開始することはできない。そのため、もしUE101、UE102の一方のみが問合せに対して、対応していること(OK)を応答として返している場合には、そのUEに対して、「UE－UE直接通信」を行わないこと(NG)を応答として返す(図2のステップS27、図3Bのステップ S34)。以上のメッセージシーケンスによって、UE101、UE102に「UE－UE直接通信」に必要な情報が渡される。UE101、UE102どうしはSA(Security Association)を確立し、このSAを用いて通信することが可能となる(図2のステップS26)。またACGW105は、E-NodeB103に対してもUE101とUE102の間に「UE－UE直接通信」を開始させることを通知する。E-NodeB103は、UE101とUE102との間のパケットの直接の送受信が可能なようにルーティング設定などの内部設定を変更する。

[0034] ＜UE－UE直接通信中＞

UE－UE直接通信中の状態のときのUE101、UE102、E-NodeB103、ACGW105の動作について説明する。「UE－UE直接通信」では、送信側UE101はUE102あてにパケットを生成し、そのパケットの一部をACGW105経由のパケットにし、ACGW105を経由しない第1のパケットと、ACGW105経由の第2のパケットとして送信する。第1のパケットと第2のパケットの両方が受信側UE102に届いて初めて、UE102はパケットの受信処理が可能となる。

[0035] ＜送信側UE101のパケット送信処理＞

送信側UE101のパケット送信処理を図4～図7を用いて説明する。まず、送信側UE101の送信パケットの構造について図4、さらには図5A、図5Bを用いて説明する。送信側UE101は、受信側UE102に送信するデータを作成し、UE102あてのパケット401を作成する。パケット401のあて先(Dt.: Destination Address)はUE102の「global address」(g_UE2)であり、送信元アドレス(Sr.: Source Address)はUE101の「global address」(g_UE1)である。なお、ここでいう「global address」と「local address」の使い分けは、UE101とUE102の通信のために使用するアドレスと、ACGW105、E-NodeB103、UE101、UE102の間でパケットを運ぶためのアドレスを意識的に区別するために、便宜的につけたものである。ネットワークのアドレス管理の方法によっては、ともに「global address」を用いる場合も、逆にともに「local address」を用いる場合も想定される。

[0036] 送信側UE101は、作成したUE102あてのパケット401を暗号化し(暗号化データ401')、次いで暗号化データ401'をカプセル化処理してパケット402を生成する。ここでは「UE－UE直接通信」を行っている場合について説明するが、例えばACGW105に送信する場合には、ACGW105あてにIPsec ESPトンネルモードで暗号化して送信する。

[0037] 暗号化データ401'をカプセル化処理したパケット402では、トンネルヘッダであるIPヘッダ402aのあて先アドレスにUE102の「local address」(l_UE2)を設定し、送信元アドレスにはUE101の「local address」(l_UE1)を設定する。ここで、UE102の「local address」は、ACGW105から「UE－UE直接通信」の指示の際に、通知されているアドレスである。送信側UE101は、UE102あてに暗号化してカプセル化したパケット402を分割し、直接ルート(1)側の第1のパケット404とACGW経由ルート(2)側の第2のパケット406を生成する。

[0038] ここで、直接ルート(1)側のパケット403は、元のパケット402から一部のデータを切り取ったパケットである。ここでは、切り取る一部のデータとして、ESPヘッダ402bとそれに続く暗号化データ401'の一部を切り取ったパケットである。ESPヘッダにはSPIが含まれ、このSPIの値によって受信側ではどの鍵で復号すればよいかを知ることが

できる。すなわち復号処理を行うための識別データの役割を持つ。また、ここでは暗号化データの一部を切り取った場合の例を示しているが、このデータのサイズは任意に調整することができ、そのサイズを0としてもよい。その場合は、暗号化データを含まない方法といえる。またさらに言えばESPヘッダの一部だけでもよく、識別データの一部だけでもよい。すなわち、ここで切り取るデータの意味は、受信側が直接ルート(1)で受信したデータだけでは意味をなさないようにすることである。ただし、本実施例では以下に記載するように切り取った箇所に第1のRPヘッダを上書きするため、切り取る一部のデータはこの第1のRPヘッダより大きいことが求められる。

[0039] なお本実施例では第1のパケットのデータを切り取った箇所を他のデータで上書きする例について説明したが、かかる切り取るデータ(以下データ部とも言う)を切り取り、その切り取った箇所にRPヘッダを挿入する方法でもよい。この場合には、受信側ではRPヘッダを取り除いたところに第2のパケットのデータを挿入すればよい。この場合には切り取るデータは、第1のRPヘッダのサイズには依存せずに決めることができる。

[0040] 図4に示す送信側のパケット処理では、元のパケット402から一部データを切り取った後の残りの部分403aには、0x00で上書きするか、又は意味のないデータで上書きし、受信側のUE102が切り取る前にあったデータを類推できないようにする。そして、パケット403の切り取った部分403aの先頭に第1の置き換え(リプレース、以下、RP)ヘッダ404bを設定してパケット404を生成する。この第1のRPヘッダ404bは、第1のパケット404と第2のパケット406を合成するときに、切り取ったデータ部405を元に戻す位置を示す。また、第1のパケット404のIPヘッダ404a内の「Next Header」領域には、ESPヘッダを示す値が入っているため、その値を第1のRPヘッダ404bを示す値と置き換える。

[0041] 第2のパケット406は、元のパケット402から切り出したESPヘッダ402bとそれに続く暗号化データ401'の一部をデータ部405とするパケットであり、このデータ部405の先頭にIPヘッダ406aと第2のRPヘッダ406bを付加する。IPヘッダ406aは、第1のパケット404のヘッダと同様にあて先アドレスにUE102の「local address」を設定し、送信元アドレスにUE101の「local address」を設定する。第1のパケット404と同じI

Pヘッダであるために、受信側のUE102は、第1のパケット404と第2のパケット406を合成するときに、他のパケットと区別することができる。また、第2のRPヘッダ406bには、第1のパケット404のIPヘッダ404a内にあった「Next Header」の値を含む。すなわちESPヘッダ402bを示す値である。これによって、受信側UE102が第1のパケット404と第2のパケット406を合成する際に、IPヘッダ404a内の「Next Header」の値を元の値に戻すことができる。また、第1のRPヘッダ404bと第2のRPヘッダ406bはRP－ID（RPヘッダ識別子）を含み、同じ値を持つ。これによって、受信側UE102は、パケット404、406を合成するときに他のパケットと取り違えることを防ぐ。

[0042] 第2のパケット406は、ACGW105あてのため、ACGW105あてに暗号化し（暗号化データ406'）、この暗号化データ406'をパケット407にカプセル化処理する。パケット407のトンネルヘッダであるIPヘッダ407aのあて先アドレスはACGW105であり、送信元アドレスはUE101の「local address」である。

[0043] 次に、RPヘッダ404b、406bのフォーマットについてそれぞれ図5A、図5Bを用いて説明する。第1及び第2のRPヘッダ404b、406bは、IPv6（RFC2460）の終点オプションヘッダなどの拡張ヘッダと同様のフォーマットである。RPヘッダ404b、406bの最初の1オクテット（501、504）には、次の拡張ヘッダを示す「Next Header」の値を設定する。第2オクテット（502、505）には、拡張ヘッダ長を示す値（RPヘッダ長）を設定する。続く2オクテット（503、506）にRP－ID、すなわちRPヘッダ404b、406bを一意に識別する識別子を示す値を設定する。そしてそれに続いてオプションを追加する。

[0044] 第1のRPヘッダ404bのフォーマットの場合には図5Aに示すように、最初の1オクテット（501）には、第1のRPヘッダ404bの次にはヘッダがこないため、「No Next Header(59)」の値を設定する。次のオクテット（502）にはRPヘッダ長を、さらに次のオクテット（503）にはRP－IDを設定する。第2のRPヘッダ406bのフォーマットの場合には図5Bに示すように、第1のRPヘッダ404aと同様に、最初の3オクテットのそれぞれ（504、505、506）には「No Next Header(59)」の値、続いてRPヘッダ長、さらにRP－IDを設定する。そして、オプションデータとして元のパケットの「Next Header」の値を設定する。元のパケットの「Next Header」を設定するオプションデータでは、最初の

1オクテット(507)に、元の「Next Header」の値のオプションデータであることを示すオプション番号を設定する。それに続いてオプションデータ長(508)、そして元の「Next Header」の値(509)を設定する。

[0045] なお第2のRPヘッダ406bが持つオプションデータとして、元のパケット402のパケットサイズが考えられる。このオプションデータによって、元のパケット402のパケットサイズをACGW105はこのオプションデータによって知ることができ、UE101とUE102のパケット通信による網の使用状況を把握することが容易になる。なお、上記ではRPヘッダ404b、406bに、RP－IDの領域を設けたが、RP－IDもオプションデータとして扱う方法であってもよい。その場合には、RPヘッダ404b、406bは終点オプションヘッダと同一としてみなすことも可能となる。以上、RPヘッダ404b、406bのフォーマットについて説明した。

[0046] 次に、UE101(及びUE102)のパケット送信部について図6を用いて説明する。「UE－UE直接通信」の開始前の場合、送信側UE101はデータ生成部601において、UE102に送信するデータを生成し、次いでそのデータを用いてパケット生成部602においてUE102あてのパケット401を生成する。生成したパケット401をパケット送信部607に渡し、送信することも可能である。一方、ACGW105に送信する場合には、IPsec暗号処理・カプセル化処理部603において暗号化し、その暗号化パケットをパケット送信部607に渡し、送信する。

[0047] 送信側UE101がACGW105から「UE－UE直接通信」の問合せを受信し、それに応じ、「UE－UE直接通信」を行うことになった場合、送信側UE101は、UE102あてに作成したパケット401をIPsec暗号処理・カプセル化処理部603に渡す。このときはACGW105あてに暗号化するのではなく、「UE－UE直接通信」の指示を受けたときに取得したUE102あての暗号鍵を用いて暗号化する。また、IPsec ESPのカプセル化ではあて先アドレスはUE102の「local address」である。送信側UE101はUE－UE直接通信では、UE102あてに暗号化したパケット402を分割処理部604に渡し、第1のパケット404と第2のパケット406を生成する。具体的には、第1のパケット404を生成する場合には、元のパケット402内のESPヘッダ402bとそれに続く暗号化されたデータ401'の一部を切り出してパケット403を生成し、データ部405を切

り出した領域は、0x00で上書きするか又は意味の無いデータで上書きする。

[0048] 送信側UE101は、RPヘッダ設定部605において、第1のRPヘッダ404bと第2のRPヘッダ406bを作成する。第1のRPヘッダ404bはパケット403に付加して、UE102あてに転送される第1のパケット404を作成し、第2のRPヘッダ406bは第2のパケット406に付加する。第1のRPヘッダ404bは第1のパケット404のESPヘッダ402bの元あった位置に上書きする。これによって、受信側UE102で第1のパケットと第2のパケットを合成する際に、データ部405を戻す位置がわかる。

[0049] また、Next Header 書き換え部606において、第1のパケット404のIPヘッダ404a内の「Next Header」のところに第1のRPヘッダ404bを示す値を設定する。これによって第1のパケット404を受信したノードは、IPヘッダ404aに続いて第1のRPヘッダ404bが置かれていることがわかる。第1のパケット404のIPヘッダ404a内に設定されていた元の「Next Header」の値は、第2のRPヘッダ406b内に設定する。これによって第1のパケット404と第2のパケット406の合成時に、「Next Header」の値を元に戻すことができる。また、第1のRPヘッダ404bと第2のRPヘッダ406bには同じRP－ID（RPヘッダの識別子）を設定する。これによって合成時に第1のパケット404と第2のパケット406を他のパケットと取り違えることを防ぐことができる。

[0050] 第1のパケット404は以上の処理を行ったあと、パケット送信部607に渡し、送信される。第2のパケット406は、データ部405と第2のRPヘッダ406bを持ち、パケット生成部602に渡される。送信側UE101は、パケット生成部602において元のパケット402から切り出したデータ部405と第2のRPヘッダ406bの前に、IPヘッダ406aを付加し、第2のパケット406を生成する。第2のパケット406のあて先はUE102の「local address」である。これは第1のパケット404のIPヘッダ404aと同じである。受信側のUE102では、IPヘッダ404a、406a及びRP－IDによって、第1のパケット404と第2のパケット406を取り違えずに合成することが可能となる。送信側UE101は、IPsec暗号処理・カプセル化処理部603において、第2のパケット406をACGW105あてに暗号化処理及びカプセル化処理し、ACGW105あてのパケット407を生成する。そして、生成したパケット407をパケット送信部607に渡し、送信する。

[0051] 次に図7を参照して送信側UE101の処理を説明する。まず、送信側UE101は図

4に示すような、UE2（UE102）に送信するパケット401を作成する（ステップS71）。次に、送信側UE101は図2、図3A及び図3Bで説明したように、ACGW105から「UE－UE直接通信」の指示を受け、受信側UE102あてにパケットを暗号化するための暗号方式、暗号鍵、SPI（Security Parameters Index）を取得しているので、これらの情報を用いてUE102あての暗号化データ401を暗号化する。このとき、送信側UE101は、受信側UE102あてに暗号化し、IPsec ESP手順を用いてカプセル化し、UE102あてのパケット402を生成する（ステップS72）。

[0052] 次に、送信側UE101は、生成したUE102あてのパケット402の一部（データ部405）を切り出し、一部（データ部405）が切り取られた第1のパケット403と、切り出したデータ部405から新たに生成した第2のパケット406を作成する（ステップS73）。第1のパケット403から切り取られた領域403aは、0x00で上書きするか、又は意味のないデータで上書きする。すなわち、第1のパケット404だけを受信しても、受信側UE102が受信処理できないようにする。具体的に切り出すデータ部405は、元のパケット402のESPヘッダ402bとそれに続く暗号化データ401'である。切り出すデータ部405のサイズは、特に指定はない。ただし、第1のRPヘッダ404bより大きいことが必要である。また切り出すデータ部405が大き過ぎると、ACGW105経由のデータが大きくなるため、望ましくない。第1のパケット403は、UE102あてのパケットであり、第2のパケット406はACGW105を経由してUE102に届くパケットである。なお、切り出したデータの領域を無意味なデータで上書きする方法ではなく、データ領域を取り除きその間に第1のRPヘッダを挿入する方法を用いた場合には、切り取るデータのサイズは第一のRPヘッダより大きいサイズでなくてもよい。

[0053] 送信側UE101は、第1のパケット403のデータを切り出した先頭部分に第1のRPヘッダ404bを付加する（ステップS74）。これは第2のパケット406のデータ部、すなわち切り出したデータ部405を元に戻すときの位置を示す情報となる。また、送信側UE101は、第1のパケット404のIPヘッダ404aにある「Next Header」の値を変更する。切り出し前のパケット402は、ESPヘッダ402bがIPヘッダ402aに続いていたため、IPヘッダ402aにある「Next Header」にはESPヘッダ402bを示す値が設定されている。IPヘッダ404a内のこの値を第1のRPヘッダ404bを示す値と置き換える。こ

れによって、受信側のノードはIPヘッダ404aに続くヘッダを判別でき、ESPヘッダ402bの処理ではなく、第1のRPヘッダ404bの処理を行うことができる。送信側UE101は、この置き換えを行った第1のパケット404をUE102あてに送信する(ステップS75)。すなわち、第1のパケット404はACGW105経由ではなく、E－NodeB103からUE102に直接転送される。

[0054] 一方、送信側UE101は、切り出したデータ部405から第2のパケット406を生成する。第2のパケット406には第2のRPヘッダ406bを付加する(ステップS76)。第1のRPヘッダ404bと第2のRPヘッダ406bには、同じ値のRP－IDが含まれている。このRP－IDによって受信側のノードは、どの第1のパケット404とどの第2のパケット406を合成すればよいのか判別することができる。また、第2のRPヘッダ406bには、元のパケット402の「Next Header」の値が含まれている。すなわち、第1のパケット404と第2のパケット406を合成した際、元のIPヘッダ402aにあった「Next Header」の値を元に戻すための値が、第2のRPヘッダ406b内に含まれている。第2のパケット406のあて先はUE102である。すなわち、第1のパケット404のIPヘッダ404aと同じである。このIPヘッダ404a、406aが同じであることと、RP－IDが同じ値であることによって、受信側ノードは、合成する第1のパケット404と第2のパケット406を判別し、合成する。

[0055] 第2のパケット406は、第1のパケット404のIPヘッダ404aと同じIPヘッダ406aを持ち、それに続いて第2のRPヘッダ406bがあり、それに続いて元のパケット402から切り取ったデータ部405がくる。この第2のパケット406は、ACGW105経由でUE102に届くパケットである。送信側UE101は、第2のパケット406に対してACGWあてのIPsec ESPのトンネルモード処理を行い、第2のパケット407を生成する(ステップS77)。次いで送信側UE101は、第2のパケット407をACGW105あてに送信する(ステップS78)。すなわち、第2のパケット407はACGW105経由で、UE102に転送されるパケットである。

[0056] ＜E-NodeBにおける処理＞

次に、E－NodeB103の構成について図8を用いて説明する。E-NodeB103は、パケット受信部801においてパケットを受信する。E－NodeB103は受信したパケッ

トが自ノードあての場合には、受信パケット処理部802に渡す。転送の必要なパケットの場合にはパケット転送処理部803に渡す。E－NodeB103は、パケット転送処理部803において、転送するパケットの確認を行う。ACGW105からUE101、102に転送するパケットの場合には特に制限はない。また逆にUE101、102からACGW105に転送するパケットの場合にも特に制限はない。UEからUEに転送する場合には、E－NodeB103は転送するパケットが条件を満たしているか確認する。E－NodeB103は、UEからUEにパケットを転送する場合には、UE－UE通信確認部804において、ACGW105から許可されている通信かどうか確認する。また、RPヘッダ確認部805において、そのパケットが第1のRPヘッダ404bを含んでいるか確認する。E－NodeB103は、転送するパケットをパケット送信部806に渡し、送信する。

[0057] 次に、E－NodeB103のパケット中継処理について図9を用いて説明する。E－NodeB103は、自ノードあてのパケットの場合には、自ノードあてのパケットとして受信処理を行う（ステップS91）。例えばACGW105からの指示などの場合がある。E－NodeB103は、自ノードあて以外のパケットの場合、転送処理を行う。このとき、ACGW105から送られてきたパケットかどうか確認を行う。ACGW105から送られてきたパケットの場合には、あて先のUEに転送する（ステップS92）。例えば、ACGW105からUE102に送信される第2のパケット1009（後述）の場合がある。

[0058] 一方、E－NodeB103は、ACGW105からではなくUE101、102から送信されたパケットを転送する場合には、ACGW105あてかどうか確認を行う。UE101、102からACGW105に送信するパケットの場合には、そのままACGW105に転送する（ステップS93）。例えば、UE101からACGW105経由でUE102に送信する第2のパケット407の場合がある。さらに、E－NodeB103は、UEからUEに送信されたパケットを転送する場合には、UE101とUE102の直接通信が許可されているか（ステップS94）、及び第1のRPヘッダ404bが付加されているか確認を行う。直接通信が許可されているかどうかは事前にACGW105より通知がある。第1のRPヘッダ404bを含むかどうかは実際に受信したパケットを調べる。この確認処理はUEから送信されたパケットだけで受信処理が成立しないようにするためである。例えばUE101からUE102に送信する第1のパケット404の場合がある。

[0059] ＜ACGWにおける処理＞

次に、ACGW105のパケット中継処理について図10を用いて説明する。ACGW105が「UE－UE直接通信」のパケット407を受信した場合、パケット407のあて先アドレスはACGW105あて、すなわちACGW105にとって自ノードあてである。このパケット407を復号化処理及びデカプセル化処理を行うと、UE101がUE102あてに生成したパケット406が出てくる。この出てきたパケット406は、あて先がUE102の「local address」であり、送信元がUE101の「local address」である。また、このパケット406は第2のRPヘッダ406bを含む。ちなみに、「UE－UE直接通信」を行っていない場合には、出てくるパケットのあて先アドレスは、UE102の「global address」であり、送信元アドレスはUE101の「global address」である。

[0060] ACGW105は、復号化処理の結果、出てきたパケット406のあて先アドレスを元に転送先を判定する。この場合にはUE102である。ACGW105はIPsec ESPトンネルモード処理を行い、UE102あてに暗号化処理し暗号化データ1008を生成し、カプセル化処理しパケット1009を生成する。パケット1009のIPヘッダ1009aのあて先アドレスは、UE102の「local address」であり、送信元アドレスはACGW105のアドレスである。

[0061] 次に、ACGW105の構成について図11を用いて説明する。ACGW105は、パケット受信部1101においてパケットを受信する。自ノードあてのパケットで暗号化されているパケットの場合には、IPsec復号処理・デカプセル化処理部1102において、復号処理及びデカプセル化処理を行う。ACGW105は、復号化処理を終えて、又は復号化処理の必要のないパケットで、自ノードあてのパケットを受信パケット処理部1103に渡す。転送するパケットは、パケット転送処理部1104に渡す。ACGW105は、パケット転送処理部1104においてパケットの転送処理を行う。その転送先を確認する処理の際に、「UE－UE直接通信」を行っている場合には、UE－UE通信確認部1106において、「UE－UE直接通信」を許可しているかどうか確認する。また、RPヘッダ確認部1107において第2のRPヘッダ406bが含まれているか確認する。

[0062] ACGW105は、UE接続状態検出部1105において、通信しているUEどうしが同じE－NodeBに接続していないかチェックする。同じE－NodeBに接続している場合

には、UEに対して「UE－UE直接通信」の機能に対応しているかどうか問合せを行い、両方のUEが対応している場合には、「UE－UE直接通信」の開始を指示する。ACGW105は、パケット転送処理部1104によって転送先を決定し、IPsec暗号処理が必要なパケットをIPsec暗号処理・カプセル化処理部1108に渡し、暗号処理したパケットをパケット送信部1109に渡し、送信する。IPsec暗号処理の必要ないパケットの場合は、そのままパケット送信部1109に渡し、送信する。

[0063] 次に、ACGW105のパケット中継処理について図12を用いて説明する。ACGW105はパケットを受信し、そのパケットがIPsec暗号化されている場合には、復号化処理とデカプセル化処理を行う(ステップS121)。デカプセル化処理して内部から出てきたパケットが自ノードあてのパケットならば、自ノードあてのパケットとして処理する(ステップS122)。ACGW105は、UEに転送するパケットを受信した場合、あて先アドレスが「local address」かどうか確認する(ステップS123)。「local address」ではなく、「global address」の場合には、UEに転送する。UEに転送する際には、UEあてにパケットを暗号化して送信する(ステップS124)。

[0064] ACGW105は、UEに転送するパケットのあて先アドレスが「local address」の場合には、「UE－UE直接通信」を許可しているかどうか確認する(ステップS125)。「global address」のパケットの場合には、そのパケットはACGW105を経由する。一方、「local address」の場合には、トランスポート用のIPであり、UE102に直接パケットを届けることが可能である。そのためACGW105はあて先アドレスのチェックを行う。またACGW105は、UEの「local address」に転送するパケットの場合には、第2のRPヘッダ406bが付加されているか確認する(ステップS126)。

[0065] これは「UE－UE直接通信」において、一部のデータ部405がACGW105を経由していることを確認するためである。このように元のパケット401の一部のデータ部405がACGW105を経由することによって、ACGW105はUE－UE間のパケット通信を制御する能力が維持される。そのうえ、元のパケット402の全データではないことによって、ACGW105とE-NodeB103との間のネットワークリソースの使用を抑えることができるとともに、ACGW105における暗号・復号処理などの処理負荷を軽減することができる。ACGW105は、第2のRPヘッダ406bを含むUEの「local address」あて

のパケット406から、IPsec ESPトンネルモードを用いて、UEあての暗号パケット1009を生成し、送信する(ステップS127)。

[0066] ＜受信側UEにおける処理＞

次に、受信側UE102のパケット受信処理について図13を用いて説明する。受信側UE102は、第1のパケット404と第2のパケット1009を受信する。第1のパケット404は、送信側UE101がUE102あてに送信し、E-NodeB103がUE102に転送したパケットである。一方、第2のパケット1009は、送信側UE101がACGW105あてに送信し、E－NodeBがACGW105に転送し、ACGW105が復号処理し、さらにUE102に転送するためにUE102あてに暗号化してから送信したパケットである。E-NodeB103はACGW105からのUE102あてのパケット1009を転送し、UE102が受信する。受信側UE102は、第1のパケット404が第1のRPヘッダ404bを含むため、同じRP－IDを持つパケットを受信するまでパケット404を保存する。

