(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2012-257328
(P2012-257328A)
(43)公開日　平成24年12月27日(2012.12.27)

(51)Int.Cl.		F I			テーマコード（参考）
H04W 12/04	(2009.01)	H04Q	7/00	182	5K067

審査請求 有　請求項の数 8　ＯＬ　（全 19 頁）

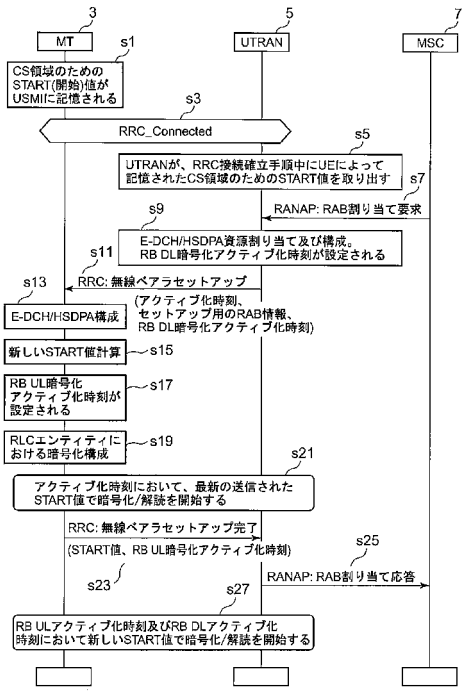
(21)出願番号　特願2012-204224 (P2012-204224)
(22)出願日　平成24年9月18日 (2012.9.18)
(62)分割の表示　特願2010-522110 (P2010-522110)の分割
原出願日　平成21年1月30日 (2009.1.30)
(31)優先権主張番号　0801825.1
(32)優先日　平成20年1月31日 (2008.1.31)
(33)優先権主張国　英国 (GB)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100077838
弁理士　池田　憲保
(74)代理人　100082924
弁理士　福田　修一
(74)代理人　100129023
弁理士　佐々木　敬
(72)発明者　シャーマ，　ビベック
東京都港区芝五丁目７番１号　日本電気株式会社内
(72)発明者　久保田　啓一
東京都港区芝五丁目７番１号　日本電気株式会社内

最終頁に続く

(54)【発明の名称】通信システム

(57)【要約】
【課題】移動通信デバイス内及びＵＴＲＡＮ内の無線ベアラをセットアップするのに２段階手順が使用される移動通信システムを提案する。
【解決手段】第１段階では、移動デバイス及びＵＴＲＡＮの双方は、古い開始値に基づいて暗号化を実行する。第２段階では、移動デバイス及びＵＴＲＡＮは、新しい開始値に基づいて暗号化を実行する。このように、無線ベアラを使用したデータ通信は、移動デバイスがセットアップ手順の完了を確認することを待つことなく開始することができる。
【選択図】図６



【特許請求の範囲】
【請求項１】
無線ベアラのセットアップ又は再構成において移動通信ノードにより実行される方法であって、
データをネットワーク通信ノードと通信できるように自移動通信ノード内の無線ベアラの構成に使用する無線ベアラセットアップメッセージを前記ネットワーク通信ノードから受信すること、
前記無線ベアラセットアップメッセージの受信に応じて、前記ネットワーク通信ノードとの間で通信されるデータの暗号化及び解読に使用される暗号入力パラメータの値を求めることに使用される新しい暗号データを算定すること、
前記新しい暗号データが含まれた 前記無線ベアラがセットアップされたことを確認する無線ベアラセットアップ完了メッセージを前記ネットワーク通信ノードに送信すること、
前記無線ベアラセットアップ完了メッセージの前記送信前では、既存の暗号データを使用して求められた暗号入力パラメータの値を使用して、前記無線ベアラにより送信されるデータを暗号化すること及び前記無線ベアラにより受信されたデータを解読すること、並びに、
前記無線ベアラセットアップ完了メッセージの前記送信後では、前記新しい暗号データを使用して求められた前記暗号入力パラメータの新しい値を使用して、前記無線ベアラにより送信されるデータを暗号化すること及び前記無線ベアラにより受信されたデータを解読すること、
を含む、方法。
【請求項２】
無線ベアラのセットアップ又は再構成においてネットワーク通信ノードにより実行される方法であって、
移動通信ノードに向けて、データをネットワーク通信ノードと通信できるように前記移動通信ノード内での無線ベアラの構成に使用させる無線ベアラセットアップメッセージを送信すること、
前記移動通信ノードが算定した新しい暗号データが含まれた 前記無線ベアラがセットアップされたことを確認する無線ベアラセットアップ完了メッセージを前記移動通信ノードから受信すること、
前記無線ベアラセットアップ完了メッセージの前記受信前では、既存の暗号データを使用して求められた暗号入力パラメータの値を使用して、前記無線ベアラにより送信されるデータを暗号化すること及び前記無線ベアラにより受信されたデータを解読すること、並びに、
前記無線ベアラセットアップ完了メッセージの前記受信後では、前記新しい暗号データを使用して求められた前記暗号入力パラメータの新しい値を使用して、前記無線ベアラにより送信されるデータを暗号化すること及び前記無線ベアラにより受信されたデータを解読すること、
を含む、方法。
【請求項３】
規定されたアクティブ化時刻に前記無線ベアラをアクティブ化すること含む請求項１又は２に記載の方法。
【請求項４】
移動通信ノードであって、
ネットワーク通信ノードから、データを前記ネットワーク通信ノードと通信できるように自移動通信ノード内の無線ベアラの構成に使用する無線ベアラセットアップメッセージを受信する手段と、
前記ネットワーク通信ノードとの間で通信されるデータの暗号化及び解読に使用される暗号入力パラメータの値を求めることに使用される新しい暗号データを算定して、前記無

線ベアラセットアップメッセージの受信に応じる手段と、
前記新しい暗号データを含めた 前記無線ベアラがセットアップされたことを確認する無線ベアラセットアップ完了メッセージを前記ネットワーク通信ノードに送信する手段と、
ｉ）前記無線ベアラセットアップ完了メッセージの前記送信前では、既存の暗号データを使用して求められた暗号入力パラメータの値を使用して、前記無線ベアラにより送信されるデータを暗号化すること及び前記無線ベアラにより受信されたデータを解読すると共に、
ｉｉ）前記無線ベアラセットアップ完了メッセージの前記送信後では、前記新しい暗号データを使用して求められた前記暗号入力パラメータの新しい値を使用して、前記無線ベアラにより送信されるデータを暗号化すること及び前記無線ベアラにより受信されたデータを解読する
ように動作する暗号化手段と、
を備える移動通信ノード。
【請求項５】
ネットワーク通信ノードであって、
移動通信ノードに向けて、データを前記ネットワーク通信ノードと通信できるように前記移動通信ノード内での無線ベアラの構成に使用させる無線ベアラセットアップメッセージを送信する手段と、
前記移動通信ノードが算定した新しい暗号データが含まれている 前記無線ベアラがセットアップされたことを確認する無線ベアラセットアップ完了メッセージを前記移動通信ノードから受信する手段と、
ｉ）前記無線ベアラセットアップ完了メッセージの前記受信前では、既存の暗号データを使用して求められた暗号入力パラメータの値を使用して、前記無線ベアラにより送信されるデータを暗号化すること及び前記無線ベアラにより受信されたデータを解読すると共に、
ｉｉ）前記無線ベアラセットアップ完了メッセージの前記受信後では、前記新しい暗号データを使用して求められた前記暗号入力パラメータの新しい値を使用して、前記無線ベアラにより送信されるデータを暗号化すること及び前記無線ベアラにより受信されたデータを解読する
ように動作する暗号化手段と、
を備えるネットワーク通信ノード。
【請求項６】
前記無線ベアラセットアップメッセージ内に規定されたアクティブ化時刻に前記無線ベアラをアクティブ化する手段を含む請求項４に記載の移動通信ノード。
【請求項７】
前記無線ベアラセットアップメッセージ内に規定されたアクティブ化時刻に前記無線ベアラをアクティブ化する手段を含む請求項５に記載のネットワーク通信ノード。
【請求項８】
請求項１ないし３のいずれか一項に記載の方法をプログラマブルコンピュータデバイスに実行させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、移動通信ネットワーク、限定はしないが、特に３ＧＰＰ（第３世代パートナーシッププロジェクト）標準規格、又はその等価規格若しくは派生規格に従って動作するネットワークに関する。
【背景技術】
【０００２】
移動通信ネットワークでは、ユーザ機器（ＵＥ）がネットワークへデータを送信したい