[0067] 受信側UE102は第2のパケット1009を受信すると、ACGW105から暗号化されたパケットであるため、ACGW105との間のSA情報により復号処理を行う。復号処理によって出てくるパケット406は、UE101からUE102あてに作成した第2のパケットであり、あて先アドレスはUE102の「local address」であり、送信元アドレスはUE101の「local address」である。また、このパケット406は第2のRPヘッダ406bを含む。受信側UE102は、同じRP－IDを含む第1のパケット404と第2のパケット406を合成する。合成の手順は、第1のパケット404の第1のRPヘッダ404bのところを先頭にして、第2のパケット406のデータ部405を上書きする。さらに、第2のRPヘッダ406bに含まれる「Next Header」の値を第1のパケット404のIPヘッダ404aの「Next Header」の領域に設定する。この合成処理によって、UE101がUE102あてに生成した元のパケット402が復元される。

[0068] 受信側UE102は、合成したパケット402がESPヘッダ402bを含み、UE102あてに暗号化されたパケットであることが判別できるため、UE101との間のSA情報により復号処理を行い、元のパケット401を復元する。復号のための鍵及びSPIは、ACGW105が「UE－UE直接通信」を指示した際にACGW105より取得している情報を使用する。受信側UE102が復号処理の結果として取得するデータは、最初にUE1

01がUE102あてに生成したパケット401であり、あて先アドレスがUE102の「global address」であり、送信元アドレスがUE101の「global address」のパケットである。

[0069] 次に、UE102（及びUE101）のパケット受信部について図14を用いて説明する。受信側UE102は、パケット受信部1401においてパケットを受信する。特に暗号化されているパケットやRPヘッダを含むパケットではない場合には、そのまま受信パケット処理部1406に渡し、受信処理する。受信側UE102が第1のパケット404を受信した場合、第1のパケット404は第1のRPヘッダ404bを含むため、RPパケット保存部1403に渡す。そして、RPパケット検索部1404において、RP－IDの等しいパケットが存在するかチェックする。すでに存在している場合には、RPパケット合成部1405において、2つのパケットを合成する。受信側UE102が第2のパケット1009を受信した場合、ACGW105から暗号化されたパケットであるため、IPsec復号処理・デカプセル化処理部1402において、復号処理とデカプセル化処理を行う。復号化されたパケット406には第2のRPヘッダ406bが含まれているため、RPパケット保存部1403に渡す。「UE－UE直接通信」を行っていない場合には、ACGW105から暗号化されたパケット402を受信した場合、IPsec復号処理・デカプセル化処理部1402において、復号化処理を行ったパケット401を、受信パケット処理部1406に渡す。

[0070] 受信側UE102が第1のパケット404を受信し、RPパケット保存部1403に保存し、また第2のパケット1009を受信してIPsec復号化処理及びデカプセル化処理1402で処理を行い、第2のRPヘッダ406bを含む第2のパケット406をRPパケット保存部1403に保存するとき、RPパケット検索部1404において同じRP－IDを含むパケットを検索した場合には、同じRP－IDを含むパケットが存在するため、RPパケット合成部1405において、第1のパケット404と第2のパケット406を合成する。具体的には、第1のパケット404の第1のRPヘッダ404bの部分を先頭にして、第2のパケット406のデータ部405を上書きする。また、第1のパケット404のIPヘッダ404a内の「Next Header」のところに、第2のRPヘッダ406bに含まれていた「Next Header」の情報を設定する。この合成処理によって、送信側UE101が作成したUE102あての元のパケット402を復元する。受信側UE102は、合成したパケット402がESPヘッダ402bを含む場合には、合成したパケット402をIPsec復号処理・デカプセル化処理部140

2に渡す。受信側UE102はパケット402を復号化処理及びデカプセル化処理し、パケット401を取得し、このパケット401を受信パケット処理部1406に渡す。

[0071] ＜UE－UE直接通信終了＞

「UE－UE直接通信」を終了するときの動作について説明する。ACGW105はUE101、UE102のそれぞれに対して「UE－UE直接通信」を終了するように指示する。また、E-NodeB103に対しても「UE－UE直接通信」が終了したことを通知する。「UE－UE直接通信」が終了するのは、UE101、UE102のそれぞれが同一のE-NodeB103に接続している状態ではなくなったとき、UE101、UE102のどちらか又は両方が他のE-NodeBにハンドオーバしたときが考えられる。また、ACGW105は、UE101、UE102の移動が行われていなくても、ACGW105の判断によって終了させることができる。例えばUE101とUE102の通信を Lawful Interception などの理由によって監視しなければならなくなった場合などが考えられる。

[0072] ACGW105から「UE－UE直接通信」の終了を指示されたUE101、UE102は、パケットを分割・合成する処理をやめて、「パケットの全データをACGW105に送信・ACGW105から受信する方法」に切り替える。ACGW105から「UE－UE直接通信」の終了を通知されたE-NodeB103は、UE101からのパケットをUE102に直接転送する処理を止める。

[0073] なお本明細書では、送信側UE101がUE102あてにパケット401を暗号処理してからパケット402を分割する方法について詳細に説明したが、パケット401の暗号化処理を行わずにパケット402を分割処理することも同様に可能である。

[0074] ＜第2の実施の形態＞

上記の実施の形態を第1の実施の形態として、次に、第2の実施の形態について説明する。以下に、第2の実施の形態の「UE－UE直接通信」のポイント(1)(2)を示す。

(1)UE101は、通信相手のUE102にパケットを暗号化して送信する。暗号化されたパケット(第1のパケット)はE－NodeB103折り返し(ACGW105を介さないで)でUE102に送信される。このとき、暗号化パケットの復号化に必要な鍵をACGW105経由でUE102に送信する(第2のパケット)。鍵データはデータ量が小さいため、E－N

odeB103－ACGW105間の折り返しのデータ量を小さくすることができる。

[0075] 鍵のパケットの対応のバリエーション

・パケットと鍵の対応を、1対1にする。すなわち、パケットの数だけ鍵も送信する。

・パケットと鍵の対応を、N対1にする。すなわち、ある一定の期間のN個のパケットに対して、同じ鍵を用いるようにする。例えば、100個のパケットごとに鍵を変更する。また別の例としては、10分ごとに鍵を変更する。受信側でどの鍵を用いて復号化するかは、IPsecで暗号化している場合には、SPIの値によって区別する。パケットの数Nによって鍵を変更する場合には、カウントする同期がはずれると困るため、各パケットに何個目のパケットかを示すカウンタを入れるなどの対応が考えられる。時間によって鍵を変更する場合には、送信側と受信側の時間の同期をとる必要があり、またパケットが到着するまでにかかる時間を計測する必要も出てくるだろうと思われるので、各パケットに送信側が送信した時刻を入れるという対応も考えられる。

[0076] 鍵の決定方法のバリエーション

・ACGW105が鍵を決め、送信側UE101と受信側UE102に通知する。

ACGW105が送信側UE101－ACGW105、受信側UE102－ACGW105の暗号化パスを用いて鍵を配布する。このとき、鍵と同時にSPIの情報も併せて送信する。このSPI情報は、E－NodeB10されていて見ることができない。

・送信側UE101が鍵を決め、ACGW105経由で受信側UE102に送信する。

送信側UE101－ACGW105の暗号化パスを用いて、送信側UE101からACGW105に鍵が送信され、ACGW105はその鍵を保持し、さらに受信側UE102に転送する。この鍵情報は、E－NodeB103には暗号化されていて見ることができない。

[0077] (2)E－NodeB103は定期的にUE－UE直接通信パケットをACGW105にコピーして転送する(第3のパケット)。

ACGW105は、転送されたパケットを復号化できることを確認する。

オプション:ACGWが復号化できているかどうか確認できるように、送信側UE101に、あらかじめ復号化できたことがわかる情報を付加させるようにする。

E－NodeB103からUE－UE折り返しパケットのコピーが届かなくなったら、ACGW105はUE101、102にUE－UE直接通信を停止させ、ACGW105経由の元の

通信に戻す。

UE－UE直接通信のパケットがE－NodeB103からACGW105に届かなくなったことによって、UE－UE直接通信での通過パケットが少ないことがわかり、直接通信のパケット量が少ないならば、E－NodeB103－ACGW105間の通信量を減らす効果が少なくなったと言えるため、UE－UE直接通信を行わせておく必要はないと言える。そのためACGW105はUE－UE直接通信を中止させ、ACGW105経由の通信に戻させる。

第2の実施の形態の効果：第1の実施の形態と同様に、E－NodeB103－ACGW105間を折り返すデータ量を減らすことによって、Core Networkのネットワークリソースを有効に活用できる。

[0078] 次に、第2の実施の形態の詳細について説明する。まず、第1の実施の形態と同様に、UE101－UE102間の通信は、最初はACGW105経由で行われている。このとき、送信側UE101－ACGW105間と受信側UE102－ACGW105間はそれぞれ別々のIPsecのSAによって保護されている。ACGW105は送信側UE101と受信側UE102とが同じE－NodeB103に接続し、UE－UE直接通信が可能な状況にあることを検出した場合に、送信側UE101と受信側UE102にE－NodeB103折り返しのUE－UE直接通信機能を持つかどうかを確認する。両方のUE101、102がこの機能を持つ場合には、それぞれに対して、UE101－UE102間に直接のIPsecのSAを確立することを指示する。また、E－NodeB103に対しては、UE101とUE102の通信に関して、UE－UE直接通信を許可したことを通知し、E－NodeB103折り返しを行うように指示する。

[0079] UE101とUE102は、ACGW105から通知されたSA情報を用いて、UE－UE直接通信を開始する。UE－UE直接通信を開始した後も、UE101－ACGW105間のSAとUE102－ACGW105間のSAはそのまま保持しておく。このSAはUE101、102とACGW105間の通信が継続するため、その後も使用する。例えば、パケットを復号化するための鍵データをUE101、102－ACGW105間で送信するために使用する。

[0080] 第2の実施の形態について、UE101からUE102にパケットを送信する場合につい

て説明する。UE101はUE102に送信するパケットを生成し、これをIPsecで暗号化する。UE101はこの暗号化されたパケットをE－NodeB103折り返し経路でUE102に送信する。UE102はACGW105から受け取った鍵データを用いて、UE101からのデータを復号化し、受信処理する。E－NodeB103は、UE101－UE102間の直接通信のパケットをACGW105に送信することなく直接相手先のUE102、UE101に転送する。また、ACGW105がUE101－UE102間の通信をチェックするために、E－NodeB103は定期的にUE101－UE102直接通信のパケットをコピーしてACGW105に転送する。

[0081] ACGW105はUE101－UE102間の直接通信のパケットのコピーがE－NodeB103から送信されてきたら、そのパケットを保存している鍵を用いて復号できるか確認する。もし、復号化できない場合には、UE101、UE102、E－NodeB103に指示し、E－NodeB103折り返しの直接通信を停止させ、ACGW105経由の通信に切り替えさせる。

[0082] UE101とUE102のUE－UE直接通信の鍵の更新は、送信側UE（UE101）が定期的に行う。送信側UE101による鍵の更新間隔は数分程度である。この更新間隔は数時間、数日程度であってもかまわない。また、1パケットごとに鍵を更新することも考えられる。送信側UE101により鍵を更新する場合には、送信側UE101が新しい鍵を生成する。UE101はこの鍵データとSPI（Security Parameters index）をACGW105に送信する。UE101が送信する鍵は、新しく更新し作成した鍵データであり、SPIは、どの鍵を利用したらよいかを受信側が識別できるようにするための情報である。ACGW105はUE101から鍵データを受信すると、鍵保存部に鍵データを保存する。この理由は、ACGW105もUE101－UE102間の直接通信のパケットのコピーがE－NodeB103から送信されてきた場合には、実際に復号できるか確認するためであり、UE102と同様に鍵データとSPIを保存しておく。

[0083] ACGW105はUE101から受信した鍵データをUE102に転送する。UE102はUE101から送信された鍵データを、ACGW105経由で受信する。UE102は受信した鍵データを保存し、UE101から暗号化されたパケットが届いたときに復号可能なように備える。また、UE102は、ACGW105に受信応答を返す。UE102からの受信応

答を受信したACGW105は、UE101に受信応答を返す。UE101は、ACGW105から受信応答を受信し、その受信応答によってUE102に新しい鍵で暗号化されたデータを送信しても、UE102が正しく復号化できることを知る。ACGW105は、UE101による鍵更新が行われない場合には、鍵の更新をUE101に要求する。また、鍵の更新の要求が実行されない場合には、UE101、UE102、E－NodeB103に指示し、UE－UE直接通信の状態からACGW105経由の通信に切り替えさせることも可能である。

[0084] 以下、図を用いて説明する。まず、図15に示すように異なるE－NodeB103、104にUE101、102がそれぞれ接続している場合には、UE－UE間の通信がACGW105を経由していても問題はない。しかし、図1に示すように同じE－NodeB103にUE101、102が接続している場合には、ACGW105－E－NodeB103間で同じパケットが往復しており、ネットワークリソースの無駄な使用が発生している。このように同じE－NodeB103に、通信している両方のUE101、102が接続している場合に、ACGW105はそれぞれのUE101、102がUE－UE直接通信に対応しているか問い合わせを行い、両方のUE101、102が対応している場合には、UE－UE直接通信を両方のUE101、102に指示するとともに、E－NodeB103にもUE－UE直接通信を許可したことを通知する。ここまでは、第1の実施の形態と同じである（図2、図3A、図3B参照）。

[0085] UE101とUE102がACGW105を経由して通信している場合、図16に示すように、UE101からUE102に送信するパケット1501は、まずUE102のアドレス（global address）をあて先アドレス（Destination Address）としている。UE101はこのUE102あてのパケット1501をACGW105に送信するために、ACGW105の域内アドレス（local address）あてのパケット1502でカプセル化し、ACGW105に送信する。ACGWあてのパケット1502のデータ部1502cは、IPsecによって暗号化される。

[0086] UE102あてのパケット1501は、Destination AddressがUE102のアドレス（global address, g_UE2）であり、送信元アドレス（Source Address）はUE101のアドレス（global address, g_UE1）である。このUE102あてのパケット1501が暗号化され（図16の1502c）、ACGW105あてのIPヘッダ1502aと、ESP拡張ヘッダ1502bと、ESP Authe

ntication trailer1502dが付加される。ACGW105あてのパケット1502は、域内で通信可能なアドレスでかまわないため、local addressでもよい。ここではlocal addressを用いる場合で説明する。ACGW105あてのパケット1502のDestination Addressは、ACGW105の域内アドレス(local address, l_ACGW)であり、Source AddressはUE102の域内アドレス(local address, l_UE1)である。

[0087] ACGW105がUE101、UE102にUE－UE直接通信を指示した後、UE101が送信するパケット1504は図17に示すようになる。まず、UE101はUE102あてのデータ1501bに、Destination AddressがUE102のアドレス(global address, g_UE2)のヘッダ1501aを付加する。このパケット1501は、先ほど説明したACGW105経由の場合のパケット1501と同様である。このUE102あてのパケット1501を暗号化し(図17の1504c)、IPヘッダ1504aと、ESPヘッダ1504bと、ESP Authentication Trailer1504dを付加する。この付加するIPヘッダ1504aのDestination Addressは、UE102の域内アドレス(local address, l_UE2)である。このUE102の域内アドレスは、上記のACGW105とUE101、102との通信によってUE101に通知されている。

[0088] 図18にIPsec ESP(IETF RFC2406)のパケット構成を示す。Security Parameters Index (SPI)とSequence Numberの部分がESPヘッダ1504bであり、Payload Data 及びPadding, Pad Length, Next Headerが暗号データ1504cであり、Authentication DataがESP Auth.1504dである。IPsec ESPの暗号パケット1504を受信したUEは、Destination Address, Source Address及びSPIを用いることによって、復号に必要な鍵を特定することが可能である。また、各転送パケットごとにSequence Numberを1つずつインクリメントすることにより、転送パケット数を特定することができる。

[0089] 第2の実施の形態の具体例1では、送信側のUEが定期的に鍵を更新する。UE－UE直接通信において双方向で通信している場合には、両方のUEがそれぞれ鍵を更新しなければならない。ここでは、UE101が送信側として鍵を更新する場合を例として説明する。UE101は一定時間間隔で鍵を更新する。鍵を更新する間隔は、送信したパケット1504の数が一定数を超えたときとしてもよい。また、1パケット1504ごとに鍵を更新してもよい。また、一定期間以上鍵を更新しない場合には、ACGW105がUE101に鍵の更新を要求する。ACGW105からの鍵の更新要求後も鍵の更新

が行われない場合には、ACGW105からUE－UE直接通信の中止、ACGW105経由の通信への切り替えを指示されることもある。

[0090] UE101が鍵を更新するとき、UE101は新しい鍵を図16に示したパケット1501、1502と同様にして送信する。UE101が鍵データとして送信する情報は、鍵データとSPI(Security Parameters Index)である。この情報以外に、暗号方式などの他の情報を含めてもよい。UE101が作成した鍵データは、UE102あてのパケット1501によって運ばれる。このパケット1501は、ACGW105あてのパケット1502でカプセル化、及び暗号化される。この鍵データを運ぶパケット1501、1502には、鍵データを運んでいることを示す、拡張ヘッダを付加してもよい。鍵データを含むことを示す拡張ヘッダを含む場合には、ACGW105が鍵データであることを判別する処理が速くなり、鍵データを取得・保持するまでに要する時間を短くすることができる。また、同様にUE102あてのパケット1501にも鍵データを含むことを示す拡張ヘッダを含む場合には、UE102が鍵データであることを判別する処理が速くなり、鍵データを取得・保持するまでに要する時間を短くすることができる。

[0091] 次に、E－NodeB103の動作を説明する。UE101、102がACGW105経由で通信している場合は普通の状態であるため、E－NodeB103は基本的に、ACGW105からのパケットをUE101、102に送信し、UE101、102からのパケットをACGW105に送信する。UE101、102からのパケットをUE102、101に転送することはない。UE－UE間の通信がE－NodeB103で折り返し、ACGW105を経由しない場合には、網側はUE－UE間でパケットがどのように通信されているか把握することができなくなり、またLawful Interceptionを行う必要が生じたときにも、パケットを傍受できない。このためUE－UE間の通信パケットをE－NodeB103で折り返す場合は、ACGW105が許可した場合だけに限定する必要がある。ACGW105が許可する場合として、E－NodeB103－ACGW105間でパケットが折り返すことになりネットワークリソースが浪費されている場合がある。このような理由により、E－NodeB103はACGW105からの指示があったUE－UE間の通信の場合にのみパケットをACGW105を通過させずにUE101、102に直接転送する。

[0092] 送信側のUEが作成し、ACGW105に送信するパケット1502は、図16に示すよう

にDestination AddressがACGW105の域内アドレス(l_ACGW)である。一方、UE102に送信するパケット1504は、図17に示すようにDestination AddressがUE102の域内アドレス(l_UE2)である。E－NodeB103はこの域内アドレスからACGW105あてのパケット1502か、UEあてのパケット1504かを判別し、さらにUEあてのパケット1504の場合には、許可されているパケットかどうかを確認する。そして許可されている場合のみ、UE102にパケットを転送する。UE-UE直接通信が許可されていない場合には、そのままパケットを破棄する。そのままパケットを破棄する場合以外の方法としては、ACGW105にパケットを転送し、ACGW105からUE101、102にエラー通知する方法や、ACGW105から「ACGW105経由の通信」に切り替えるように指示する方法も考えられる。または、E－NodeB103からエラー通知をUE101、102に送信する方法も考えられる。

[0093] E－NodeB103は、UE－UE直接通信のパケット1504を定期的にコピーしてACGW105に転送する。パケット1504をコピーしACGW105に送信する間隔は、ACGW105からUE－UE直接通信の指示を受け取ったときに通知されている。この間隔は時間で指定される。数分間くらいを指定してもよい。それより長い間隔でも、逆に短い間隔でもよい。または、通過するパケット1504の数で指定してもよい。パケット1504が100個通過するごとにコピーしACGW105に転送するようにACGW105が指定してもよい。または、すべてのパケット1504をコピーしてACGW105に転送するようにACGW105が指定してもよい。このコピーしてACGW105に転送する間隔は、ACGW105が必要に応じて変更することができる。変更する場合はE－NodeB103にUE－UE直接通信の許可を通知する方法と同じ方法を用いる。

[0094] E－NodeB103がACGW105にUE－UE直接通信のパケットを転送する場合のパケット構成図を図19に示す。E－NodeB103に届くパケット1505は、UE102の域内アドレス(l_UE2)をDestination Address(IPヘッダ1505a)とするパケットである。データ部1505はUE102が復号化できるように暗号化されている。このパケット1505をACGW105の域内アドレス(l_ACGW)をあて先とするIPヘッダ1506aを付加して(パケット1506)、ACGW105あてに送信する。E－NodeB103からACGW105あてに送信するパケット1506は暗号化する必要はない。ただし、暗号化して転送しても

かまわない。

[0095] 次に、各装置のブロック図を用いて第2の実施の形態の各装置の処理動作を説明する。UE101、102では送信部と受信部に分けて説明する。最初に図20を参照して、パケット送信部10を説明する。UE101、102はパケットを送信するとき、ACGW105あてのパケットを送信する場合には、データ作成部11によって作成したデータをパケット作成部12においてACGW105あてのパケットにし、IPsec暗号処理部13においてACGW105あてに暗号化し、パケット送信部14によって送信する。ACGW105あてのパケットを暗号化する場合の鍵データは、ACGW105より通知され鍵データ蓄積部16に保存されているデータを用いる。

[0096] UE101がUE102あてのパケット1501をACGW105経由で送信する場合には、UE102あてのデータ1501bをデータ作成部11において作成し、UE102あてのパケット1501をパケット作成部12において作成する。このパケット1501を同じパケット作成部12においてACGW105あてのパケット1502でカプセル化し、IPsec暗号処理部13においてACGW105あてに暗号化し、パケット送信部14より送信する。UE101がUE102あてのパケット1503をUE-UE直接通信する場合には、UE102あてのデータ1501bをデータ作成部11において作成し、UE102あてのパケット1501をパケット作成部12において作成する。このパケット1501をIPsec暗号処理部13においてUE102あてに暗号化し、パケット送信部14により送信する。UE102あての暗号用の鍵データは、鍵データ蓄積部16よりIPsec暗号処理部13が取得する。

[0097] UE101がUE102あてに送信する鍵データは、鍵データ作成部15によって作成される。作成された鍵データは鍵データ蓄積部16に保存される。UE101は、新しく作成した鍵データをパケット作成部12に渡し、UE102あてのパケット1501を生成し、さらに同じパケット作成部12においてACGW105あてのパケット1502でカプセル化し、IPsec暗号処理部13においてACGW105あてに暗号化し、パケット送信部14より送信する。

[0098] 次に、図21を参照してUE101、102のパケット受信部20を説明する。UE101、102はパケット受信部21においてパケットを受信する。パケットが暗号化されている場合には、IPsec復号処理・デカプセル化処理部22において復号化処理を行い、受信

パケット処理部23に渡す。パケットが暗号化されていない場合には、パケット受信部21から受信パケット処理部23に渡される。受信パケット処理部23において、パケットによって鍵データが運ばれている場合には、鍵データを鍵データ蓄積部24に渡し、鍵データを蓄積する。蓄積された鍵データは、IPsec復号処理・デカプセル化処理部22において復号処理に用いられる。

[0099] 次に、図22を参照してE－NodeB103のブロック図を説明する。E－NodeB103はパケット受信部31においてパケットを受信する。E－NodeB103あてのパケットの場合には受信パケット処理部32によって処理する。E－NodeB103あてのパケットにはACGW105から送信されるUE－UE直接通信の許可を通知するメッセージがある。E－NodeB103はE－NodeB103あて以外のパケットをパケット転送処理部33によって転送処理する。UE101、102からACGW105に送信されるパケットや、ACGW105からUE101、102に送信されるパケットの場合には、そのままパケット送信部34より送信される。UEからUEに送信されるパケットを転送する場合には、そのパケットがUE-UE直接通信を許可されたパケットかどうかUE-UE通信確認部35により確認し、許可されている場合のみパケット送信部34より送信される。さらにUE－UE直接通信が許可されている場合には、定期的にパケットコピー処理部36によってUEから送信されたUE-UE直接通信のパケットはコピーされ、ACGW105あてのパケットに入れられて、パケット送信部34よりACGW105あてに送信される。

[0100] 次に、図23を参照してACGW105のブロック図を説明する。ACGW105はパケット受信部41においてパケットを受信する。受信したパケットが暗号化されていない場合には、受信パケット処理部42によって受信処理を行う。暗号化されているパケットの場合には、IPsec復号処理・デカプセル化処理部43において復号化し、ACGW105あてのパケットの場合には、受信パケット処理部42に渡し、受信処理を行う。ACGW105あてでなく他の通信装置あてのパケットの場合には、パケット転送処理部44に渡す。パケット転送処理部44では、転送する際に暗号化が必要ならばIPsec暗号処理・カプセル化処理部45に渡し、パケット送信部46より送信する。暗号化が必要ないならばそのままパケット送信部46に渡す。

[0101] ACGW105はパケット転送部44におけるUE接続状態検出部47において、通信

しているUEどうしが同じE－NodeB103に接続していないか確認する。また、UE－UE直接通信許可判定部48において、UEどうしの通信量が多いかどうか、UE－UE間のLawful Interceptionが必要となってないかどうかなどを確認し、UE-UE直接通信をUE101、102に指示するかどうかを判定する。

[0102] ACGW105は暗号化されているパケットを受信した際、又は暗号化してパケットを送信する際の鍵データを鍵データ蓄積部49から取得する。受信したパケットの復号化は、IPsec復号処理・デカプセル化処理部43によって行い、送信パケットの暗号化は、IPsec暗号処理・カプセル化処理部45によって行う。UE101、102からUE101、102が使用する鍵データが送信された場合には、鍵データのパケットをパケット受信部41で受信し、IPsec復号処理・デカプセル化処理部43で復号化し、受信パケット処理部42に渡す。受信パケット処理部42で鍵データを取り出し、鍵データ蓄積部49に保存する。

[0103] E－NodeB103からUE－UE直接通信パケットがコピーして送信されてきた場合には、パケット受信部41により受信し、受信パケット処理部42によってUE－UE直接通信のパケットが取り出され、このパケットをIPsec復号処理確認部50によって復号処理が行えるかどうか確認する。IPsec復号処理確認部50は、鍵データ蓄積部49より鍵データを取り出し、復号処理を行う。以上、各装置101、102、103、105の動作をブロック図を用いて説明した。

[0104] 次に、図24を参照してUE－UE直接通信中のパケット構成について説明する。図24中の(1)、(2)、(3)、(4)についてそれぞれ説明する。

(1)UE1(UE101)は、UE2(UE102)あてのデータを送信するために、UE2(g_UE2)あてのパケット1501を作成し、このパケット1501をUE2(l_UE2)あてのパケット(第2の実施の形態の第1のパケット)1504でカプセル化し、送信する。このパケット1504はE－NodeB103によってUE2に転送される。

(2)UE1は、UE2あてに鍵データを送信するために、UE2(g_UE2)あてのパケット1501を作成し、このパケット1501をACGW(l_ACGW)あてのパケット1502(第2の実施の形態の第2のパケット)でカプセル化し、送信する。このパケット1502はE－NodeB103によってACGW105に転送される。更にこのパケット1502はACGW105で

処理されて、パケット1504、1501としてUE2に転送される((4)参照)。

[0105] (3)E－NodeB103がUE1－UE2の間のUE－UE直接通信のパケット1505をコピーしてACGW105に送信する場合、E－NodeB103はUE2(l_UE2)あてのパケット1505をACGW105(l_ACGW)あてのパケット(第2の実施の形態の第3のパケット)1506でカプセル化し、ACGW105に送信する。カプセル化される内部パケット1505は、(1)で生成されたパケット1504である。

(4)ACGW105は、UE2(g_UE2)あての鍵データを含むパケット1501を、UE2(l_UE2)あてのパケット1504(第2の実施の形態の第2のパケット)でカプセル化し、送信する。このパケット1504はE－NodeB103によってUE2に転送される。UE2(g_UE2)あての鍵データを含むパケット1501は、UE1によって作成されたパケット1501である((1)参照)。

[0106] UE－UE直接通信でない場合には、次の図25のように通信が行われる。先のUE－UE直通通信の図24で使用した番号と同じ番号を使うと、(2)と(4)を用いて、UE1はUE2にデータを送信する。この場合には、(1)と(3)のパケットの流れは無い。

[0107] 次に、UE1－UE2間の通信パケットにシーケンス番号を入れる場合について説明する。ACGW105がUE1－UE2間のUE－UE直接通信のデータ量を把握する方法として、UE1－UE2間の通信パケットに送信側がシーケンス番号を入れる方法が考えられる。シーケンス番号を入れる方法としては、図26のように新しくシーケンス番号を含むことを示す拡張ヘッダをIPヘッダとデータの間に入れる方法が考えられる。図26は、UE2(g_UE2)あてのパケット1501のIPヘッダ1501aとUE2あてのデータ1501bの間にシーケンス番号1501cを含む拡張ヘッダを付加している例である。UE1はこのUE2(g_UE2)あてのパケット1501をUE2(l_UE2)あてのパケット1504でカプセル化して、送信する。同様に、ACGW105あてに送信する場合には、このシーケンス番号を含むパケット1501をACGW(l_ACGW)あてのパケットでカプセル化して、ACGW105に送信する。また、別のシーケンス番号を入れる方法としては、IPヘッダの未定義領域を用いる方法、Hop-by-Hop Option拡張ヘッダに、オプションとして付加する方法、Destination Option拡張ヘッダにオプションとして付加する方法などが考えられる。

[0108] UE—UE間のパケット数をACGW105が把握する方法として、UEがパケットにシーケンス番号1501cを付加する方法について説明した。この方法では番号によってUE1が送信したパケット1504の個数をACGW105が把握することができる。また、図27に示すようにパケット1501にシーケンス番号1501cではなく通信開始からの総データ量(総データバイト数1501d)を入れることも考えられる。また、シーケンス番号1501cと総データバイト数1501dの両方をパケット1501のIPヘッダ1501aとデータ1501bの間に拡張ヘッダとして入れる方法も考えられる。

[0109] 以上では、UE－UE間のシーケンス番号(パケット数)やデータ量をACGW105がUE1、UE2からのパケットによって把握する方法について説明したが、E－NodeB103から報告を受けるという方法でもよい。また、上記の説明はUEが送信する各パケットにパケット数、データ量などの情報を付加する方法について説明したが、定期的にUEがACGWにパケット数、データ量などの情報を通知するという方法であってもよい。

[0110] 次に、図28を参照してUE1からUE2への鍵データを送信する場合について説明する。UE1はUE2に鍵データを送信するとき、UE2(g_UE2)あてのパケット1501を作成し、このUE2あてのパケット1501をACGW(l_ACGW)あてのパケット1502でカプセル化し、送信する。ACGW105は、UE2あてのパケット1501の中身を確認し、鍵データが含まれている場合には、その鍵データを取得し、保持する。

[0111] ACGW105及び受信側のUE(UE2)が、UE1から送信されたパケットに鍵データが含まれているかどうかを判別するために、次のような方法が考えられる。

・IPヘッダのプロトコル番号に新しく鍵データを含むことを示す番号を定義する。この方法ならば、IPヘッダのプロトコル番号を確認するだけで鍵データが含まれるかどうか判別できる。この方法の延長として、鍵データを含むことを示す拡張ヘッダを定義する方法も考えられる。

・また、Destination Option拡張ヘッダを用いて鍵データを運ぶために、新たに鍵データ用のオプションを定義する。この方法ならば、Destination Option拡張ヘッダを走査するだけで鍵データが含まれるかどうか判別できる。

[0112] どちらの場合も概念的に図29に示すと、IPヘッダ1501aに続いて鍵データを含む

ことを示す情報1501eがあり、その後に鍵データ1501fが含まれる。また、鍵データをTCP(Transmission Control Protocol)やUDP(User Datagram Protocol)を用いて送信する方法や、ICMP(Internet Control Message Protocol)メッセージを用いて通信する方法なども考えられる。この場合にはACGW105は、TCPやUDPの中まで走査し、メッセージを解析し、鍵データを取り出す。

[0113] 以上では、鍵データをUE1がUE2あてに送信するためにパケット1501を作成し、ACGW105がそのパケット1501を解析することによって鍵データを取得する方法について説明した。この方法以外に、UE1がACGW105あてに鍵データを送信し、ACGW105がUE2に転送する方法であってもよい。その場合も上述したように鍵データは転送される。以上、鍵データをACGW105経由でUE1からUE2に送信する方法について説明した。

[0114] ＜データ分割の例＞

次にデータ分割の例を説明する。ここで、データ分割の例として、スケーラブル音声符号化を使用した場合について説明する。スケーラブル音声符号化とは、音声データの符号化時に基本音声データ部と音質向上用データ部(拡張データ)に分ける符号化方法である。従来技術には例えば非特許文献3、特許文献1などがあり、非特許文献3では、広帯域音声(～7kHz)を低域信号(～4kHz)と高域信号(4kHz～7kHz)に分割する例が記載されている。また、特許文献1には音声帯域を3分割する例が記載されている。このスケーラブル音声符号化を用いることによって、2つの効果が得られる。1つは、拡張データが失われても基本音声データが受信側に届けば音声の再生を行うことができることである。もう1つは、拡張データが届いても基本音声データが届かなければ受信側で音声再生を行うことができないことである。

[0115] この2つの効果について、非特許文献3のP. 1108に次のように記載している。

「このため音質保証拡張コーデックや高域部拡張コーデックの符号化列がパケットロスにより欠落しても、コアコーデックの符号化列が到着していれば、狭帯域の音声信号は復号することができ、音切れを防止することが可能である。しかし、コアコーデックの符号化列を格納するパケットがパケットロスにより欠落すると音声の再生が行えなくなってしまう。」

また、特許文献1の段落0017、0023、0025では、スケーラブル音声符号化したデータをパケット送信する際に、基本音声データと音質向上用の拡張データを別のパケットで送信し、基本音声データが通信中に損失することがないようにパケットの優先度を高くすることが記載されている。

[0116] 一方、本発明は、第1の実施の形態の具体例、第1、第2の実施の形態の変形例において、基本音声データがなければ音声の再生ができないことを積極的に活用する。本発明では、送信側UE101において送信音声データをスケーラブル音声符号化によって基本音声データと音質向上用の拡張データに分割し、基本音声データをACGW105経由で、拡張データをE－NodeB103折り返しで受信側UE102に送信する。受信側UE102は、ACGW105経由の基本音声データが届かなければ音声の再生を行うことができない。また、本発明の新しい効果として、ACGW105経由で基本音声データを通信するため、ACGW105では必要なときに通信傍受(Lawful Inspection)を行うことができる。

[0117] ＜ポイント＞

(1)送信側のUE101は、通信相手の受信側UE102に音声データをパケットを用いて送信する。このとき、スケーラブル音声符号化を用いて音声データを符号化し、パケットデータとして送信する。スケーラブル音声符号化では、音声データを基本音声データと拡張音声データに分ける。送信側UE101は、音声再生に不可欠な基本音声データをACGW105経由で送信し、音質向上用の拡張音声データをE－NodeB103折り返しで送信する。基本音声データは音声データ全体を送信するときと比べて小さいため、E－NodeB103－ACGW105間の折り返しのデータ量を小さくすることができる。さらに新しい効果として、基本音声データのみであっても、音質は劣化しているが再生することが可能なため、ACGW105において通信傍受を行わなければならなくなった場合に、容易に通信傍受を開始できる。

[0118] ＜音声データのパケット送信方法のバリエーション＞

・パケット内を分割する方法に適用(第1の実施の形態の具体例)

まず、1つのパケット内にスケーラブル符号化した基本音声データ部と音質向上用データを含む音声データ全体を乗せる。そして、基本音声データ部と音質向上用デ

ータを分割して、それぞれをACGW105経由、E－NodeB103折り返しで送信する。

・パケットを別々に用意し、送信する方法に適用（第1、第2の実施の形態の変形例）

音声データをスケーラブル符号化し、基本音声データと音質向上用データをそれぞれ別のパケットに乗せて送信する。第2の実施の形態の鍵データの代わりに基本音声データを乗せたパケットをACGW105経由で、音質向上用データを乗せたパケットをE－NodeB103折り返しで送信する。

[0119] ＜効果＞

E－NodeB103－ACGW105間を折り返すデータ量を減らすことによって、コア・ネットワーク（Core Network）のネットワークリソースを有効に活用できる。また、ACGW105にはスケーラブル音声符号化による基本音声データ部だけが流れるが、この基本音声データのみであっても通信傍受が可能であるため、ACGW105では、必要となった場合に容易に通信傍受を開始できるという効果がある。

[0120] ＜実施例＞

最初に、スケーラブル音声符号化を用いた音声データの分割方法について説明し、次に音声データをパケットで伝送する方法について説明する。図30において、送信側通信装置における符号化装置2000は、マイクロホン（MIC）、A／D変換器、帯域分割フィルタからの入力音声データ（PCMデータ）をスケーラブル音声符号化方法を用いて符号化する。スケーラブル音声符号化方法では、基本音声データ符号化器2001と拡張音声データ符号化器2002において音声データをそれぞれ符号化し、基本音声データと拡張音声データを生成する。基本音声データ符号化器2001と拡張音声データ符号化器2002とは符号化に用いるサンプリング周波数が異なり、低周波成分を基本音声データとして符号化し、高周波成分を拡張音声データとして符号化する。また、拡張音声データ符号化器2002に基本音声データの符号化データを入力することによって、基本音声データとの差分データである拡張音声データを生成する。送信側通信装置は、符号化した音声データをパケット送信器2003によりパケット化し、受信側通信装置（復号装置2010）に送信する。送信されたパケットはIP網や無線網を経由して受信側通信装置に届く。

[0121] 受信側通信装置における復号装置2010は、パケット受信器2011においてパケットを受信し、符号化された音声データをそれぞれ基本音声データ復号器2012及び拡張音声データ復号器2013に渡す。拡張音声復号器2013では基本音声データ復号器2012からの出力を受け、拡張音声データを復号する。受信側通信装置は、基本音声データ復号器2012及び拡張音声データ復号器2013からの出力を加算器2014で合成し、復号音声(PCMデータ)を不図示のD／A変換器、スピーカ(SP)を介して再生する。

[0122] 次に、スケーラブル音声符号化したデータのパケット送信方法を説明する。音声符号化データのパケット送信方法は次の2通りが考えられる。1つは、1つのパケット内に基本音声データ及び拡張データを乗せる方法に適用する。この場合には第1の実施の形態のように、送信するパケットの中から基本音声データ部を切り出し、切り出した基本音声データ部をACGW105経由で送信する。もう1つは、基本音声データと拡張データを別々のパケットに乗せる方法に適用する。この場合には、第2の実施の形態の鍵データの代わりに、基本音声データを乗せたパケットをACGW105経由で送信する。

[0123] まず、図31を参照して1つのパケットに基本音声データ及び拡張データを乗せる方法に適用する場合について説明する。送信側通信装置(UE101)から受信側送信装置(UE102)に送信する音声データ2020のパケット2021への格納方法は、図31のように基本音声データ2020aに続いて拡張音声データ2020bを配置するようにする。このパケット2021のIPヘッダ2021aにおける宛先アドレスはUE(local address)である。このパケット2021から基本音声データ2020aを切り出し、切り出した基本音声データ2020aにIPヘッダ2022aと第2のRPヘッダ2022bを付加する。新しく付加したIPヘッダ2022aの宛先アドレスはUE(local address)である。この新しく生成したパケット2022をACGW105あてに暗号化し(図の2023)、IPヘッダ2024a及びIPsec ESP拡張ヘッダ(図中、単にESPヘッダと記す)2024bを付加する。新しく生成したパケット2024はACGW105あてに送信し、ACGW105経由で受信側通信装置(受信側UE102)に届く。

[0124] 基本音声データ2020aを切り出した残りのパケット2025には、切り取り部2025bに

第1のRPヘッダ2026bを付加する。このパケット2026はE－NodeB103で折り返して受信側通信装置（受信側UE102）に届く。拡張音声データを含むこのパケット2026は暗号化処理を行わなくてもよい。拡張音声データのみでは再生することができないからである。なお、基本音声データ2020aを切り出す例について説明したが、切り出すデータ部は、基本音声データ2020aの全部と拡張音声データ2020bの一部であってもよい。また、ACGW105での通信傍受の効果は得られなくなるが、切り出すデータ部は基本音声データ2020aの一部だけであってもよい。この場合であっても、受信側で両方のデータがそろわなければ再生できないという効果が得られる。

[0125] 次に、図32を参照して基本音声データ2020aと拡張音声データ2020bを別々のパケットに乗せる方法に適用する場合について説明する。送信側通信装置（送信側UE101）は、基本音声データ2020aと拡張音声データ2020bをそれぞれ別のIPパケット2030、2033に格納する。それぞれのIPパケット2030、2033の宛先は受信側UE102（local address）である。基本音声データ2020aを含むパケット2030は、ACGW105あてに暗号化し（図の2031）、さらにIPヘッダ2032aとIPsec ESPヘッダ（図中、単にESPヘッダと記す）2032bを付加する。暗号化された基本音声データ2031を含むパケット2032はACGW105経由で受信側UE102に届く。拡張音声データ2020bを含むパケット2033、2034はE－NodeB103で折り返され、受信側UE102に届く。この拡張音声データ2020bを含むパケット2033、2034は暗号化しなくてもよい（パケット2033、2034は同じ）。拡張音声データ2020bだけでは再生することができないからである。

[0126] UE101、102の送信部の構成は、図6に示すデータ作成部601（及びパケット作成部602）において図30に示す符号化装置2000を備えることにより、上記のパケット内を分割して送信する方法と個別パケットで送信する方法で基本音声データ2020aと拡張音声データ2020bを分割して送信することができる。また、UE101、102の受信部の構成は、図14に示す受信パケット処理部1406において図30に示す復号装置2010を備えることにより、上記の方法で分割された基本音声データ2020aと拡張音声データ2020bを復号、合成することができる。さらに、ACGW105では、図11に示すパケット転送処理部1104において通信傍受用の音声再生処理行うことがで

きる。

[0127] ＜他の実施例＞

ここで、本発明は、音声データだけではなく、映像データを含んだ場合にも適用することができる。例えばMPEG2を用いる場合には、フレーム内符号化データであるIピクチャだけをACGW105経由で送信し、フレーム間差分予測符号化データであるP、Bピクチャをe－NodeB103折り返しで送信する。また、MPEG4やH．264／AVCを用いる場合には、画面内予測符号化データであるIスライスだけをACGW105経由で送信し、画面間差分予測符号化データであるP、Bスライスをe－NodeB103折り返しで送信する。P、Bピクチャ（P、Bスライス）は差分データであるため、受信側UE102はIピクチャ（Iスライス）がないと復号できないが、Iピクチャ（Iスライス）はそれだけで復号できるので、ACGW105は通信傍受が可能となる。また、MPEG2では例えば15フレームの先頭フレームはIピクチャでなければならないと定められているので、この先頭フレームのIピクチャのみをACGW105経由とすれば、ネットワークリソースを効率的に使用することができ、また、ACGW105の負荷を軽減することができる。

[0128] 上記実施の形態では、第三世代携帯電話（3GPP：登録商標）におけるACGW105、e－NodeB103を例にして説明したが、他のシステムにも適用することができる。例えばIEEE 802．11におけるアクセス・コントローラ（Access Controller）、アクセスポイント（Access Point）にそれぞれACGW105、e－NodeB103を適用することができ、また、以下に示すCAPWAP（Control And Provisioning of Wireless Access Points）におけるアクセス・コントローラ（Access Controller）、WTP（Wireless Termination Point）にそれぞれACGW105、e－NodeB103を適用することができる。

RFC4118 “Architecture Taxonomy for Control and Provisioning of Wireless Access Points (CAPWAP)”, http://www.ietf.org/rfc/rfc4118.txt

[0129] また、UE101、102が同一のe－NodeB103に接続する場合について説明したが、物理的に同一のe－NodeB103であることに限定するものではない。物理的には異なるe－NodeB装置であっても論理的に同一のe－NodeB装置とみなせる場合にも適用可能である。この場合には、e－NodeBで折り返すデータは、複数のe－N

odeBの間で伝送されたあと受信側UE102に送信される。この場合であっても、E－NodeBとACGW105間に伝送されるパケットデータ量を削減するという本発明の効果を同様に得られる。さらに、第三世代携帯電話のアーキテクチャと無線LANのアーキテクチャの混在した環境においては、E－NodeBとAccess PointやWTPなどが混在したネットワークが形成されるが、そのようなネットワークにおいても、ACGWやAccess Controllerに送信するデータを一部だけに限定し、他の大部分のデータをE－NodeB、Access Point、WTP間で折り返すように適用することも可能である。

[0130] なお、上記実施の形態の説明に用いた各機能ブロックは、典型的には集積回路であるLSIとして実現される。これらは個別に1チップ化されてもよいし、一部又はすべてを含むように1チップ化されてもよい。ここでは、LSIとしたが、集積度の違いにより、IC、システムLSI、スーパーLSI、ウルトラLSIと呼称されることもある。また、集積回路化の手法はLSIに限るものではなく、専用回路又は汎用プロセッサで実現してもよい。LSI製造後に、プログラムすることが可能なFPGA（Field Programmable Gate Array）や、LSI内部の回路セルの接続や設定を再構成可能なリコンフィギュラブル・プロセッサーを利用してもよい。さらには、半導体技術の進歩又は派生する別技術によりLSIに置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて機能ブロックの集積化を行ってもよい。例えば、バイオ技術の適用などが可能性としてあり得る。

産業上の利用可能性

[0131] 本発明は、送信側と受信側の無線端末が同じ無線中継装置に無線接続している場合にネットワークリソースを効率的に使用することができ、また、制御装置の負荷を軽減することができるとともに、制御装置が無線端末の通信を管理することができるという効果を有し、3GPP（登録商標）、IEEE 802.11、CAPWAP（Control And Provisioning of Wireless Access Points）などのネットワークなどに利用することができる。

請求の範囲

[1] 無線端末と相互に無線通信を行う無線中継装置と、前記無線中継装置との間でパケット転送を行うとともに前記無線端末及び無線中継装置間の無線通信を管理する制御装置とを備えた通信システムにおいて、

送信側の無線端末は、受信側の無線端末が同一の無線中継装置に接続されている場合に、前記受信側の無線端末あての送信パケットを、前記制御装置を介さない第1のパケットと前記制御装置を介する第2のパケットに分割して前記無線中継装置に送信し、

前記無線中継装置は、前記送信側の無線端末から送信された前記第1及び前記第2のパケットを受信して、前記第1のパケットを前記受信側の無線端末に送信するとともに前記第2のパケットを前記制御装置に送信し、

前記制御装置は、前記無線中継装置から送信された前記第2のパケットを受信して前記無線中継装置に送信し、

前記無線中継装置は、前記制御装置から送信された前記第2のパケットを受信して前記受信側の無線端末に送信し、

前記受信側の無線端末は、前記無線中継装置から送信された前記第1及び前記第2のパケットを受信して元のパケットを復元することを特徴とする通信システム。

[2] 前記送信側の無線端末は、前記受信側の無線端末あての送信データを暗号化して、前記暗号化データを前記受信側の無線端末側で復号するための識別データを取り除いた前記第1のパケットを生成するとともに、前記識別データを含む前記第2のパケットを生成し、

前記受信側の無線端末は、前記第2のパケット内の前記識別データを、前記第1のパケット内の前記識別データが切り取られた部分にセットして前記第1のパケット内の前記暗号化データを復号することを特徴とする請求項1に記載の通信システム。

[3] 前記送信側の無線端末は、前記受信側の無線端末あての送信データを暗号化して、前記暗号化データを前記受信側の無線端末側で復号するための識別データ及び前記暗号化データの一部を取り除いた前記第1のパケットを生成するとともに、前記識別データ及び前記暗号化データの一部を含む前記第2のパケットを生成し、

前記受信側の無線端末は、前記第2のパケット内の前記識別データ及び前記暗号化データの一部を、前記第1のパケット内の前記識別データ及び前記暗号化データの一部が切り取られた部分にセットして前記第1のパケット内の前記暗号化データを復号することを特徴とする請求項1に記載の通信システム。

[4] 前記送信側の無線端末は、前記受信側の無線端末あての送信データを暗号化して、前記暗号化データを前記受信側の無線端末側で復号するために必要なデータの一部を取り除いた前記第1のパケットを生成するとともに、前記復号するために必要なデータの一部を含む前記第2のパケットを生成し、

前記受信側の無線端末は、前記第2のパケット内の前記復号するために必要なデータの一部を、前記第1のパケット内の前記復号するために必要なデータの一部が切り取られた部分にセットして前記第1のパケット内の前記暗号化データを復号することを特徴とする請求項1に記載の通信システム。

[5] 前記パケットを暗号化・復号化する方法としてIPsec ESPのトンネルモードを用いることを特徴とする請求項2に記載の通信システム。

[6] 無線端末と無線中継装置との間で相互に無線通信を行い、制御装置が前記無線中継装置との間でパケット転送を行うとともに前記無線端末及び無線中継装置間の無線通信を管理する通信方法において、

送信側の無線端末及び受信側の無線端末が同一の前記無線中継装置に接続されている場合に、前記送信側の無線端末が、受信側の無線端末あての送信パケットを、前記制御装置を介さない第1のパケットと前記制御装置を介する第2のパケットに分割して前記無線中継装置に送信するステップと、

前記無線中継装置が、前記送信側の無線端末から送信された前記第1及び前記第2のパケットを受信して、前記第1のパケットを前記受信側の無線端末に送信するとともに前記第2のパケットを前記制御装置に送信するステップと、