とき又はネットワークからデータを受信したいとき、ネットワークは、ＵＥが正しいパラメータを使用してネットワークと通信できるように、最初に、ＵＥへ構成データを送信する。この構成データは、特に、ＵＥがネットワークへ送信するアップリンクデータの暗号化をＵＥが開始すべき時（アクティブ化時刻）を含む。ＵＥは、構成データの受信に応答して、それに従い自身の内部資源を構成し、構成が成功したことを確認するメッセージをネットワークへ返信する。ネットワークは、この確認メッセージの受信後、次に、ダウンリンクデータの暗号化を開始する。しかしながら、実際には、この確認メッセージは、アクティブ化時刻の後になるまで送信されない場合があり、この場合、ネットワークが構成確認メッセージを受信する前は、ＵＥからネットワークへ送信されるいかなるアップリンクデータも又はネットワークからＵＥへ送信されるいかなるダウンリンクデータも、適切に解読することができない。

【０００３】

３ＧＰＰ標準規格ＴＳ２５．３３１ Ｖ８．１．０（この内容は参照により本明細書に援用される）は、この構成がＵＴＲＡＮ（ユニバーサル移動電気通信システム（ＵＭＴＳ）地上無線アクセスネットワーク）でどのように実行されるべきかを規定している。

【発明の概要】

【発明が解決しようとする課題】

【０００４】

本発明は、少なくともこの問題を軽減する代替的な構成を提供することを目的とする。

【課題を解決するための手段】

【０００５】

１つの態様によれば、本発明は、無線ベアラのセットアップ又は再構成において通信ノードにより実行される方法であって、無線ベアラセットアップメッセージを別の通信ノードと通信する第１の通信ステップ；規定されたアクティブ化時刻に無線ベアラをアクティブ化すること；無線ベアラがセットアップされたことを確認する無線ベアラセットアップ完了メッセージを通信すると共に、別の通信ノードとの間で通信されるデータの暗号化及び解読に使用される暗号入力パラメータの値を変更することに使用される新しい暗号データを通知する第２の通信ステップを含む、方法を提供する。無線ベアラの暗号化構成は、２段階プロセスにおいて完成する。第１の段階では、無線ベアラのアクティブ化と新しい暗号データを通信することとの間で、本方法は、上記暗号入力パラメータの第１の値を使用して、無線ベアラにより送信されるデータを暗号化することと無線ベアラにより受信されたデータを解読する。第２の段階では、本方法は、新しい暗号データを通信した後に、上記新しい暗号データを使用して生成された上記暗号入力パラメータの第２の値を使用して、無線ベアラにより送信されるデータを暗号化することと無線ベアラにより受信されたデータを解読する。

【０００６】

通常、アクティブ化時刻は、無線ベアラセットアップメッセージ内に規定され、新しい暗号データは、無線ベアラセットアップ完了メッセージで通信される。

【０００７】

一つの実施の形態では、暗号入力パラメータの第１の値は、上記第１の通信ステップより前（ＲＲＣ接続セットアップ手順の間等）に別の通信ノードと通信された以前の暗号データを使用して生成される。暗号データは、通信ノードのうちの１つによって保持される開始値とすることができる。この暗号データは、通信されるデータを暗号化又は解読するのに直接使用されないが、暗号入力パラメータの値（カウントｃとすることができる）を求めるのに使用される計算の一部である。

【０００８】

暗号入力パラメータの第１の値及び第２の値は、送信されるデータを暗号化することに使用される送信暗号入力パラメータ値鍵及び受信されたデータを解読することに使用される受信暗号入力パラメータ値を含むことができる。これらの暗号入力パラメータ値は、データパケットが通信されるごとに、既知の暗号化技法を使用して更新することができる。