前記制御装置が、前記無線中継装置から送信された前記第2のパケットを受信して前記無線中継装置に送信するステップと、

前記無線中継装置が、前記制御装置から送信された前記第2のパケットを受信して前記受信側の無線端末に送信するステップと、

前記受信側の無線端末が、前記無線中継装置から送信された前記第1及び前記第2のパケットを受信して元のパケットに復元するステップとを、

有することを特徴とする通信方法。

[7] 無線端末と相互に無線通信を行う無線中継装置と、前記無線中継装置との間でパケット転送を行うとともに前記無線端末及び無線中継装置間の無線通信を管理する制御装置とを備えた通信システムにおける送信側の前記無線端末において、

自己及び受信側の無線端末が同一の前記無線中継装置に接続されている場合に、前記受信側の無線端末あての送信パケットを、前記制御装置を介さない第1のパケットと前記制御装置を介する第2のパケットに分割して前記無線中継装置に送信する手段を備え、

前記無線中継装置が、前記送信側の無線端末から送信された前記第1及び前記第2のパケットを受信して、前記第1のパケットを前記受信側の無線端末に送信するとともに前記第2のパケットを前記制御装置に送信し、

前記制御装置が、前記無線中継装置から送信された前記第2のパケットを受信して前記無線中継装置に送信し、

前記無線中継装置が、前記制御装置から送信された前記第2のパケットを受信して前記受信側の無線端末に送信し、

前記受信側の無線端末が、前記無線中継装置から送信された前記第1及び前記第2のパケットを受信して元のパケットに復元するようにした無線端末。

[8] 無線端末と相互に無線通信を行う無線中継装置と、前記無線中継装置との間でパケット転送を行うとともに前記無線端末及び無線中継装置間の無線通信を管理する制御装置とを備えた通信システムにおける前記無線中継装置において、

送信側の無線端末及び受信側の無線端末が自己に接続されている場合に、前記送信側の無線端末が、前記受信側の無線端末あての送信パケットを、前記制御装置を介さない第1のパケットと前記制御装置を介する第2のパケットに分割して自己に送信したとき、前記送信側の無線端末から送信された前記第1及び前記第2のパケットを受信して、前記第1のパケットを前記受信側の無線端末に送信するとともに前記第2のパケットを前記制御装置に送信する手段と、

前記制御装置が、自己から送信された前記第2のパケットを受信して自己に送信したとき、前記制御装置から送信された前記第2のパケットを受信して前記受信側の無線端末に送信する手段とを備え、

前記受信側の無線端末が、自己から送信された前記第1及び前記第2のパケットを受信して元のパケットに復元するようにしたことを特徴とする無線中継装置。

[9] 無線端末と相互に無線通信を行う無線中継装置と、前記無線中継装置との間でパケット転送を行うとともに前記無線端末及び無線中継装置間の無線通信を管理する制御装置とを備えた通信システムにおける前記制御装置において、

送信側の無線端末が、受信側の無線端末が同一の無線中継装置に接続されている場合に、前記受信側の無線端末あての送信パケットを、自己を介さない第1のパケットと自己を介する第2のパケットに分割して前記無線中継装置に送信し、前記無線中継装置が、前記送信側の無線端末から送信された前記第1及び前記第2のパケットを受信して、前記第1のパケットを前記受信側の無線端末に送信するとともに前記第2のパケットを自己あてに送信したとき、前記無線中継装置から送信された前記第2のパケットを受信して前記無線中継装置に送信する手段と、

前記第2のパケットに基づいて前記無線端末及び無線中継装置間の無線通信を管理する手段とを備え、

前記無線中継装置が、自己から送信された前記第2のパケットを受信して前記受信側の無線端末に送信し、

前記受信側の無線端末が、前記無線中継装置から送信された前記第1及び前記第2のパケットを受信して元のパケットに復元するようにしたことを特徴とする制御装置。

[10] 無線端末と相互に無線通信を行う無線中継装置と、前記無線中継装置との間でパケット転送を行うとともに前記無線端末及び無線中継装置間の無線通信を管理する制御装置とを備えた通信システムにおける受信側の前記無線端末において、

送信側の無線端末及び自己が同一の無線中継装置に接続されている場合に、前記送信側の無線端末が自己あての送信パケットを、前記制御装置を介さない第1のパケットと前記制御装置を介する第2のパケットに分割して前記無線中継装置に送信

し、前記無線中継装置が、前記送信側の無線端末から送信された前記第1及び前記第2のパケットを受信して、前記第1のパケットを前記受信側の無線端末に送信するとともに前記第2のパケットを前記制御装置に送信し、前記制御装置が、前記無線中継装置から送信された前記第2のパケットを受信して前記無線中継装置に送信し、前記無線中継装置が、前記制御装置から送信された前記第2のパケットを受信して自己に送信したとき、前記無線中継装置から送信された前記第1及び前記第2のパケットを受信して元のパケットに復元する手段を、

備えたことを特徴とする無線端末。

[11] 無線端末と相互に無線通信を行う無線中継装置と、前記無線中継装置との間でパケット転送を行うとともに前記無線端末及び無線中継装置間の無線通信を管理する制御装置とを備えた通信システムにおいて、

送信側の無線端末は、受信側の無線端末が同一の無線中継装置に接続されている場合に、前記受信側の無線端末あての送信データを暗号化した後にパケット化し、このパケットを前記制御装置を介さない前記受信側の無線端末あての第1のパケットとして前記無線中継装置に送信するとともに、前記暗号化されたデータを復号するための鍵データをパケット化し、このパケットを前記制御装置を介する前記受信側の無線端末あての第2のパケットとして前記無線中継装置に送信し、

前記無線中継装置は、前記送信側の無線端末から送信された前記第1及び前記第2のパケットを受信して、前記第1のパケットを前記受信側の無線端末に転送するとともに前記第2のパケットを前記制御装置に転送し、さらに複数の前記第1のパケットの内の一部のパケットを定期的にコピーしてこのパケットを第3のパケットとして前記制御装置に送信し、

前記制御装置は、前記無線中継装置から転送された前記第2のパケットを受信して内部の鍵データを確認して前記第2のパケットを前記無線中継装置に転送するとともに、前記無線中継装置から送信された前記第3のパケットに基づいて前記第1のパケットの管理情報を取得し、

前記無線中継装置は、前記制御装置から転送された前記第2のパケットを受信して前記受信側の無線端末に転送し、

前記受信側の無線端末は、前記無線中継装置から転送された前記第1及び前記第2のパケットを受信して、前記暗号化されたデータを前記鍵データにより復号することを特徴とする通信システム。

[12] 前記送信側の無線端末は、前記第1のパケットの各パケット内にそれぞれシーケンス番号をセットし、

前記制御装置は、前記第3のパケット内のシーケンス番号に基づいて前記第1のパケットの転送パケット数を管理することを特徴とする請求項11に記載の通信システム。

[13] 前記制御装置は、前記第2のパケット内の鍵データを保持し、この鍵データに基づいて前記第3のパケット内の暗号化データを復号し、復号できない場合に、前記無線中継装置に対して前記第1のパケットの前記受信側の無線端末への転送を禁止することを特徴とする請求項11に記載の通信システム。

[14] 前記送信側の無線端末は、前記第1のパケットの所定の転送パケット数ごとに、又は所定時間ごとに前記鍵データを更新することを特徴とする請求項11に記載の通信システム。

[15] 無線端末と無線中継装置との間で相互に無線通信を行い、制御装置が前記無線中継装置との間でパケット転送を行うとともに前記無線端末及び無線中継装置間の無線通信を管理する通信方法において、

送信側の無線端末が、受信側の無線端末が同一の無線中継装置に接続されている場合に、前記受信側の無線端末あての送信データを暗号化した後にパケット化し、このパケットを前記制御装置を介さない前記受信側の無線端末あての第1のパケットとして前記無線中継装置に送信するとともに、前記暗号化されたデータを復号するための鍵データをパケット化し、このパケットを前記制御装置を介する前記受信側の無線端末あての第2のパケットとして前記無線中継装置に送信するステップと、

前記無線中継装置が、前記送信側の無線端末から送信された前記第1及び前記第2のパケットを受信して、前記第1のパケットを前記受信側の無線端末に転送するとともに前記第2のパケットを前記制御装置に転送し、さらに複数の前記第1のパケットの内の一部のパケットを定期的にコピーしてこのパケットを第3のパケットとして前記

制御装置に送信するステップと、

前記制御装置が、前記無線中継装置から転送された前記第2のパケットを受信して内部の鍵データを確認して前記第2のパケットを前記無線中継装置に転送するとともに、前記無線中継装置から送信された前記第3のパケットに基づいて前記第1のパケットの管理情報を取得するステップと、

前記無線中継装置が、前記制御装置から転送された前記第2のパケットを受信して前記受信側の無線端末に転送するステップと、

前記受信側の無線端末は、前記無線中継装置から転送された前記第1及び前記第2のパケットを受信して、前記暗号化されたデータを前記鍵データにより復号するステップとを、

有する通信方法。

[16] 無線端末と相互に無線通信を行う無線中継装置と、前記無線中継装置との間でパケット転送を行うとともに前記無線端末及び無線中継装置間の無線通信を管理する制御装置とを備えた通信システムにおける送信側の前記無線端末において、

自身と受信側の無線端末が同一の無線中継装置に接続されている場合に、前記受信側の無線端末あての送信データを暗号化した後にパケット化し、このパケットを前記制御装置を介さない前記受信側の無線端末あての第1のパケットとして前記無線中継装置に送信するとともに、前記暗号化されたデータを復号するための鍵データをパケット化し、このパケットを前記制御装置を介する前記受信側の無線端末あての第2のパケットとして前記無線中継装置に送信する手段を備え、

前記無線中継装置が、前記送信側の無線端末自身から送信された前記第1及び前記第2のパケットを受信して、前記第1のパケットを前記受信側の無線端末に転送するとともに前記第2のパケットを前記制御装置に転送し、さらに複数の前記第1のパケットの内の一部のパケットを定期的にコピーしてこのパケットを第3のパケットとして前記制御装置に送信し、

前記制御装置が、前記無線中継装置から転送された前記第2のパケットを受信して内部の鍵データを確認して前記第2のパケットを前記無線中継装置に転送するとともに、前記無線中継装置から送信された前記第3のパケットに基づいて前記第1のパケ

ットの管理情報を取得し、

前記無線中継装置が、前記制御装置から転送された前記第2のパケットを受信して前記受信側の無線端末に転送し、

前記受信側の無線端末が、前記無線中継装置から転送された前記第1及び前記第2のパケットを受信して、前記暗号化されたデータを前記鍵データにより復号することを特徴とする無線端末。

[17] 前記第1のパケットの所定の転送パケット数ごとに、又は所定時間ごとに前記鍵データを更新することを特徴とする請求項16に記載の無線端末。

[18] 無線端末と相互に無線通信を行う無線中継装置と、前記無線中継装置との間でパケット転送を行うとともに前記無線端末及び無線中継装置間の無線通信を管理する制御装置とを備えた通信システムにおける前記無線中継装置において、

送信側の無線端末が、受信側の無線端末が同一の無線中継装置に接続されている場合に、前記受信側の無線端末あての送信データを暗号化した後にパケット化し、このパケットを前記制御装置を介さない前記受信側の無線端末あての第1のパケットとして前記無線中継装置自身に送信するとともに、前記暗号化されたデータを復号するための鍵データをパケット化し、このパケットを前記制御装置を介する前記受信側の無線端末あての第2のパケットとして前記無線中継装置自身に送信した場合に、前記送信側の無線端末から送信された前記第1及び前記第2のパケットを受信して、前記第1のパケットを前記受信側の無線端末に転送するとともに前記第2のパケットを前記制御装置に転送し、さらに複数の前記第1のパケットの内の一部のパケットを定期的にコピーしてこのパケットを第3のパケットとして前記制御装置に送信する手段と、

前記制御装置が、前記無線中継装置自身から転送された前記第2のパケットを受信して内部の鍵データを確認して前記第2のパケットを前記無線中継装置自身に転送するとともに、自身から送信された前記第3のパケットに基づいて前記第1のパケットの管理情報を取得した場合に、前記制御装置から転送された前記第2のパケットを受信して前記受信側の無線端末に転送する手段とを備え、

前記受信側の無線端末が、前記無線中継装置自身から転送された前記第1及び

前記第2のパケットを受信して、前記暗号化されたデータを前記鍵データにより復号することを特徴とする無線中継装置。

[19] 無線端末と相互に無線通信を行う無線中継装置と、前記無線中継装置との間でパケット転送を行うとともに前記無線端末及び無線中継装置間の無線通信を管理する制御装置とを備えた通信システムにおける前記制御装置において、

送信側の無線端末が、受信側の無線端末が同一の無線中継装置に接続されている場合に、前記受信側の無線端末あての送信データを暗号化した後にパケット化し、このパケットを自身を介さない前記受信側の無線端末あての第1のパケットとして前記無線中継装置に送信するとともに、前記暗号化されたデータを復号するための鍵データをパケット化し、このパケットを自身を介する前記受信側の無線端末あての第2のパケットとして前記無線中継装置に送信し、前記無線中継装置が、前記送信側の無線端末から送信された前記第1及び前記第2のパケットを受信して、前記第1のパケットを前記受信側の無線端末に転送するとともに前記第2のパケットを自身に転送し、さらに複数の前記第1のパケットの内の一部のパケットを定期的にコピーしてこのパケットを第3のパケットとして自身に送信した場合、前記無線中継装置から転送された前記第2のパケットを受信して内部の鍵データを確認して前記第2のパケットを前記無線中継装置に転送するとともに、前記無線中継装置から送信された前記第3のパケットに基づいて前記第1のパケットの管理情報を取得する手段を備え、

前記無線中継装置が、前記制御装置自身から転送された前記第2のパケットを受信して前記受信側の無線端末に転送し、

前記受信側の無線端末が、前記無線中継装置から転送された前記第1及び前記第2のパケットを受信して、前記暗号化されたデータを前記鍵データにより復号することを特徴とする制御装置。

[20] 前記送信側の無線端末が前記第1のパケットの各パケット内にそれぞれシーケンス番号をセットする場合、前記第3のパケット内のシーケンス番号に基づいて前記第1のパケットの転送パケット数を管理する手段を更に備えたことを特徴とする請求項19に記載の制御装置。

[21] 前記第2のパケット内の鍵データを保持し、この鍵データに基づいて前記第3のパ

ケット内の暗号化データを復号し、復号できない場合に、前記無線中継装置に対して前記第1のパケットの前記受信側の無線端末への転送を禁止する手段を更に備えたことを特徴とする請求項19に記載の制御装置。

[22] 無線端末と相互に無線通信を行う無線中継装置と、前記無線中継装置との間でパケット転送を行うとともに前記無線端末及び無線中継装置間の無線通信を管理する制御装置とを備えた通信システムにおける受信側の前記無線端末において、

送信側の無線端末が、受信側の無線端末が同一の無線中継装置に接続されている場合に、前記受信側の無線端末自身あての送信データを暗号化した後にパケット化し、このパケットを前記制御装置を介さない前記受信側の無線端末自身あての第1のパケットとして前記無線中継装置に送信するとともに、前記暗号化されたデータを復号するための鍵データをパケット化し、このパケットを前記制御装置を介する自身あての第2のパケットとして前記無線中継装置に送信し、前記無線中継装置が、前記送信側の無線端末から送信された前記第1及び前記第2のパケットを受信して、前記第1のパケットを前記受信側の無線端末自身に転送するとともに前記第2のパケットを前記制御装置に転送し、さらに複数の前記第1のパケットの内の一部のパケットを定期的にコピーしてこのパケットを第3のパケットとして前記制御装置に送信し、前記制御装置が、前記無線中継装置から転送された前記第2のパケットを受信して内部の鍵データを確認して前記第2のパケットを前記無線中継装置に転送するとともに、前記無線中継装置から送信された前記第3のパケットに基づいて前記第1のパケットの管理情報を取得し、前記無線中継装置が、前記制御装置から転送された前記第2のパケットを受信して前記受信側の無線端末自身に転送した場合に、前記無線中継装置から転送された前記第1及び前記第2のパケットを受信して、前記暗号化されたデータを前記鍵データにより復号する手段を、

備えたことを特徴とする無線端末。

[23] 請求項1に記載の通信システムにおいて、

前記制御装置を介さない第1のパケットは、音声信号の帯域を分割した低域側の基本音声データと高域側の拡張音声データのうち前記拡張音声データを含み、前記制御装置を介する第2のパケットは前記基本音声データを含むことを特徴とする通信

システム。

[24] 請求項6に記載の通信方法において、

前記制御装置を介さない第1のパケットは、音声信号の帯域を分割した低域側の基本音声データと高域側の拡張音声データのうち前記拡張音声データを含み、前記制御装置を介する第2のパケットは前記基本音声データを含むことを特徴とする通信方法。

[25] 請求項7に記載の無線端末において、

前記制御装置を介さない第1のパケットは、音声信号の帯域を分割した低域側の基本音声データと高域側の拡張音声データのうち前記拡張音声データを含み、前記制御装置を介する第2のパケットは前記基本音声データを含むことを特徴とする無線端末。

[26] 請求項8に記載の無線中継装置において、

前記制御装置を介さない第1のパケットは、音声信号の帯域を分割した低域側の基本音声データと高域側の拡張音声データのうち前記拡張音声データを含み、前記制御装置を介する第2のパケットは前記基本音声データを含むことを特徴とする無線中継装置。

[27] 請求項9に記載の制御装置において、

前記制御装置を介さない第1のパケットは、音声信号の帯域を分割した低域側の基本音声データと高域側の拡張音声データのうち前記拡張音声データを含み、前記制御装置を介する第2のパケットは前記基本音声データを含むことを特徴とする制御装置。

[28] 請求項1に記載の通信システムにおいて、

前記制御装置を介さない第1のパケットは、画像信号を画面内でのみ符号化した画面内符号化データと、画面間差分を予測符号化した画面間差分予測符号化データのうち前記画面間差分予測符号化データを含み、前記制御装置を介する第2のパケットは前記画面内符号化データを含むことを特徴とする通信システム。

[29] 請求項6に記載の通信方法において、

前記制御装置を介さない第1のパケットは、画像信号を画面内でのみ符号化した画

面内符号化データと、画面間差分を予測符号化した画面間差分予測符号化データのうち前記画面間差分予測符号化データを含み、前記制御装置を介する第2のパケットは前記画面内符号化データを含むことを特徴とする通信方法。

[30] 請求項7に記載の無線端末において、

前記制御装置を介さない第1のパケットは、画像信号を画面内でのみ符号化した画面内符号化データと、画面間差分を予測符号化した画面間差分予測符号化データのうち前記画面間差分予測符号化データを含み、前記制御装置を介する第2のパケットは前記画面内符号化データを含むことを特徴とする無線端末。

[31] 請求項8に記載の無線中継装置において、

前記制御装置を介さない第1のパケットは、画像信号を画面内でのみ符号化した画面内符号化データと、画面間差分を予測符号化した画面間差分予測符号化データのうち前記画面間差分予測符号化データを含み、前記制御装置を介する第2のパケットは前記画面内符号化データを含むことを特徴とする無線中継装置。

[32] 請求項9に記載の制御装置において、

前記制御装置を介さない第1のパケットは、画像信号を画面内でのみ符号化した画面内符号化データと、画面間差分を予測符号化した画面間差分予測符号化データのうち前記画面間差分予測符号化データを含み、前記制御装置を介する第2のパケットは前記画面内符号化データを含むことを特徴とする制御装置。

[33] 前記パケットを暗号化・復号化する方法としてIPsec ESPのトンネルモードを用いることを特徴とする請求項3に記載の通信システム。

[34] 前記パケットを暗号化・復号化する方法としてIPsec ESPのトンネルモードを用いることを特徴とする請求項4に記載の通信システム。

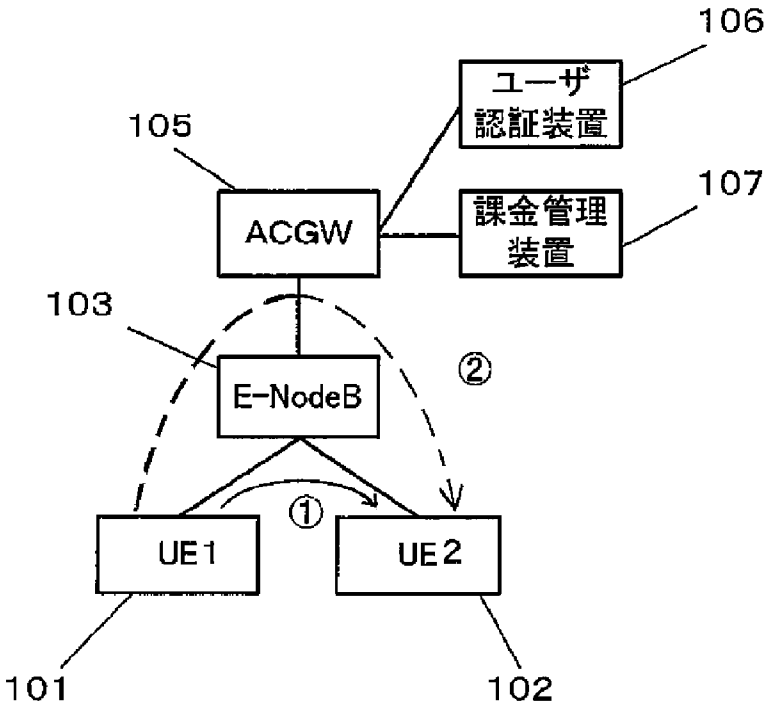
[35] 請求項10に記載の無線端末において、

前記制御装置を介さない第1のパケットは、音声信号の帯域を分割した低域側の基本音声データと高域側の拡張音声データのうち前記拡張音声データを含み、前記制御装置を介する第2のパケットは前記基本音声データを含むことを特徴とする無線端末。

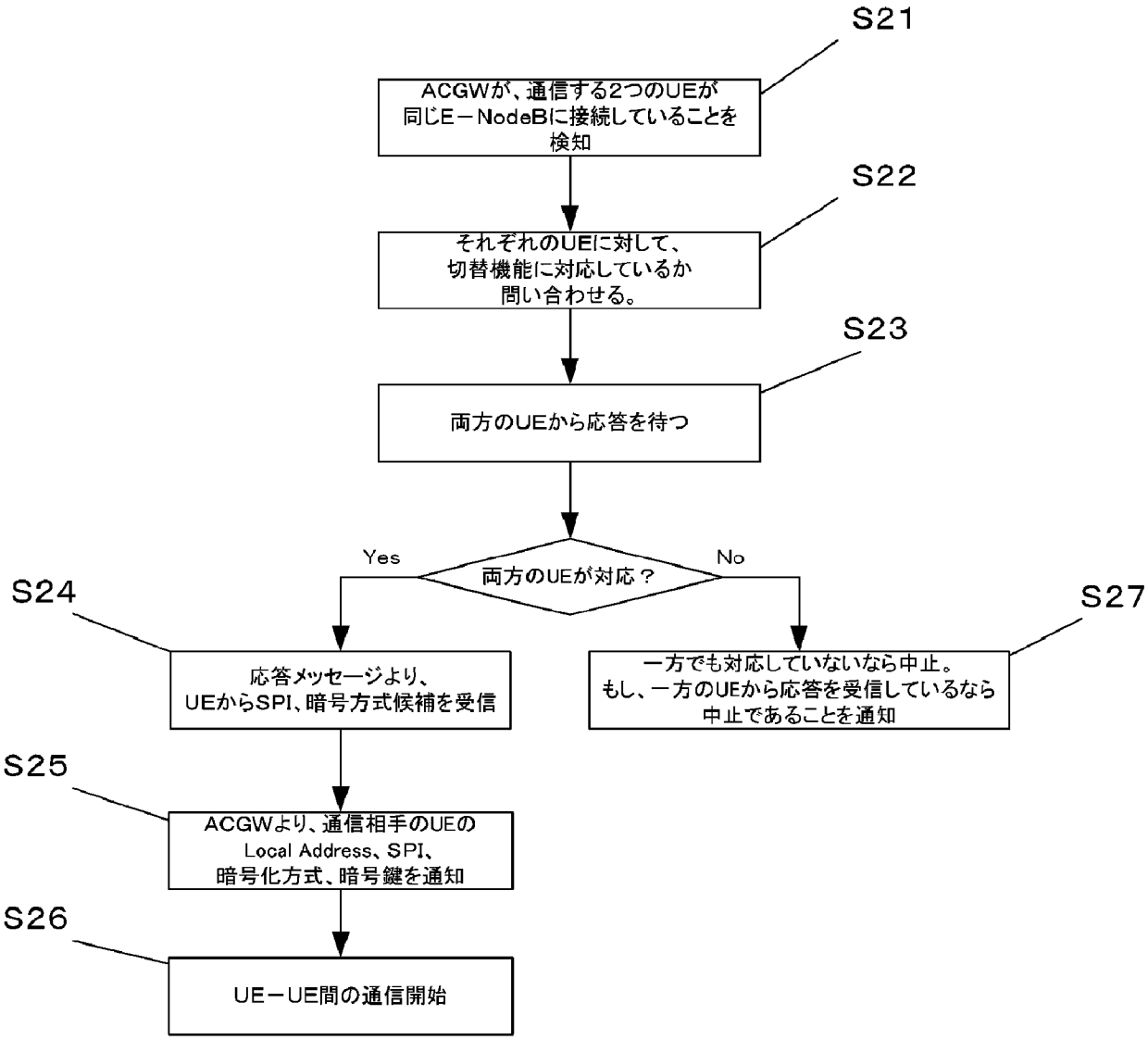
[36] 請求項10に記載の無線端末において、

前記制御装置を介さない第1のパケットは、画像信号を画面内でのみ符号化した画面内符号化データと、画面間差分を予測符号化した画面間差分予測符号化データのうち前記画面間差分予測符号化データを含み、前記制御装置を介する第2のパケットは前記画面内符号化データを含むことを特徴とする無線端末。