【０００９】
この方法は、移動通信デバイス（移動電話又は携帯電話等）が実行することができる。この場合、第１の通信ステップは受信ステップとなり、第２の通信ステップは送信ステップとなる。代替的に、この方法は、ネットワーク通信ノード（ＵＴＲＡＮ等）が実行することもでき、この場合、第１の通信ステップは送信ステップとなり、第２の通信ステップは受信ステップとなる。
【００１０】
好ましい実施の形態では、双方の通信ノードは、好ましくは、それぞれの送信暗号アクティブ化時刻及び受信暗号アクティブ化時刻まで、変更された暗号入力パラメータを使用したデータの暗号化又は解読を開始しない。アップリンク暗号アクティブ化時刻は、ダウンリンク暗号アクティブ化時刻と異なる場合がある。これらの暗号アクティブ化時刻は、通信ノードの一方又は双方が計算することができ、システムフレーム番号又は無線ベアラを使用して通信されるパケットのシーケンス内におけるパケットのシーケンス番号等、時間依存パラメータによって規定することができる。暗号アクティブ化時刻を計算するノードは、他方のノードへその情報を送信しなければならず、その結果、該他方のノードは、変更された暗号入力パラメータを使用したデータの暗号化／解読を開始する時を知る。暗号アクティブ化時刻の計算は、（例えば、無線ベアラセットアップメッセージにおいて）無線ベアラについて規定されたデータレートと、他方の通信ノードが、変更された暗号入力パラメータを使用してデータを暗号化／解読する準備ができる推定時刻とに基づいて行うことができる。
【００１１】
本発明のこの態様は、上記方法を実行する、移動デバイス又はネットワークデバイス等の通信ノードも提供する。
【００１２】
一実施の形態は、移動通信デバイス内の無線ベアラを構成する方法を説明する。この方法は、無線ベアラを構成するための制御データ及び構成された無線ベアラをアクティブ化するためのアクティブ化時刻を規定するデータを受信すること；無線ベアラによって送信されるアップリンクデータを暗号化することに使用される新しい暗号データを求めること；暗号アクティブ化時刻を求めること；求められた暗号アクティブ化時刻及び求められた新しい暗号データを通信ノードへシグナリングすることを含み、上記アクティブ化時刻と上記暗号アクティブ化時刻との間では、本方法は、以前の暗号データを使用して送信用のアップリンクデータを暗号化することをさらに含み；上記暗号アクティブ化時刻の後は、この方法は、上記新しい暗号データを使用して送信用のアップリンクデータを暗号化することを含む。
【００１３】
別の実施の形態は、無線ベアラのセットアップ又は再構成において移動通信デバイスにより実行される方法を説明する。この方法は、遠隔の通信ノードから無線ベアラセットアップメッセージを受信することであって、遠隔の通信ノードとデータを通信するように無線ベアラを構成することに使用される前記無線ベアラセットアップメッセージを受信すること；受信された無線ベアラセットアップメッセージに従って無線ベアラを構成すること；構成された無線ベアラを、遠隔の通信ノードによって規定されたアクティブ化時刻にアクティブ化すること；上記無線ベアラによって上記遠隔の通信デバイスへ送信されるデータを暗号化することに使用される新しい暗号データを求めること；新しい暗号データを使用してアップリンクデータの暗号化アクティブ化時刻を求めること；上記新しい暗号データ及び上記暗号アクティブ化時刻を上記遠隔の通信デバイスへ送信すること；並びに上記新しい暗号データを使用した上記暗号アクティブ化時刻の後に、上記無線ベアラによって送信されるアップリンクデータを暗号化することを含む。
【００１４】
本発明は、開示される全ての方法に関して、対応する機器において実行するための対応するコンピュータプログラム又はコンピュータプログラム製品、機器自体（ユーザ機器、

ノード又はその構成要素）、及び機器を更新する方法を提供する。
【図面の簡単な説明】
【００１５】
次に、添付図面を参照して、本発明の一実施形態を例として説明する。
【００１６】
【図１】実施形態が適用可能なタイプの移動電気通信システムを概略的に示す図である。
【図２】ＵＴＲＡＮシステムのアーキテクチャを概略的に示す図である。
【図３】図１に示す移動通信デバイス及びＵＴＲＡＮにおいて使用されるプロトコルスタックの３つの層を示す図である。
【図４】図１に示すシステムのＵＴＲＡＮを形成する部分を概略的に示す図である。
【図５】図１に示すシステムの移動通信デバイスを形成する部分を概略的に示す図である。
【図６】図５に示す移動通信デバイスと図４に示すＵＴＲＡＮとの間で構成データを交換することができる一方法を示す図である。
【図７】図５に示す移動通信デバイスと図４に示すＵＴＲＡＮとの間で構成データを交換することができる別の方法を示す図である。
【発明を実施するための形態】
【００１７】
概説
図１は、移動（セルラ）通信システム１を概略的に示している。該システムにおいて、移動電話（ＭＴ）３－０、３－１及び３－２のユーザが、ＵＴＲＡＮ（ユニバーサル移動電気通信システム（ＵＭＴＳ）地上無線アクセスネットワーク）及びコアネットワーク７を介して、他のユーザ（図示せず）と通信することができる。移動電話３とＵＴＲＡＮ５との間の無線リンクのために、複数のアップリンク及びダウンリンク通信資源（チャネライゼーションコード、周波数、サブキャリア、タイムスロット等）を利用することができる。この実施形態において、移動電話３に送信すべきデータの量に応じて、ＵＴＲＡＮ５は、各移動電話３にダウンリンク資源を割り当てる。同様に、移動電話３がＵＴＲＡＮ５に送信しなければならないデータの量及びタイプに応じて、ＵＴＲＡＮ５は、各移動電話３にアップリンク資源を割り当てる。
【００１８】
データが移動電話３とＵＴＲＡＮ５との間で送信されるとき、ＵＴＲＡＮ５は、中でも特に、新しい構成が効力を有するアクティブ化時刻を規定する構成データを移動電話３へ送信する。以下でより詳細に説明するように、移動電話３は、受信された構成データに従って内部資源をセットアップし、完了すると構成確認メッセージを送信する。この実施形態では、少なくとも、アクティブ化時刻と、移動電話３が構成完了メッセージを送信する時刻との間、移動電話３及びＵＴＲＡＮ５の双方は、構成完了メッセージがＵＴＲＡＮ５によって受信される前であってもアップリンクデータ及びダウンリンクデータを送信及び受信できるように、以前の暗号化データ（開始値）を使用する。
【００１９】
プロトコル
図３は、移動電話３及びＵＴＲＡＮ５において用いられるプロトコルスタックの一部（下位の３つの層）を示す。第１の層は物理層（Ｌ１）であり、無線通信チャネルを介してデータを実際に送信する役割を担う。その上には第２の層（Ｌ２）があり、Ｌ２は３つの副層、すなわち、無線インタフェースへのアクセスを制御する役割を担う媒体アクセス制御層（Ｌ２／ＭＡＣ）と、必要に応じて、データパケットの連結及びセグメント化、データパケットの暗号化及び解読、パケットの肯定応答、並びにデータパケットの再送の役割を担うＲＬＣ層（Ｌ２／ＲＬＣ）と、ヘッダ圧縮の役割を担うＰＤＣＰ層（Ｌ２／ＰＤＣＰ）とに分割される。第２の層上には、ＵＴＲＡＮ５と移動電話３との間の無線インタフェースにおいて用いられる無線資源を制御する役割を担う無線資源制御（ＲＲＣ）層（Ｌ３／ＲＲＣ）がある。