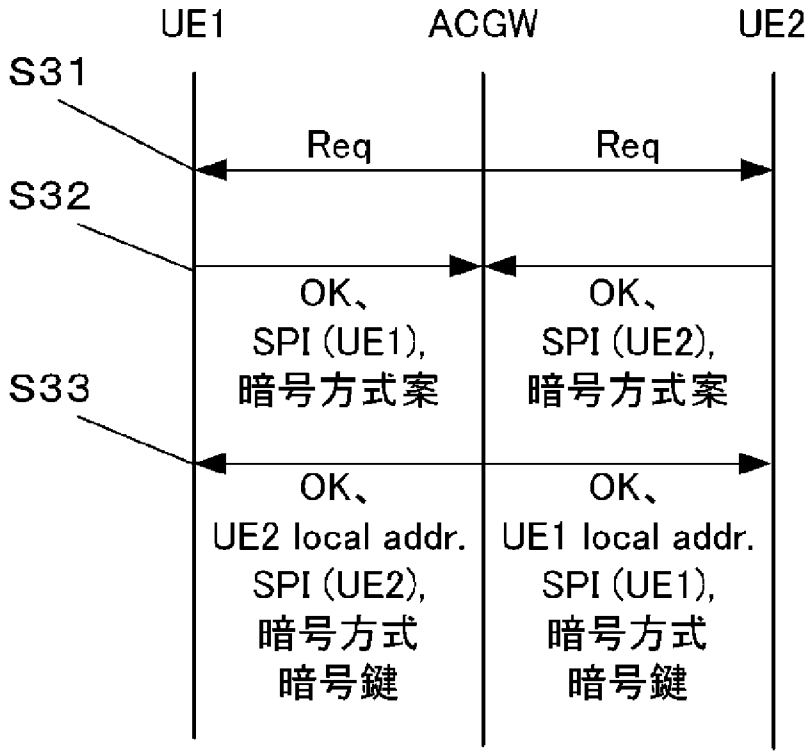
[図1]


106
ユーザ
認証装置
105
ACGW
107
課金管理
装置
103
E-NodeB
②
①
UE1
UE2
101
102

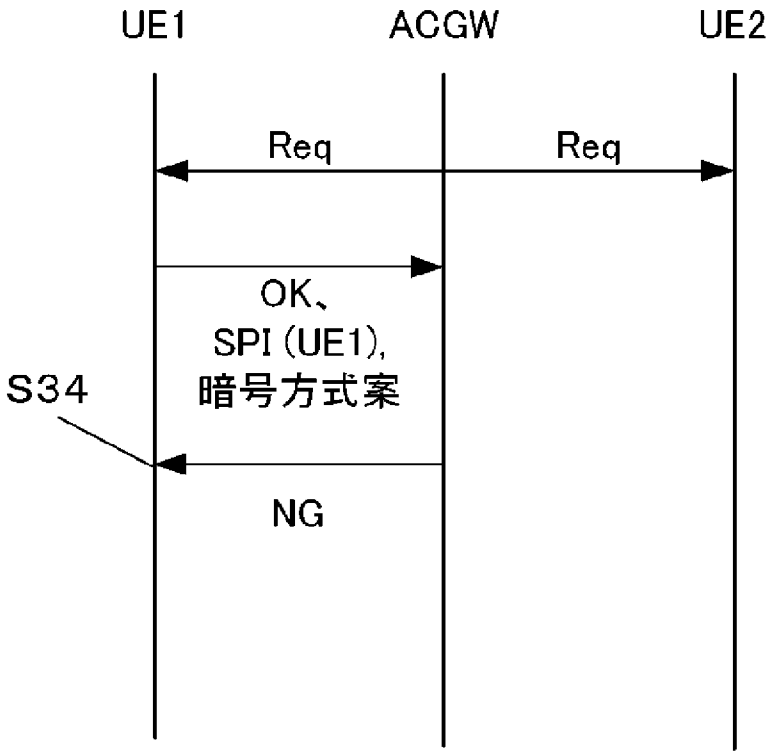
[図2]


S21
ACGWが、通信する2つのUEが
同じE－NodeBに接続していることを
検知
S22
それぞれのUEに対して、
切替機能に対応しているか
問い合わせる。
S23
両方のUEから応答を待つ
Yes
両方のUEが対応？
No
S24
応答メッセージより、
UEからSPI、暗号方式候補を受信
S27
一方でも対応していないなら中止。
もし、一方のUEから応答を受信しているなら
中止であることを通知
S25
ACGWより、通信相手のUEの
Local Address、SPI、
暗号化方式、暗号鍵を通知
S26
UE－UE間の通信開始

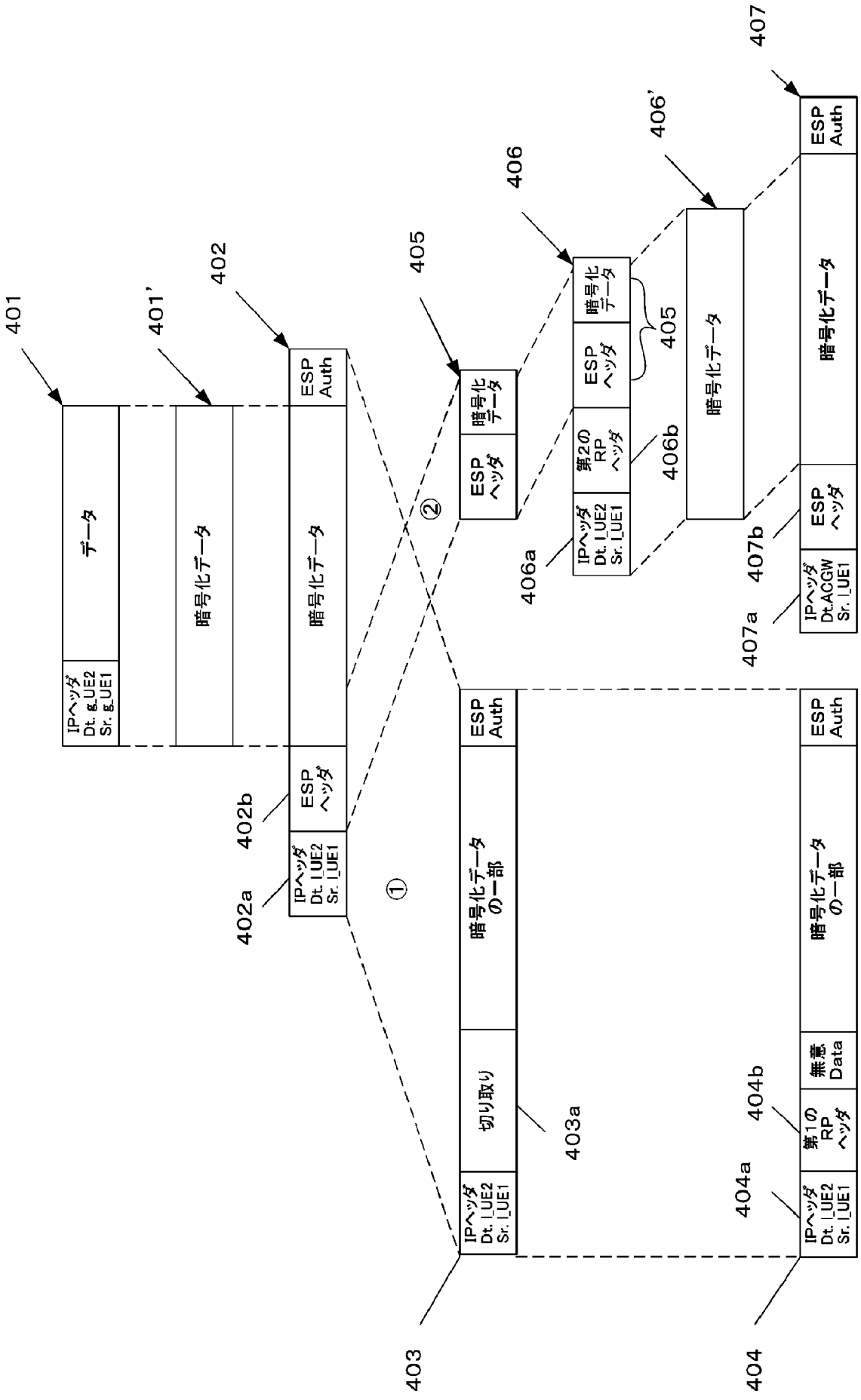
[図3A]


UE1
ACGW
UE2
S31
Req
Req
S32
OK、
SPI (UE1),
暗号方式案
OK、
SPI (UE2),
暗号方式案
S33
OK、
UE2 local addr.
SPI (UE2),
暗号方式
暗号鍵
OK、
UE1 local addr.
SPI (UE1),
暗号方式
暗号鍵

[図3B]


UE1
ACGW
UE2
Req
Req
OK、
SPI (UE1),
暗号方式案
S34
NG

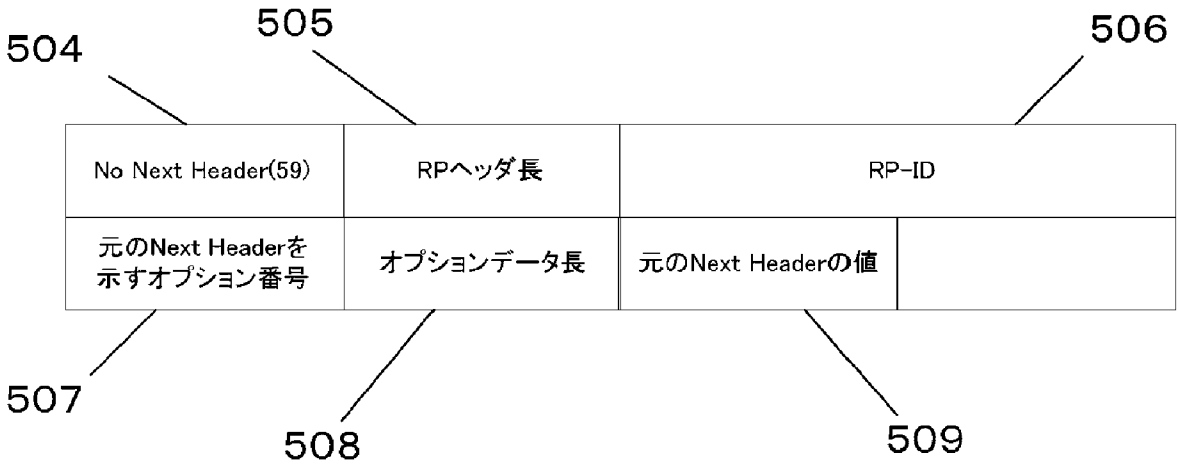
[図4]


401
401'
402
405
406
406'
407
IPヘッダ Dt. g_UE2 Sr. g_UE1
データ
暗号化データ
ESP Auth
暗号化データ
402b
ESP ヘッダ
402a
IPヘッダ Dt. I_UE2 Sr. I_UE1
①
②
ESP ヘッダ
暗号化データ
406a
IPヘッダ Dt. I_UE2 Sr. I_UE1
第2の RP ヘッダ
406b
ESP ヘッダ
暗号化データ
405
暗号化データ
407a
IPヘッダ Dt.ACGW Sr. I_UE1
407b
ESP ヘッダ
暗号化データ
ESP Auth
403
IPヘッダ Dt. I_UE2 Sr. I_UE1
切り取り
403a
暗号化データの一部
ESP Auth
404
IPヘッダ Dt. I_UE2 Sr. I_UE1
404a
第1の RP ヘッダ
404b
無意 Data
暗号化データの一部
ESP Auth

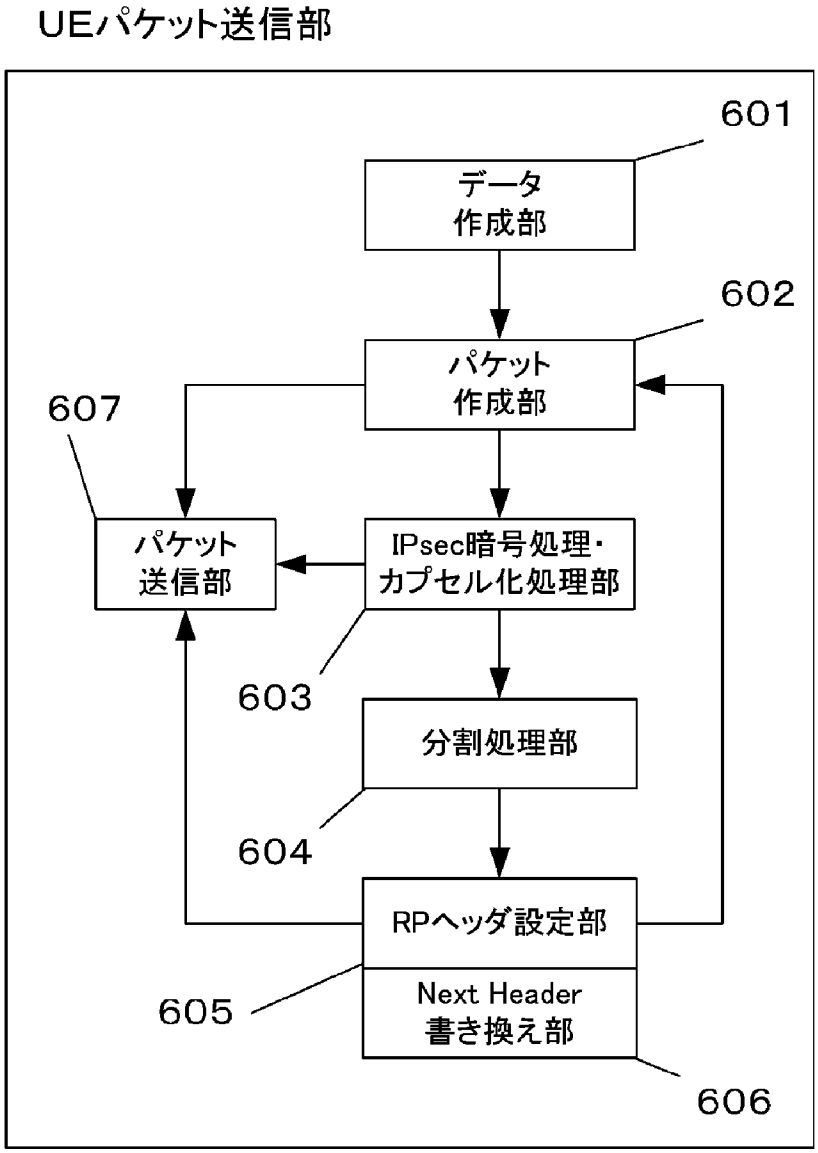
[図5A]


No Next Header(59)
RPヘッダ長
RP-ID
501
502
503

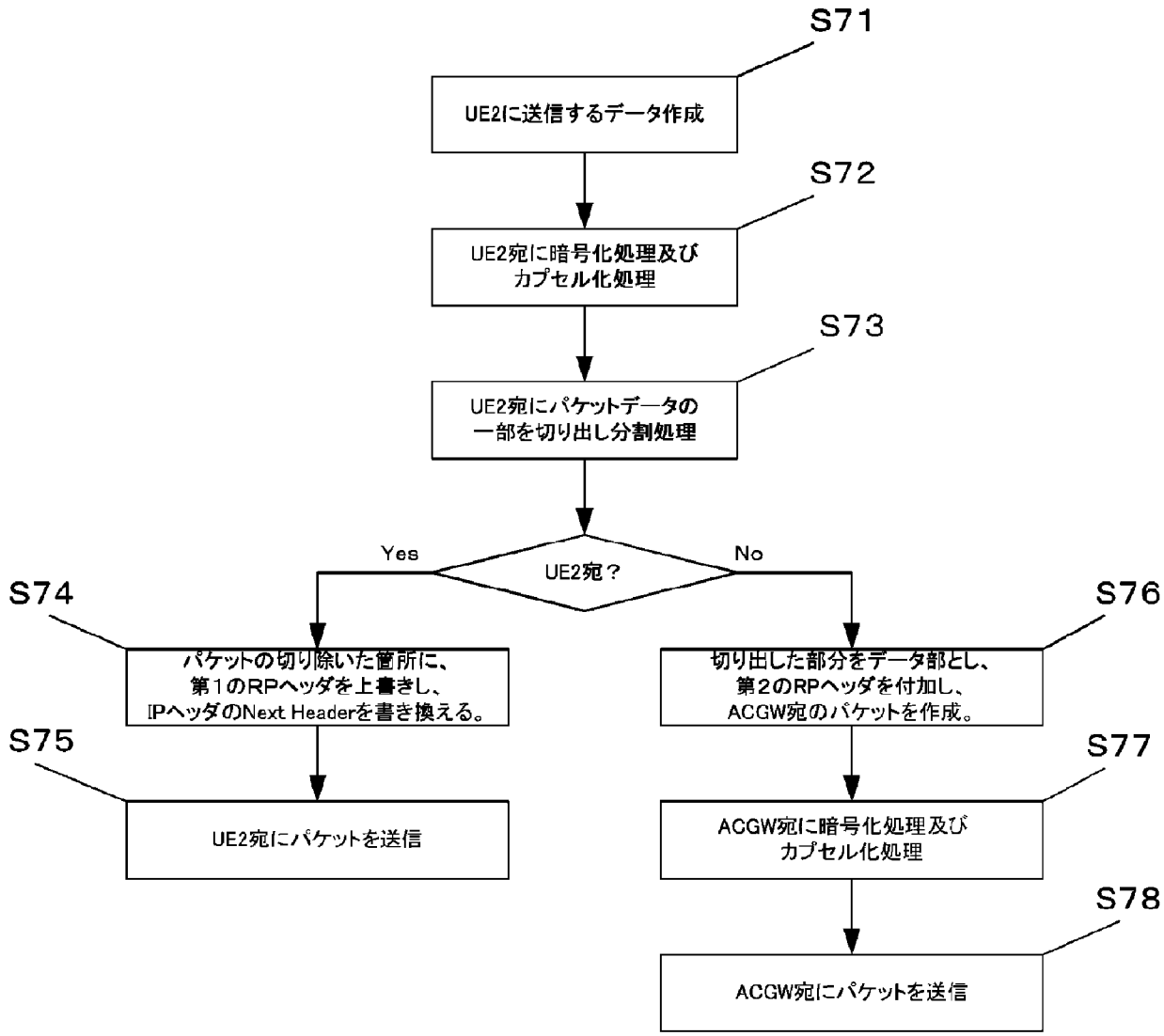
[図5B]


504
505
506
No Next Header(59)
RPヘッダ長
RP-ID
元のNext Headerを
示すオプション番号
オプションデータ長
元のNext Headerの値
507
508
509

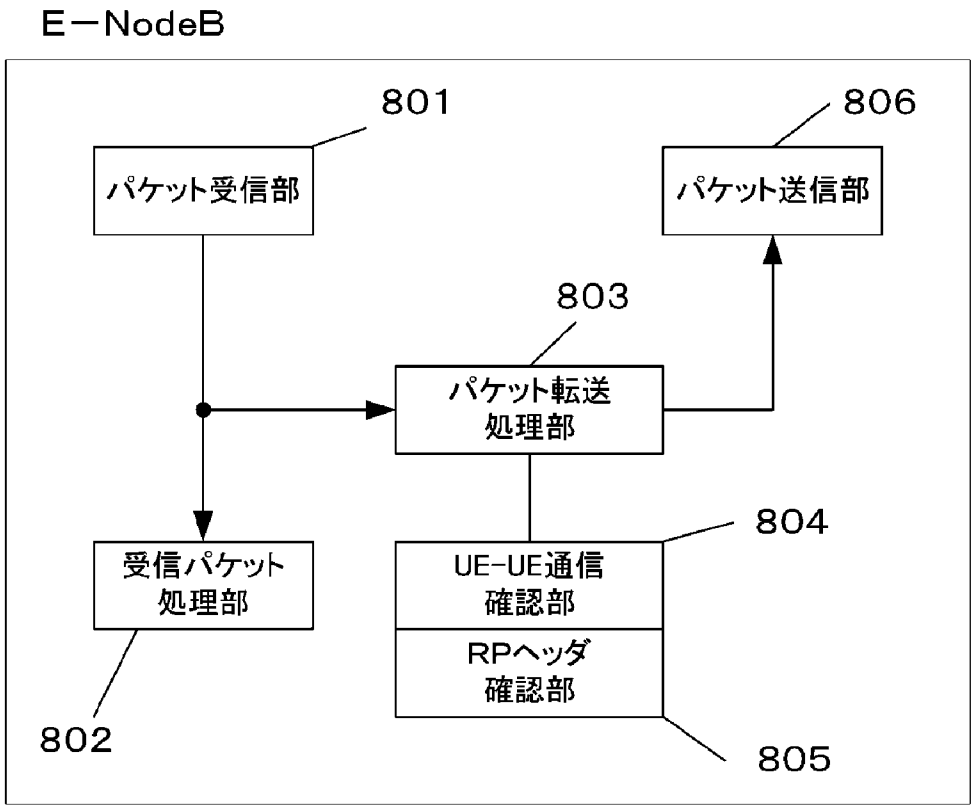
[図6]


UEパケット送信部
601
データ
作成部
602
パケット
作成部
607
パケット
送信部
IPsec暗号処理・
カプセル化処理部
603
分割処理部
604
RPヘッダ設定部
605
Next Header
書き換え部
606

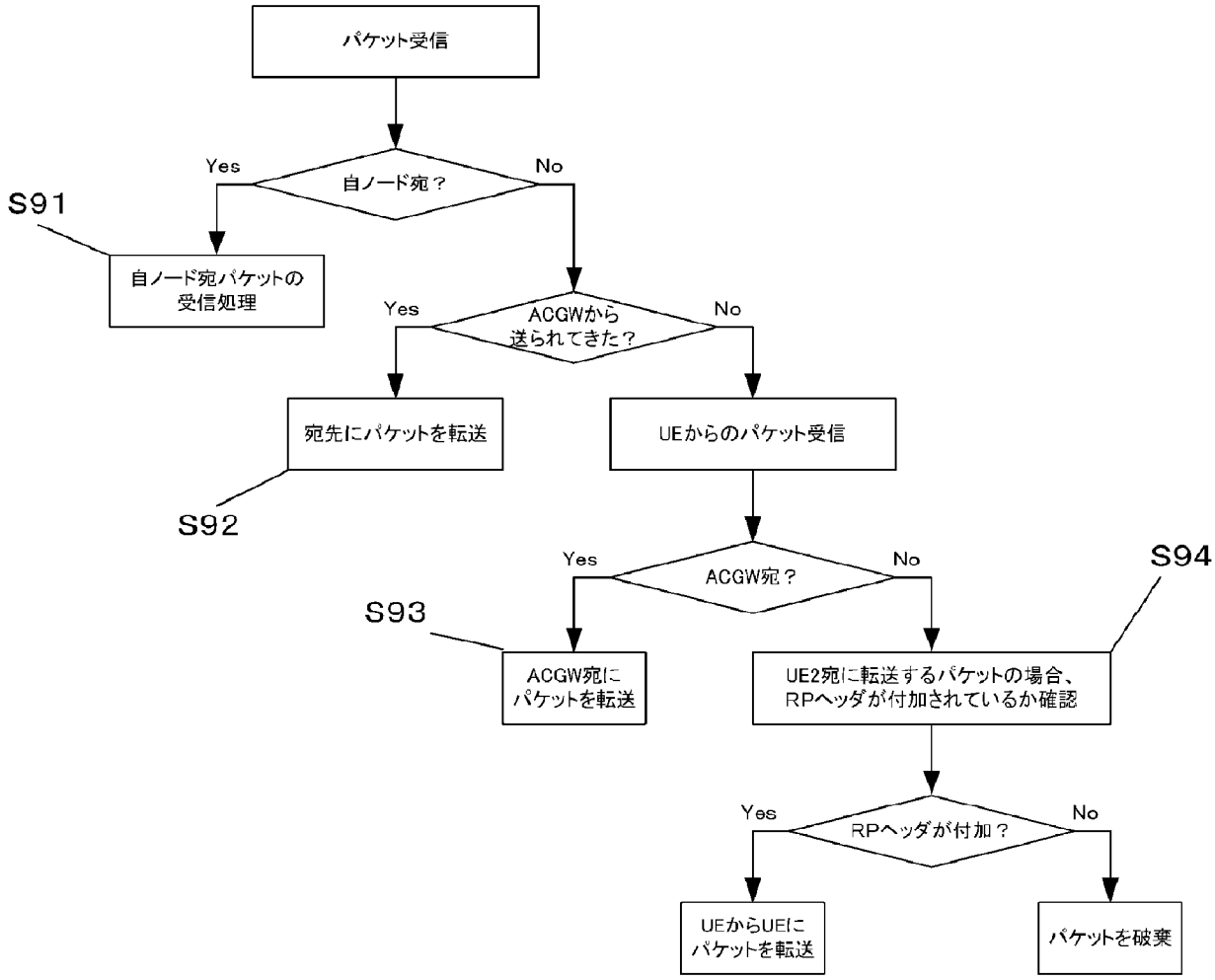
[図7]


S71
UE2に送信するデータ作成
S72
UE2宛に暗号化処理及び
カプセル化処理
S73
UE2宛にパケットデータの
一部を切り出し分割処理
UE2宛？
Yes
No
S74
パケットの切り除いた箇所に、
第1のRPヘッダを上書きし、
IPヘッダのNext Headerを書き換える。
S75
UE2宛にパケットを送信
S76
切り出した部分をデータ部とし、
第2のRPヘッダを付加し、
ACGW宛のパケットを作成。
S77
ACGW宛に暗号化処理及び
カプセル化処理
S78
ACGW宛にパケットを送信

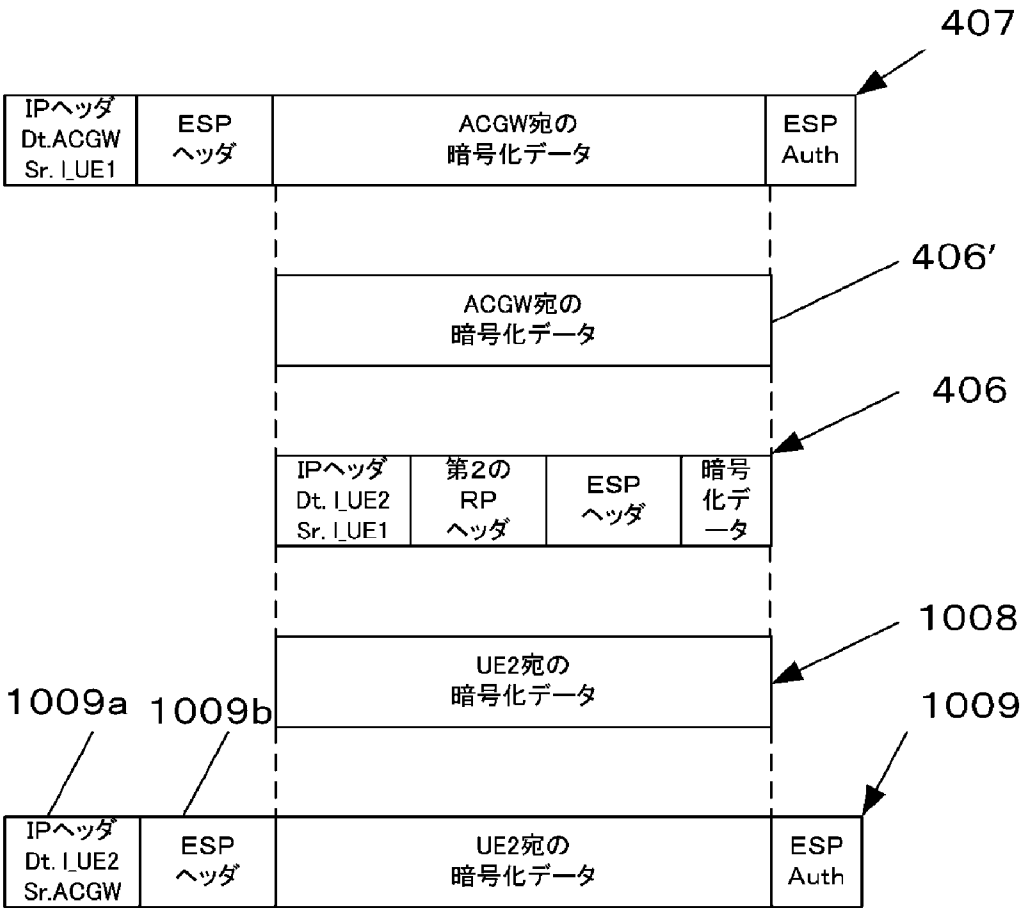
[図8]


E－NodeB
801
パケット受信部
806
パケット送信部
803
パケット転送
処理部
804
受信パケット
処理部
UE-UE通信
確認部
RPヘッダ
確認部
802
805

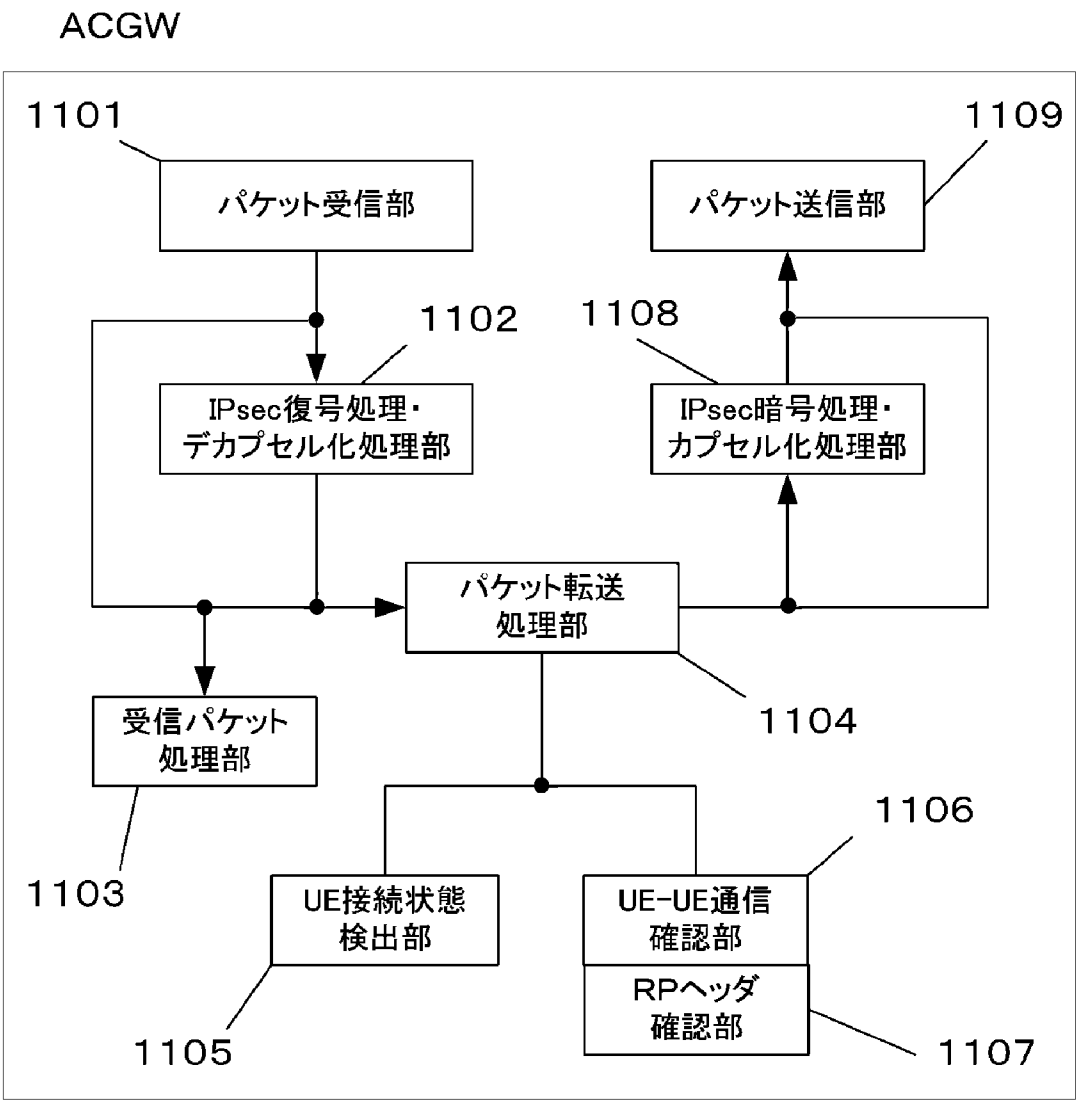
[図9]


パケット受信
自ノード宛？
Yes
No
S91
自ノード宛パケットの
受信処理
ACGWから
送られてきた？
Yes
No
宛先にパケットを転送
S92
UEからのパケット受信
ACGW宛？
Yes
No
S93
ACGW宛に
パケットを転送
S94
UE2宛に転送するパケットの場合、
RPヘッダが付加されているか確認
RPヘッダが付加？
Yes
No
UEからUEに
パケットを転送
パケットを破棄

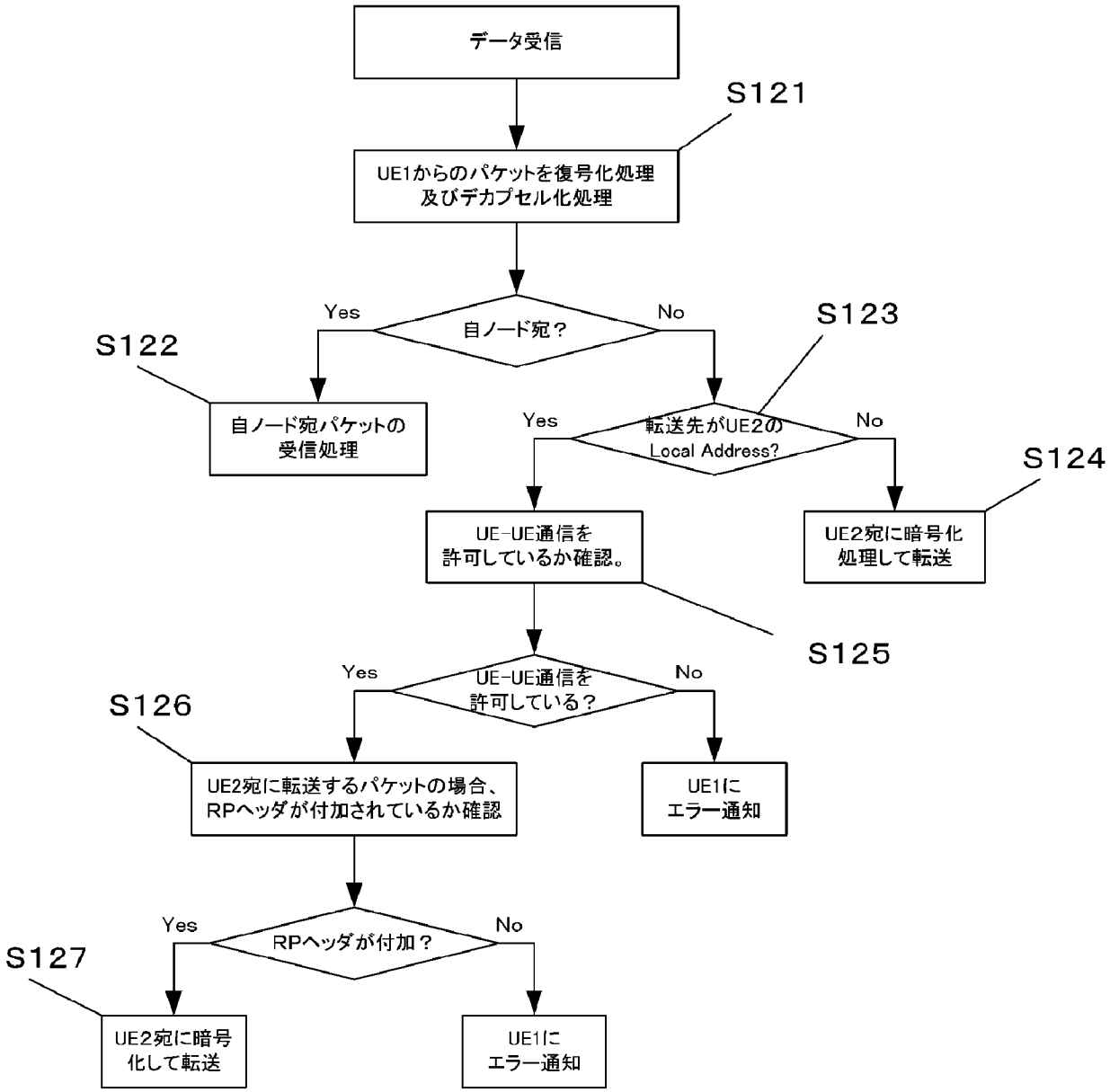
[図10]


407
IPヘッダ
Dt.ACGW
Sr. I_UE1
ESP
ヘッダ
ACGW宛の
暗号化データ
ESP
Auth
406'
ACGW宛の
暗号化データ
406
IPヘッダ
Dt. I_UE2
Sr. I_UE1
第2の
RP
ヘッダ
ESP
ヘッダ
暗号
化デ
ータ
1008
UE2宛の
暗号化データ
1009a
1009b
1009
IPヘッダ
Dt. I_UE2
Sr.ACGW
ESP
ヘッダ
UE2宛の
暗号化データ
ESP
Auth

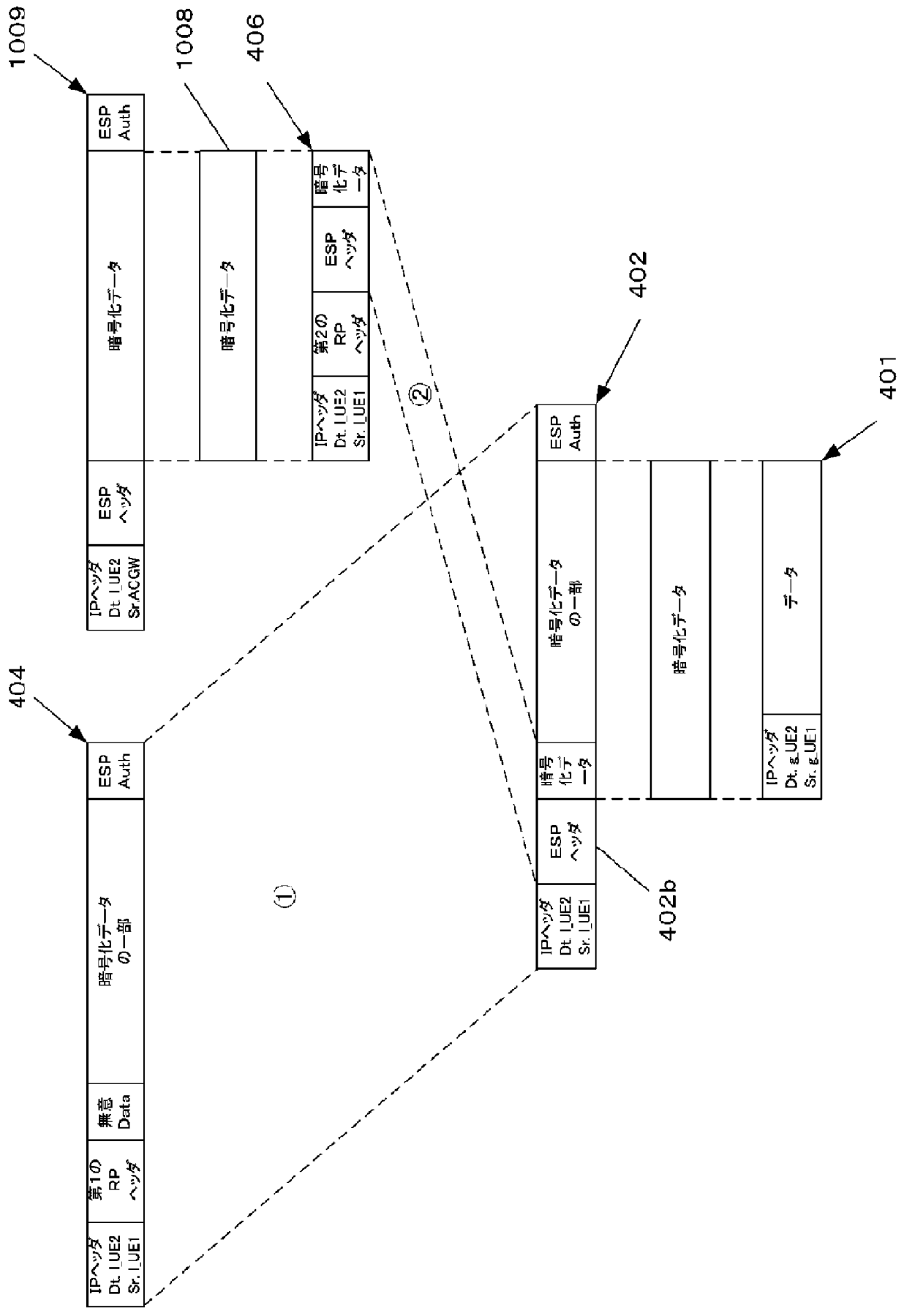
[図11]


ACGW
1101
パケット受信部
1109
パケット送信部
1102
IPsec復号処理・
デカプセル化処理部
1108
IPsec暗号処理・
カプセル化処理部
パケット転送
処理部
1104
受信パケット
処理部
1103
1106
UE接続状態
検出部
UE-UE通信
確認部
RPヘッダ
確認部
1105
1107

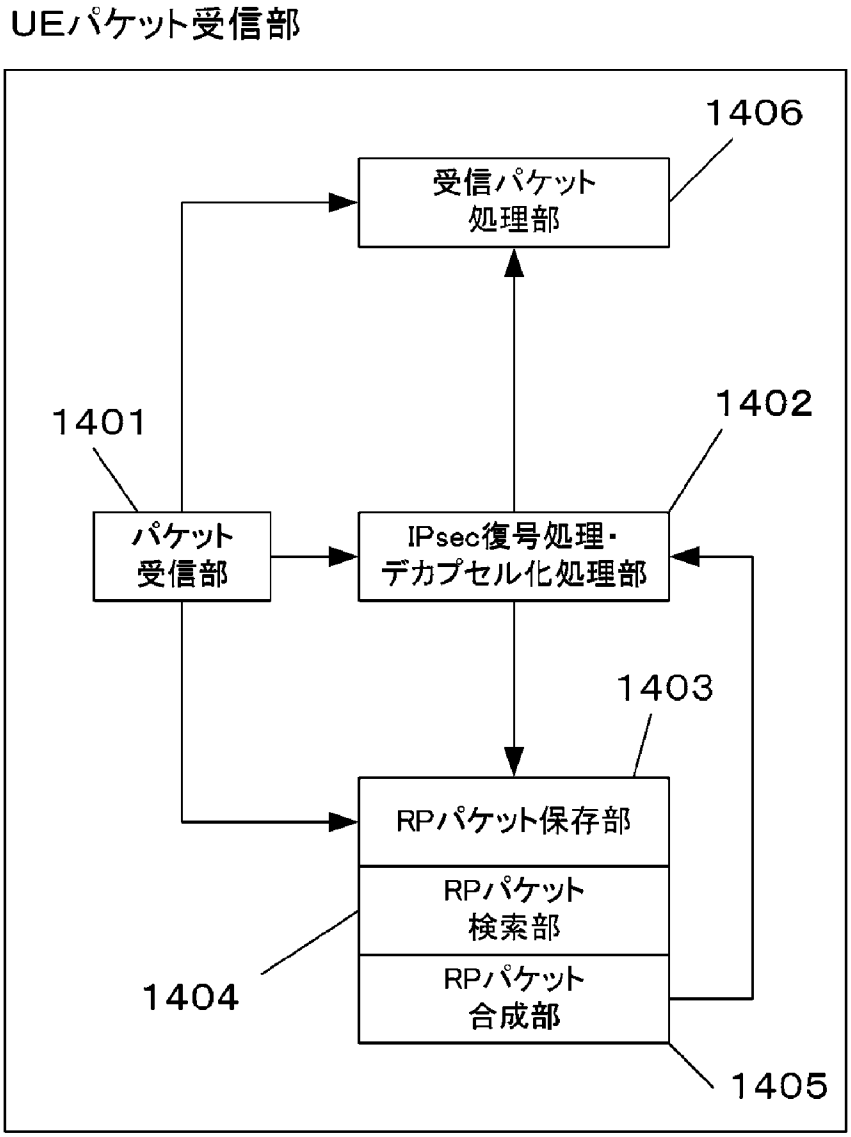
[図12]


データ受信
S121
UE1からのパケットを復号化処理
及びデカプセル化処理
Yes
自ノード宛？
No
S122
S123
自ノード宛パケットの
受信処理
Yes
転送先がUE2の
Local Address?
No
S124
UE-UE通信を
許可しているか確認。
UE2宛に暗号化
処理して転送
S125
Yes
UE-UE通信を
許可している？
No
S126
UE2宛に転送するパケットの場合、
RPヘッダが付加されているか確認
UE1に
エラー通知
Yes
RPヘッダが付加？
No
S127
UE2宛に暗号
化して転送
UE1に
エラー通知

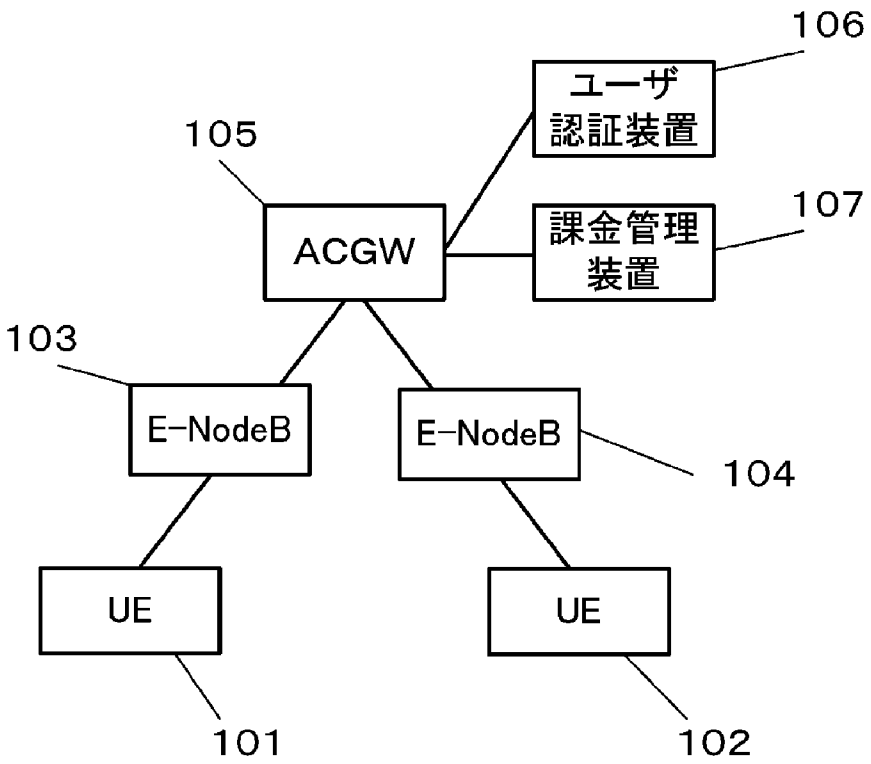
[図13]


1009
1008
406
402
401
404
402b
ESP Auth
暗号化データ
ESP ヘッダ
IPヘッダ Dt. I_UE2 Sr.ACGW
暗号化データ
暗号化データ
第2の RP ヘッダ
IPヘッダ Dt. I_UE2 Sr. I_UE1
ESP Auth
暗号化データの一部
暗号化データ
データ
ESP ヘッダ
IPヘッダ Dt. I_UE2 Sr. I_UE1
IPヘッダ Dt. g_UE2 Sr. g_UE1
ESP Auth
暗号化データの一部
第1の RP ヘッダ
無意 Data
IPヘッダ Dt. I_UE2 Sr. I_UE1
①
②