【００２０】
Ｕプレーン１９は、移動電話３とＵＴＲＡＮ５との間のユーザデータトランスポートをハンドリングするのに対して、Ｃプレーン２０は、移動電話３とＵＴＲＡＮ５との間のシグナリングデータのトランスポートをハンドリングする。図示するように、Ｌ２／ＲＬＣ層は、Ｃプレーンデータ及びＵプレーンデータの送信を管理するのに使用される複数のＲＬＣエンティティ１５を含み、Ｌ２／ＰＤＣＰ層は、Ｕプレーンデータを処理するのに使用されるＰＤＣＰエンティティ１７を含む。
【００２１】
図３は、送信／受信すべきデータの異なる複数のデータ源に割り当てられる無線ベアラ１８も示す。いくつかのソフトウエアアプリケーションが、同時に動作していることがあり、各アプリケーションがデータを送信及び／又は受信していることがある。それぞれの無線ベアラは、各タスクに関連付けられることになり、いくつかの無線ベアラは、他の無線ベアラよりも高い優先度を割り当てられる。たとえば、リアルタイムサービスに割り当てられる無線ベアラは、非リアルタイムサービスに割り当てられる無線ベアラよりも高い優先度を割り当てられる。図３に示すように、制御プレーン（Ｃプレーン）シグナリングのために別個の無線ベアラ１８が提供される。アップリンクのためにＵＴＲＡＮ５によって割り当てられる通信資源は、それらの割り当てられる優先度及びデータレートに応じて、無線ベアラ１８間で共有される。
【００２２】
移動電話３のＲＲＣ１６は、ＵＴＲＡＮ５と移動電話３との間のすべての無線ベアラ１８をセットアップ及び構成する役割を担う。無線ベアラ１８をセットアップ及び構成するのに、複数の構成手順がＲＲＣ１６に利用可能である。これらの構成手順では、ＵＴＲＡＮ５が特定のメッセージを移動電話３へ送信し、次に移動電話３が対応するメッセージで応答することが必要とされる。一般的に言えば、これらのメッセージは、シグナリング無線ベアラ１８を介して送信される。メッセージには、中でも特に「無線ベアラセットアップ」及び「無線ベアラ再構成」が含まれる。これらのメッセージのそれぞれについて、移動電話３は、移動電話３上での手順の成功を示す対応する「完了」応答メッセージ又は手順の失敗を示す対応する「失敗」応答メッセージを有し、移動電話３は、ＵＴＲＡＮ５が手順を完了するのに必要なあらゆる情報をＵＴＲＡＮ５に提供することができる。加えて、構成メッセージ及び応答メッセージは、オプションの情報要素（ＩＥ）も運ぶことができ、これらの情報要素は、補助情報を保持するデータのフィールドである。
【００２３】
ＳＮ、ＨＦＮ、及び開始リスト
上記で論述したように、作動中、移動電話３は、複数の無線ベアラ１８によりＵＴＲＡＮ５と通信する。移動電話３の各無線ベアラ１８は、ＵＴＲＡＮ５の対応する無線ベアラから受信されたプロトコルデータユニット（ＰＤＵ）を保持するための受信バッファ（図示せず）、及びＵＴＲＡＮ５の対応する無線ベアラへの送信を待っているＰＤＵを保持するための送信バッファ（図示せず）を有する。通常、各無線ベアラ１８は、新しいＰＤＵが送信バッファに追加されるごとにインクリメントされる送信シーケンス番号（ＳＮ）、及びＰＤＵが受信バッファに受信されるごとにインクリメントされる受信シーケンス番号（ＳＮ）を保持する。送信シーケンス番号は、対応するＰＤＵのヘッダに含まれ、送信されたＰＤＵの連続した順序を示す。したがって、受信側は、受信されたＰＤＵ内に組み込まれたシーケンス番号をスキャンして、ＰＤＵの連続した順序を判断することができ、いずれかのＰＤＵが欠落しているか否かを判断することができる。肯定応答モード（ＡＭ）で動作している場合、受信側は、受信された各ＰＤＵのシーケンス番号を使用することによっていずれのＰＤＵが受信されたのかを示すメッセージを送信側へ送信することもできるし、又は再送されるＰＤＵのシーケンス番号を指定することによってＰＤＵを再送するように要求する場合もある。
【００２４】
各シーケンス番号は、ｎビットの数字（通常、７ビットの数字）によって規定され、し