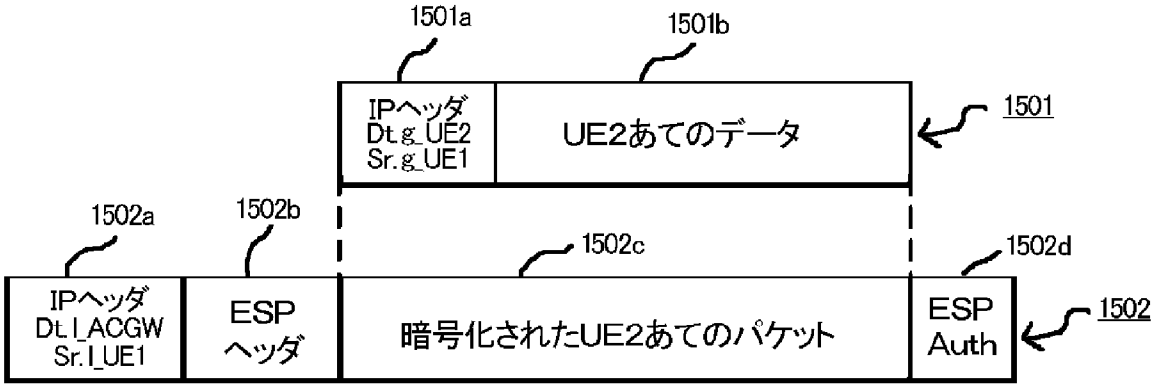
[図14]


UEパケット受信部
1406
受信パケット
処理部
1401
1402
パケット
受信部
IPsec復号処理・
デカプセル化処理部
1403
RPパケット保存部
RPパケット
検索部
1404
RPパケット
合成部
1405

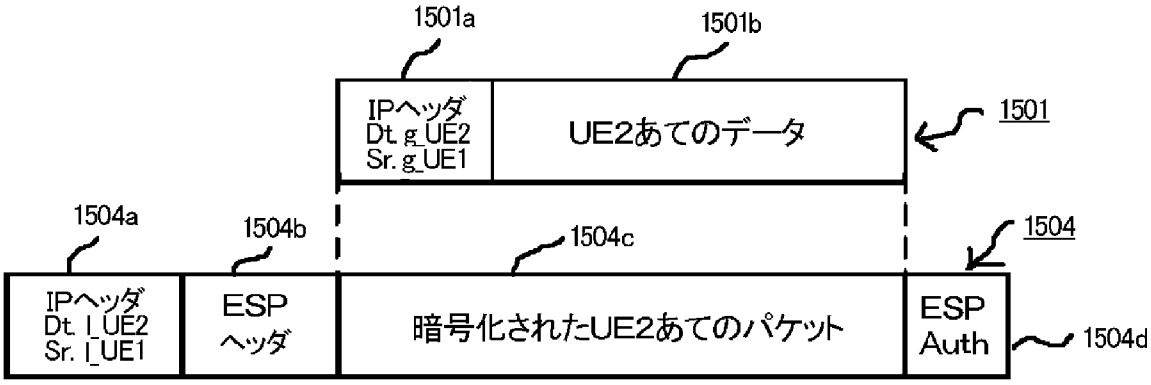
[図15]


106
ユーザ
認証装置
105
ACGW
107
課金管理
装置
103
E-NodeB
E-NodeB
104
UE
UE
101
102

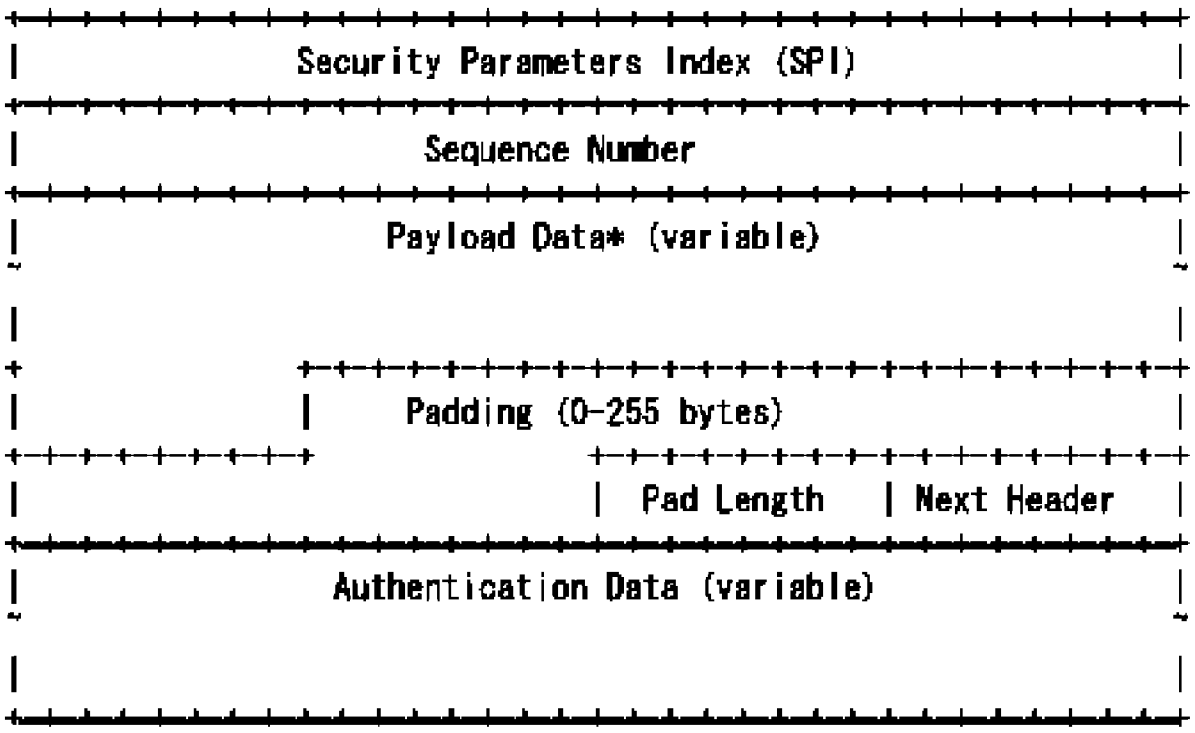
[図16]


1501a
1501b
IPヘッダ
Dt.g_UE2
Sr.g_UE1
UE2あてのデータ
1501
1502a
1502b
1502c
1502d
IPヘッダ
Dt.l_ACGW
Sr.l_UE1
ESP
ヘッダ
暗号化されたUE2あてのパケット
ESP
Auth
1502

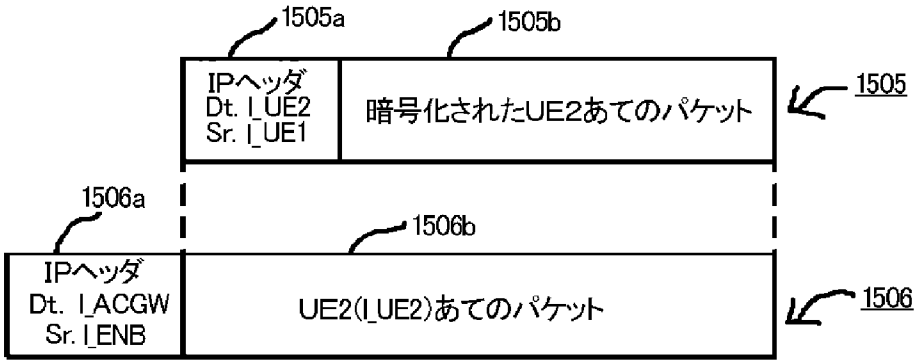
[図17]


1501a
1501b
IPヘッダ
Dt. g_UE2
Sr. g_UE1
UE2あてのデータ
1501
1504a
1504b
1504c
1504
IPヘッダ
Dt. l_UE2
Sr. l_UE1
ESP
ヘッダ
暗号化されたUE2あてのパケット
ESP
Auth
1504d

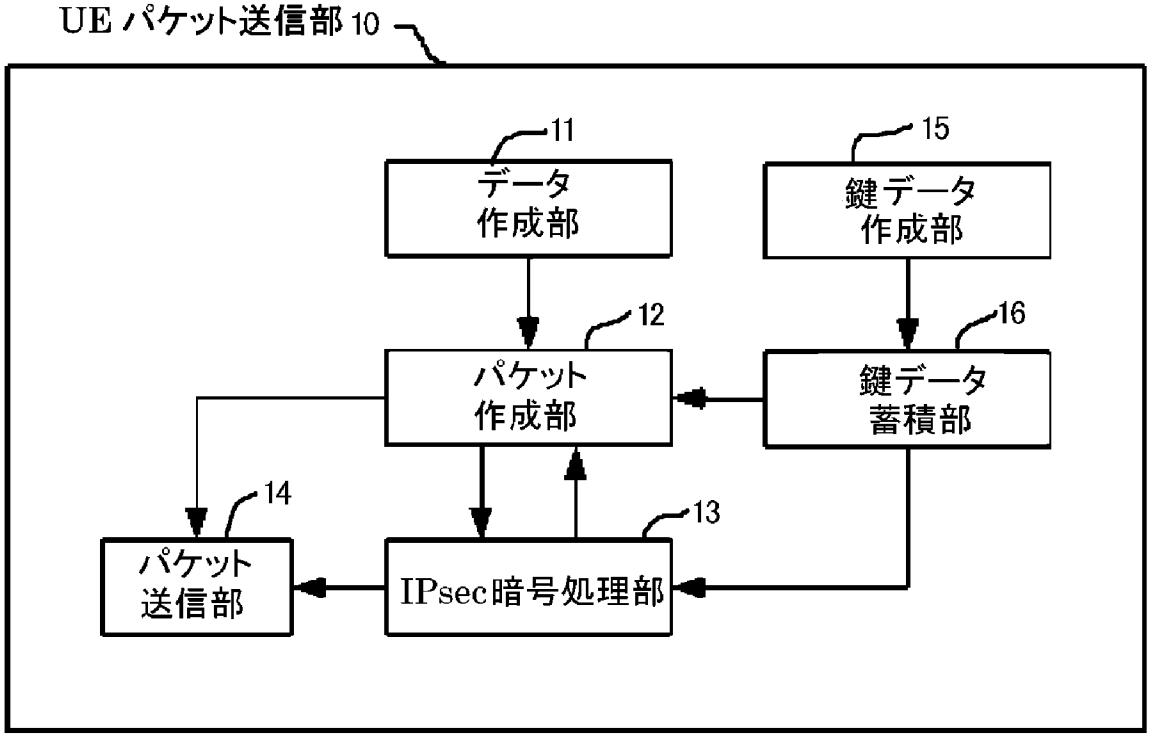
[図18]


Security Parameters Index (SPI)
Sequence Number
Payload Data* (variable)
Padding (0-255 bytes)
Pad Length
Next Header
Authentication Data (variable)

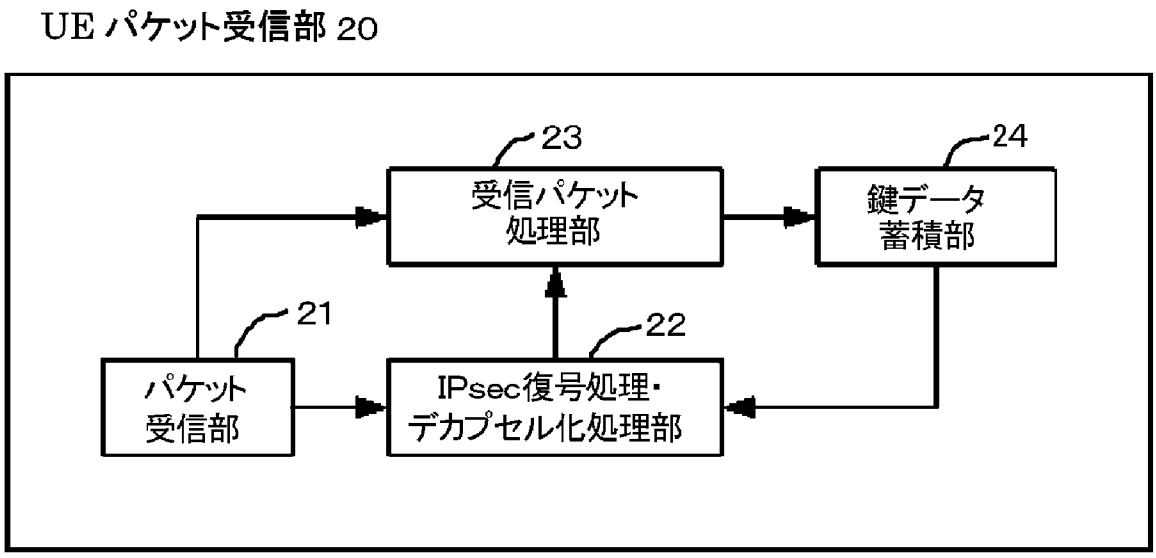
[図19]


1505a
1505b
IPヘッダ
Dt. I_UE2
Sr. I_UE1
暗号化されたUE2あてのパケット
1505
1506a
1506b
IPヘッダ
Dt. I_ACGW
Sr. I_ENB
UE2(I_UE2)あてのパケット
1506

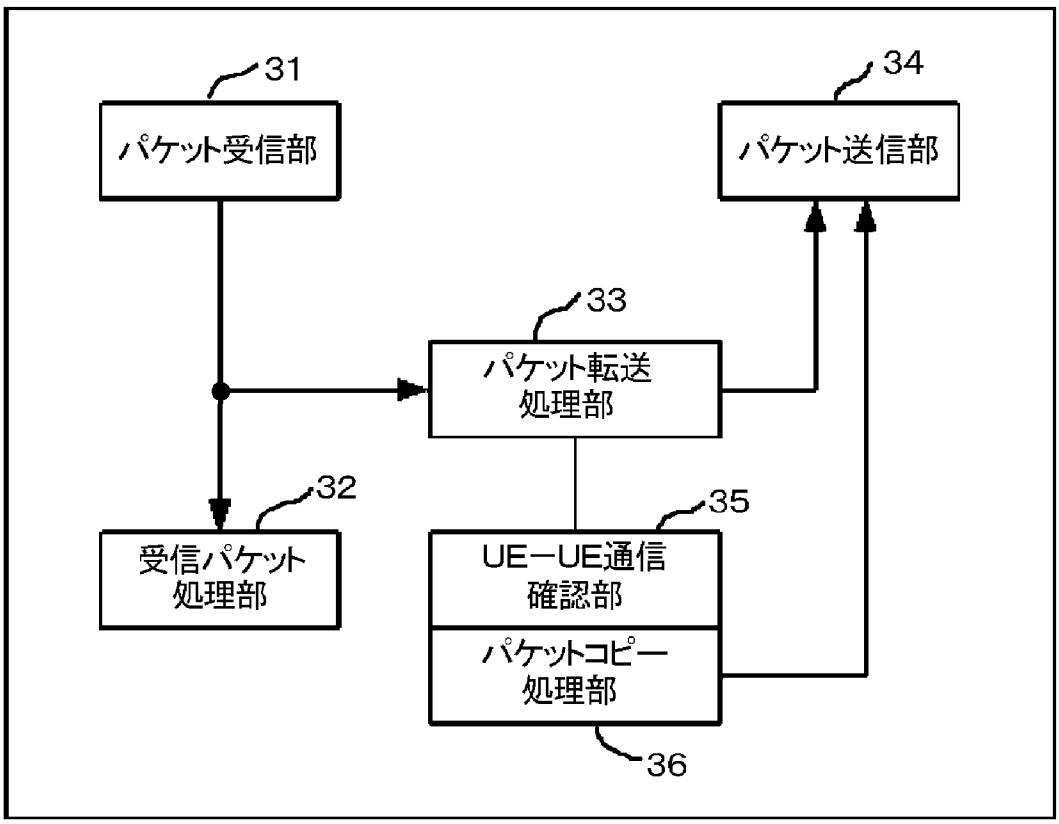
[図20]


UE パケット送信部 10
11
データ
作成部
15
鍵データ
作成部
12
パケット
作成部
16
鍵データ
蓄積部
14
パケット
送信部
13
IPsec暗号処理部

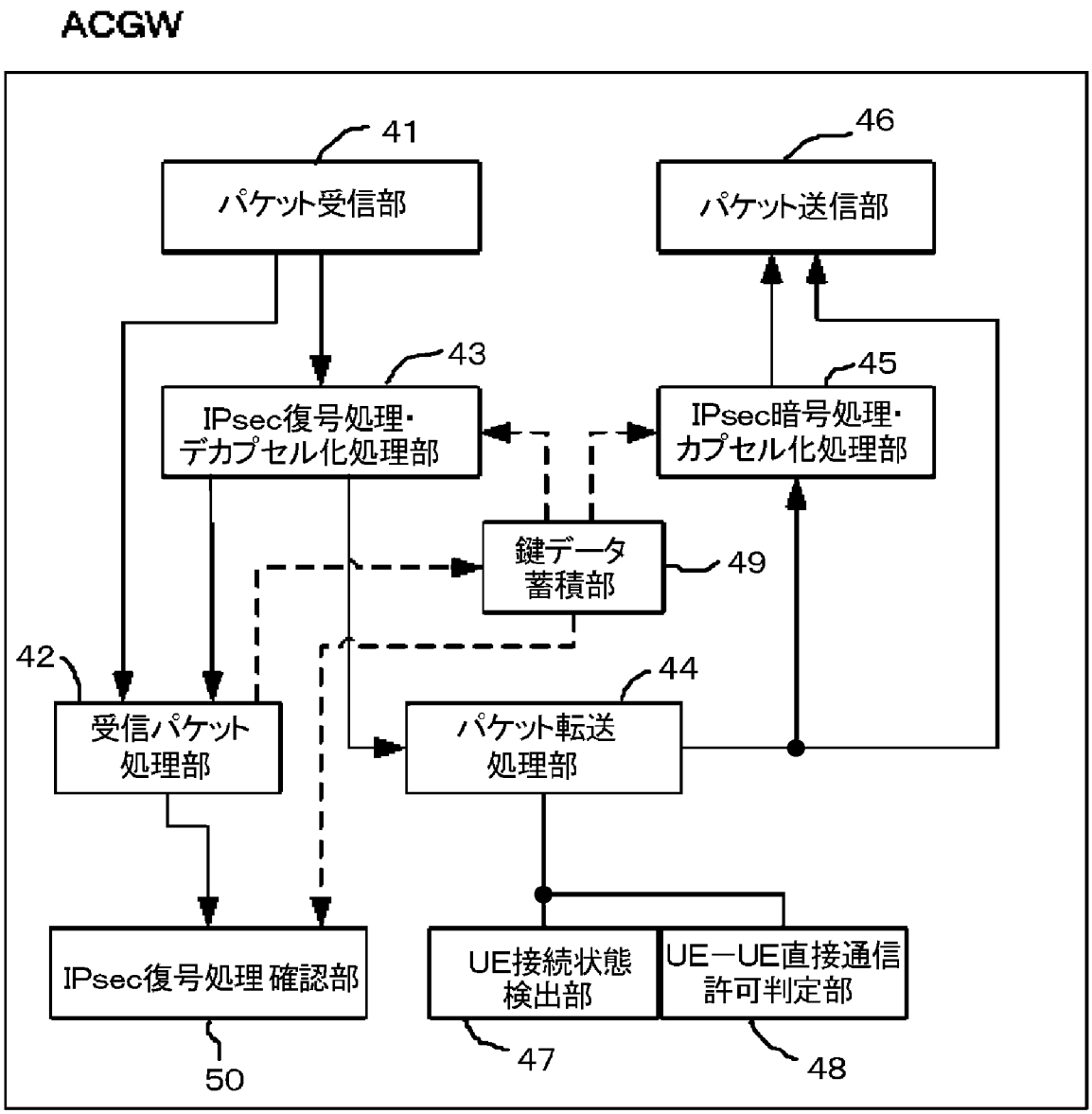
[図21]


UE パケット受信部 20
23
受信パケット
処理部
24
鍵データ
蓄積部
21
パケット
受信部
22
IPsec復号処理・
デカプセル化処理部

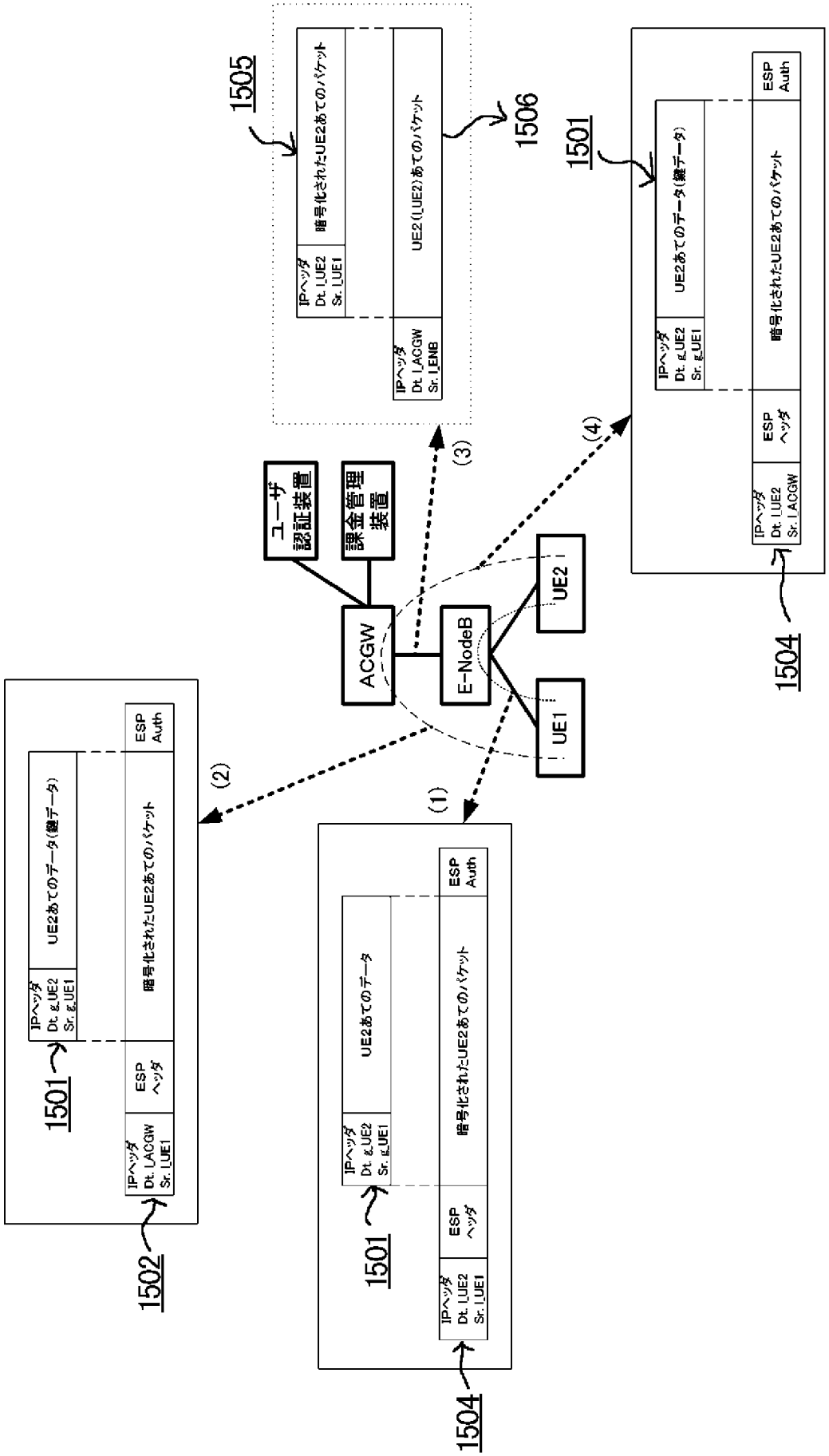
[図22]


E−NodeB
31
パケット受信部
34
パケット送信部
33
パケット転送
処理部
32
受信パケット
処理部
35
UE−UE通信
確認部
パケットコピー
処理部
36

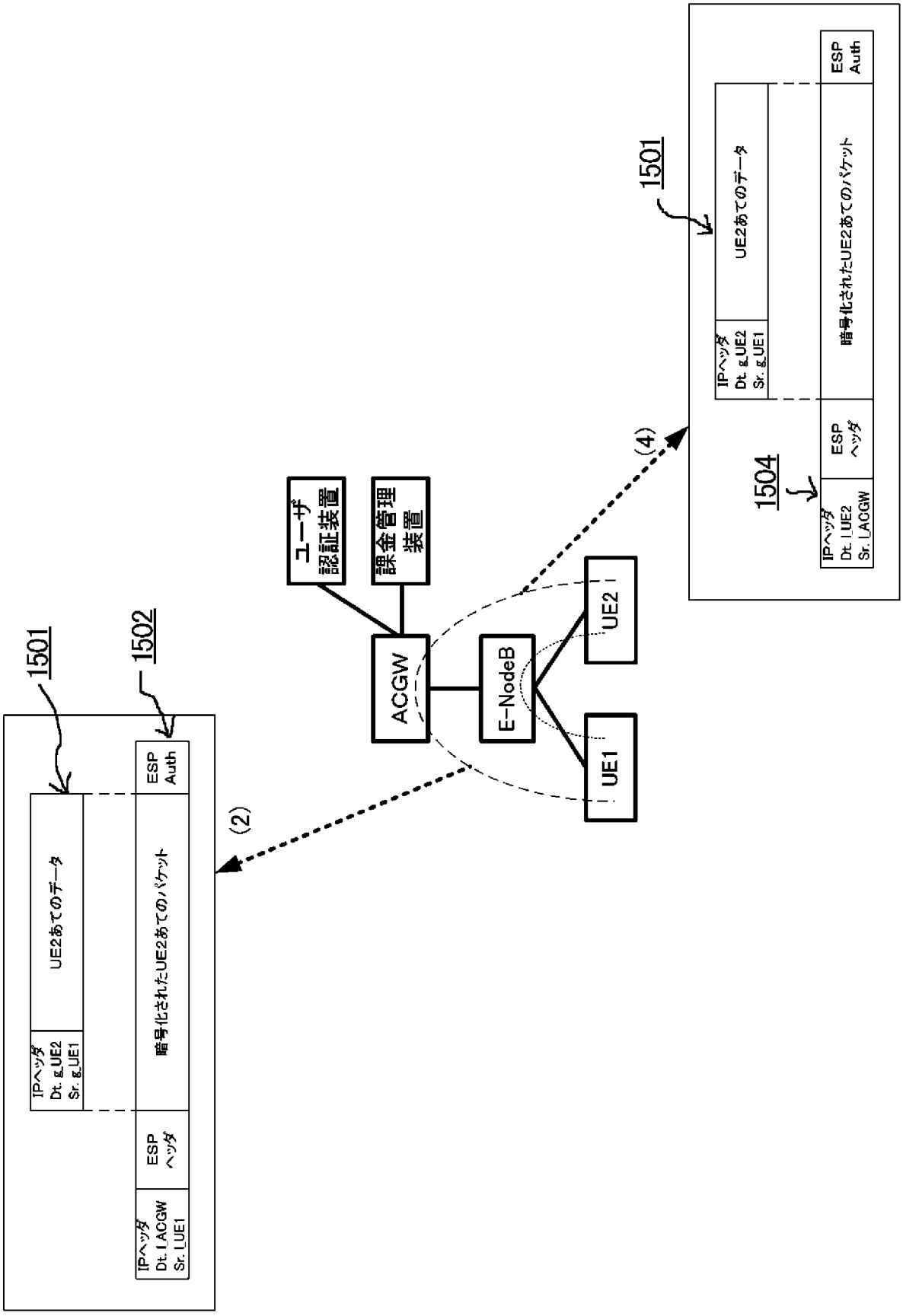
[図23]


ACGW
41
パケット受信部
46
パケット送信部
43
IPsec復号処理・
デカプセル化処理部
45
IPsec暗号処理・
カプセル化処理部
鍵データ
蓄積部
49
42
受信パケット
処理部
44
パケット転送
処理部
IPsec復号処理 確認部
50
UE接続状態
検出部
47
UE－UE直接通信
許可判定部
48

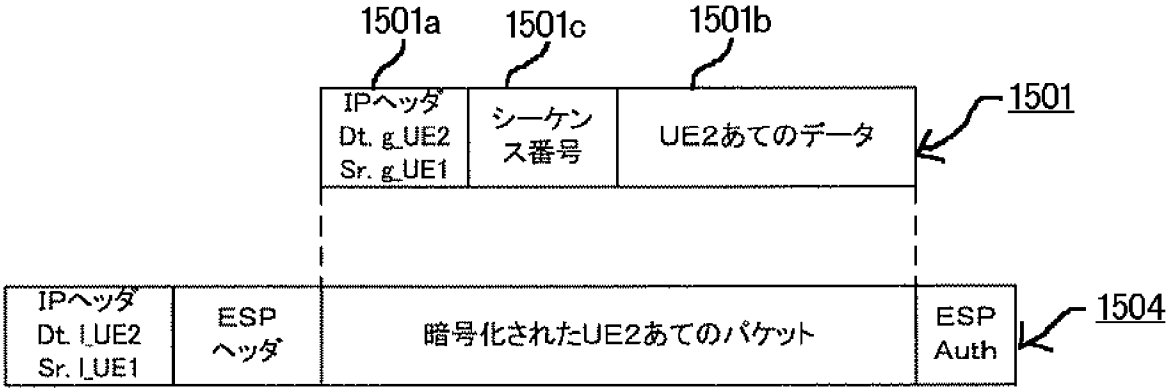
[図24]


1505
1506
1501
1504
1502
ユーザ認証装置
課金管理装置
ACGW
E-NodeB
UE2
UE1
(1)
(2)
(3)
(4)
IPヘッダ Dt. LUE2 Sr. LUE1
暗号化されたUE2あてのパケット
IPヘッダ Dt. LACGW Sr. LENB
UE2(LUE2)あてのパケット
IPヘッダ Dt. gUE2 Sr. gUE1
UE2あてのデータ(鍵データ)
ESP ヘッダ
ESP Auth
IPヘッダ Dt. LACGW Sr. LUE1
UE2あてのデータ

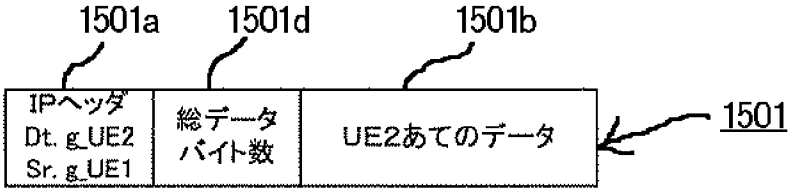
[図25]


1501
1502
IPヘッダ
Dt. I_ACGW
Sr. I_UE1
ESP
ヘッダ
暗号化されたUE2あてのパケット
ESP
Auth
IPヘッダ
Dt. g_UE2
Sr. g_UE1
UE2あてのデータ
(2)
ACGW
E-NodeB
UE1
UE2
ユーザ
認証装置
課金管理
装置
(4)
1501
1504
IPヘッダ
Dt. I_UE2
Sr. I_ACGW
ESP
ヘッダ
暗号化されたUE2あてのパケット
ESP
Auth
IPヘッダ
Dt. g_UE2
Sr. g_UE1
UE2あてのデータ

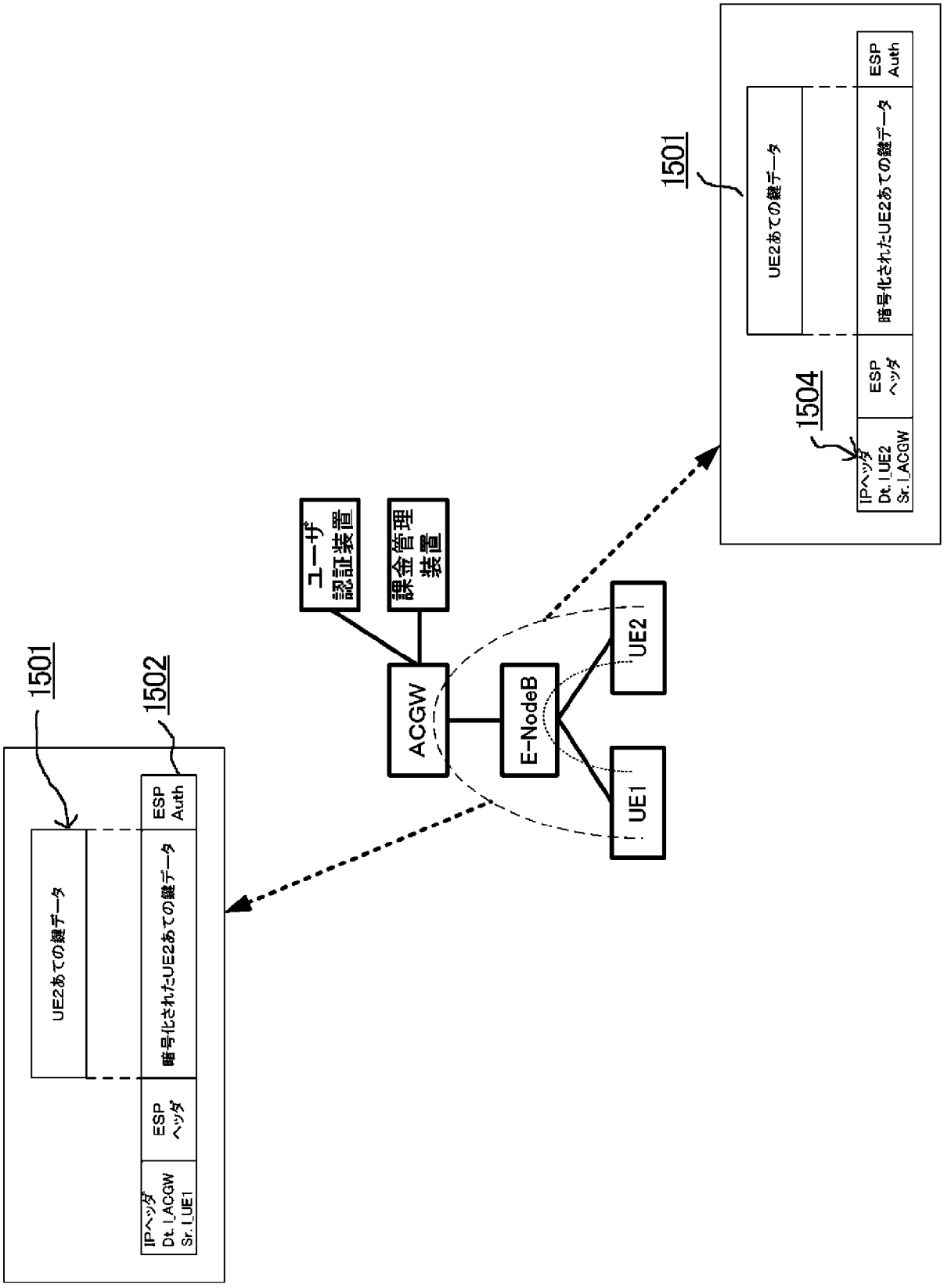
[図26]


1501a
1501c
1501b
IPヘッダ
Dt. g_UE2
Sr. g_UE1
シーケンス番号
UE2あてのデータ
1501
IPヘッダ
Dt. l_UE2
Sr. l_UE1
ESP ヘッダ
暗号化されたUE2あてのパケット
ESP Auth
1504

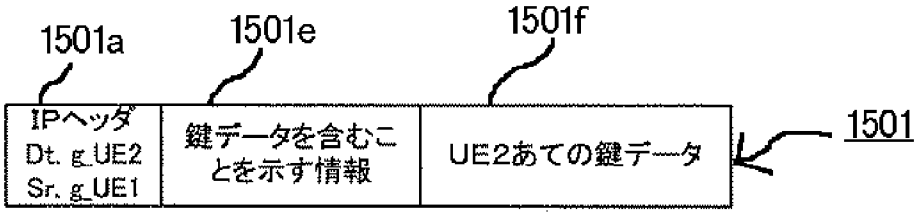
[図27]


1501a
1501d
1501b
IPヘッダ
Dt. g_UE2
Sr. g_UE1
総データバイト数
UE2あてのデータ
1501

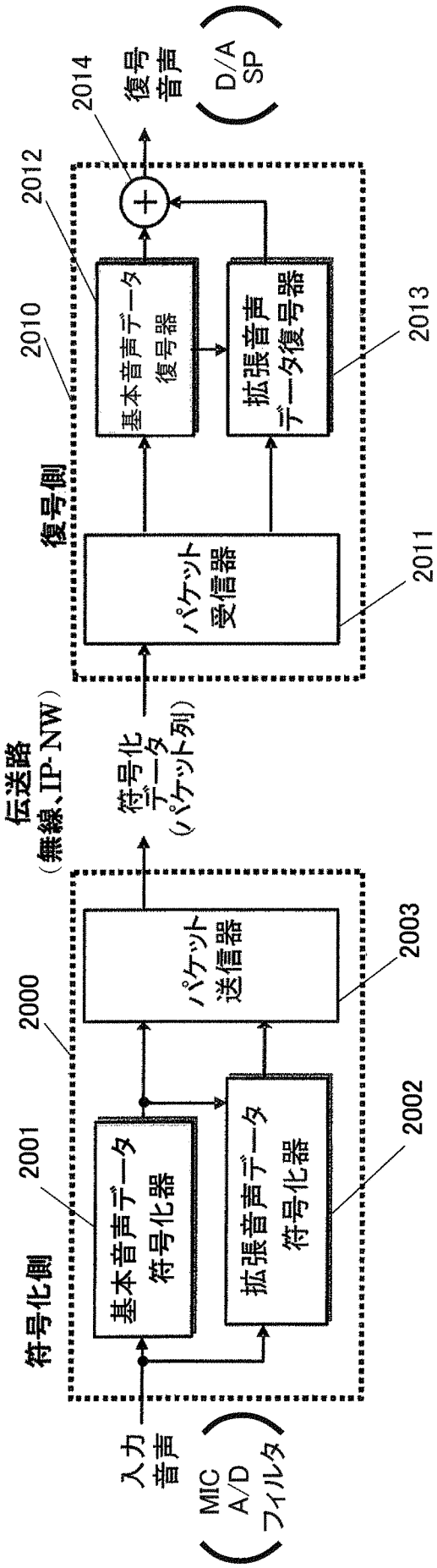
[図28]


1501
1502
UE2あての鍵データ
暗号化されたUE2あての鍵データ
ESP Auth
ESP ヘッダ
IPヘッダ Dt. I_ACGW Sr. I_UE1
ユーザ認証装置
課金管理装置
ACGW
E-NodeB
UE2
UE1
1501
UE2あての鍵データ
暗号化されたUE2あての鍵データ
ESP Auth
ESP ヘッダ
1504
IPヘッダ Dt. I_UE2 Sr. I_ACGW

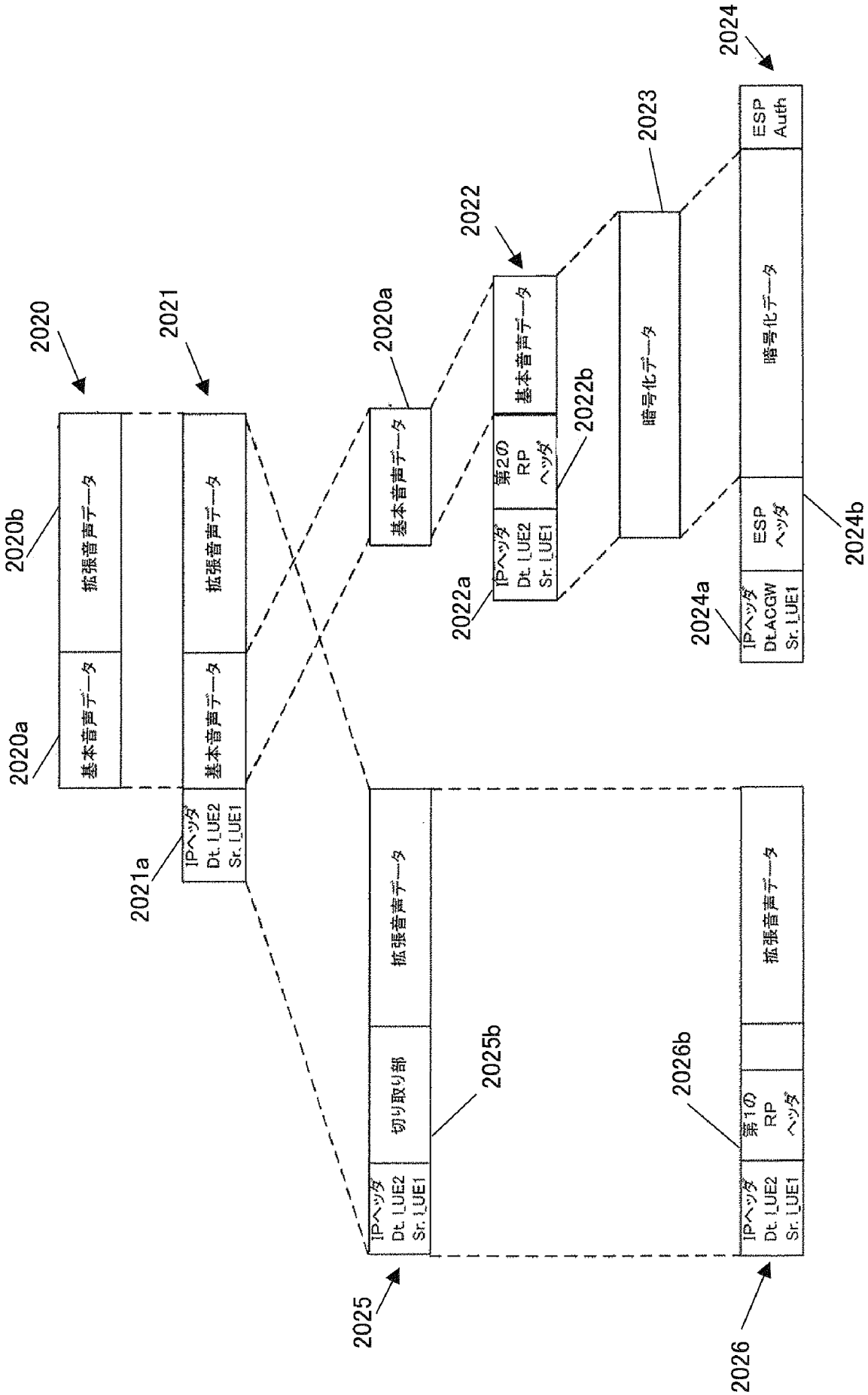
[図29]


1501a
1501e
1501f
IPヘッダ
Dt. g_UE2
Sr. g_UE1
鍵データを含むこ
とを示す情報
UE2あての鍵データ
1501

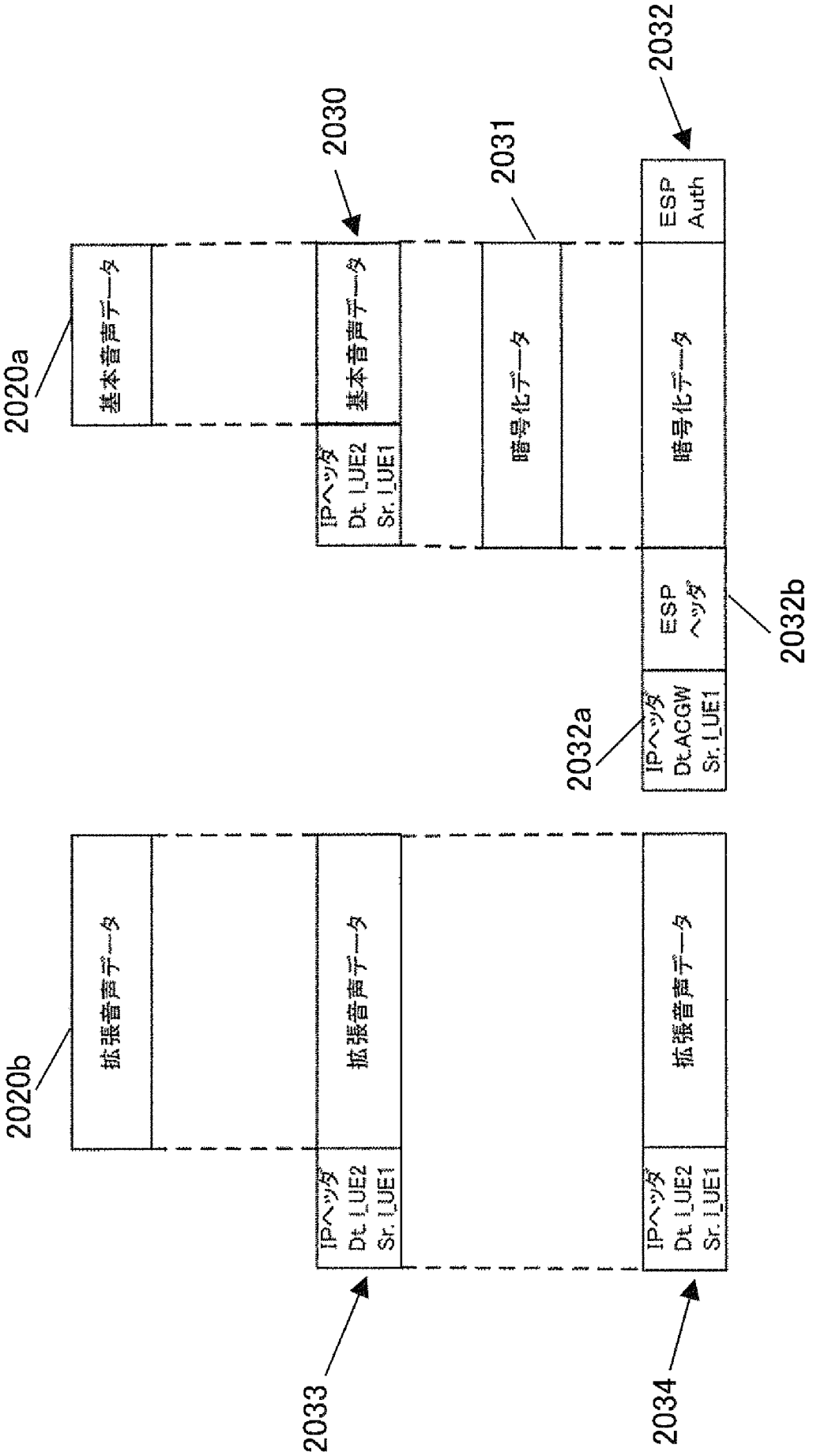
[図30]


入力音声
MIC
A/D
フィルタ
符号化側
2000
2001
基本音声データ符号化器
2002
拡張音声データ符号化器
2003
パケット送信器
伝送路
（無線、IP-NW）
符号化データ
（パケット列）
復号側
2010
2011
パケット受信器
2012
基本音声データ復号器
2013
拡張音声データ復号器
2014
復号音声
D/A
SP

[図31]


2020
2021
2020a
2020b
2021a
2022
2022a
2022b
2023
2024
2024a
2024b
2025
2025b
2026
2026b
基本音声データ
拡張音声データ
IPヘッダ
Dt. LUE2
Sr. LUE1
第2のRPヘッダ
暗号化データ
ESP ヘッダ
ESP Auth
IPヘッダ
Dt.ACGW
Sr. LUE1
切り取り部
第1のRPヘッダ

[図32]


2020a
基本音声データ
2030
IPヘッダ
Dt. I_UE2
Sr. I_UE1
基本音声データ
2031
暗号化データ
2032
ESP
Auth
暗号化データ
2032b
ESP
ヘッダ
2032a
IPヘッダ
Dt.ACGW
Sr. I_UE1
2020b
拡張音声データ
IPヘッダ
Dt. I_UE2
Sr. I_UE1
拡張音声データ
2033
IPヘッダ
Dt. I_UE2
Sr. I_UE1
拡張音声データ
2034

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2007/066416

A. CLASSIFICATION OF SUBJECT MATTER
H04Q7/38(2006.01)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)
H04Q7/38

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 1996-2007
Kokai Jitsuyo Shinan Koho 1971-2007 Toroku Jitsuyo Shinan Koho 1994-2007

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 2006-211614 A (Mitsubishi Electric Corp.), 10 August, 2006 (10.08.06), Full text; all drawings (Family: none)	1-36
A	JP 2004-007457 A (Sony Corp.), 08 January, 2004 (08.01.04), Full text; all drawings & US 2004/029602 A1 & US 7242942 B2	1-36
A	JP 2006-157454 A (Sharp Corp.), 15 June, 2006 (15.06.06), Full text; all drawings (Family: none)	1-36

☒ 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	Date of mailing of the international search report
09 November, 2007 (09.11.07)	20 November, 2007 (20.11.07)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2007/066416

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
E,A	JP 2007-235827 A (NEC Corp.), 13 September, 2007 (13.09.07), Full text; all drawings (Family: none)	1-36

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００７／０６６４１６

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04Q7/38(2006.01)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（ＩＰＣ））

Int.Cl.　H04Q7/38

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	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００７年
日本国実用新案登録公報	１９９６－２００７年
日本国登録実用新案公報	１９９４－２００７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	関連する請求の範囲の番号
A	JP 2006-211614 A (三菱電機株式会社) 2006.08.10, 全文及び全図 (ファミリーなし)	1-36
A	JP 2004-007457 A (ソニー株式会社) 2004.01.08, 全文及び全図 & US 2004/029602 A1 & US 7242942 B2	1-36

☑　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	国際調査報告の発送日
０９．１１．２００７	２０．１１．２００７

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
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）　５Ｊ　３５６９
小河　誠巳
電話番号　０３－３５８１－１１０１　内線　３５３４

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	関連する請求の範囲の番号
A	JP 2006-157454 A (シャープ株式会社) 2006.06.15, 全文及び全図 (ファミリーなし)	1-36
EA	JP 2007-235827 A (日本電気株式会社) 2007.09.13, 全文及び全図 (ファミリーなし)	1-36