たがって、ＳＮは、２^{n}個のＰＤＵごとにロールオーバする。ハイパーフレーム番号（ＨＦＮ）も、移動電話３及びＵＴＲＡＮ５によって保持される。これらのＨＦＮは、対応するシーケンス番号の上位ビット（すなわち、ＭＳＢ）と考えることができ、通常、ＰＤＵと共に送信されない。移動電話３の各無線ベアラ１８は、受信ハイパーフレーム番号（HFN_R）及び送信ハイパーフレーム番号（HFN_T）を有する。同様に、ＵＴＲＡＮ５上の対応する無線ベアラも、HFN_R及びHFN_Tを有する。移動電話３が、受信バッファにおいてＰＤＵの受信シーケンス番号のロールオーバを検出すると、移動電話３はHFN_Rをインクリメントする。同様に、送信されたＰＤＵのシーケンス番号のロールオーバ時には、移動電話３は、HFN_Tをインクリメントする。同様のプロセスは、ＵＴＲＡＮ５上でも行われる。

【００２５】

この実施形態では、無線ベアラ１８が最初にセットアップされると、ＲＬＣシーケンス番号が０の開始値からインクリメントされる。他方、ＨＦＮは、移動電話３の不揮発性メモリ（通常、ＵＳＩＭ）に記憶された開始リスト（図示せず）によって規定される開始値に初期化される。開始リストは、ＣＳ領域トラフィック及びＰＳ領域トラフィックの別個の開始値を保持する。新しい各無線ベアラがセットアップされるときに移動電話３及びＵＴＲＡＮ５の双方のＨＦＮを同じ値に初期化できるように、移動電話３に電源が投入されると、この開始リストは、ＵＴＲＡＮ５へ送信される。これは、ＨＦＮ及びＲＬＣ ＳＮが、送信及び受信されるＰＤＵの暗号化及び解読において使用されることから重要である。

【００２６】

ＵＴＲＡＮ

図４は、この実施形態において用いられるＵＴＲＡＮ５の主な構成要素を示すブロック図である。図示するように、ＲＮＣ機能及び基地局機能は、単一のデバイスによって実装される。図示するように、ＵＴＲＡＮ５はトランシーバ回路２１を備えており、該トランシーバ回路２１は、１つ又は複数のアンテナ２３を介して移動電話３に対し信号を送受信するように動作することができ、且つネットワークインタフェース２５を介してコアネットワーク７に対し信号を送受信するように動作することができる。コントローラ２７が、メモリ２９に記憶されるソフトウエアに従って、トランシーバ回路２１の動作を制御する。そのソフトウエアは、特に、オペレーティングシステム３１及び暗号化エンジンを含む。メモリは、各移動電話３について、開始リスト３４も含み、関連付けられる各移動電話３及び各無線ベアラについて、送信シーケンス番号及び受信シーケンス番号（ＳＮ）並びに送信ハイパーフレーム番号及び受信ハイパーフレーム番号（ＨＦＮ）３５も含む。暗号化エンジン３３は、暗号化鍵、ベアラＩＤ、方向、カウントｃ値等を含む多くの入力パラメータを有する暗号化アルゴリズムを使用して、移動電話３へ送信されるダウンリンクデータを暗号化し、移動電話３から受信されたアップリンクデータを解読するように動作可能である。この実施形態では、暗号化アルゴリズムは、これらの入力パラメータを使用して、鍵ストリームブロックを求める。この鍵ストリームブロックは、平文ユーザデータを暗号化するのに使用される。カウントｃ入力パラメータは、関連のあるＨＦＮ及びＳＮから計算される。

【００２７】

移動電話

図５は、図１に示される移動電話３のそれぞれの主な構成要素を示すブロック図である。図示するように、移動電話３は、１つ又は複数のアンテナ７３を介してＵＴＲＡＮ５に対し信号を送受信するように動作することができるトランシーバ回路７１を備える。図示するように、移動電話３はコントローラ７５も備えており、該コントローラは、移動電話３の動作を制御し、且つトランシーバ回路７１に接続され、スピーカ７７、マイクロホン７９、ディスプレイ８１及びキーパッド８３に接続される。コントローラ７５は、メモリ８５内に記憶されるソフトウエア命令に従って動作する。図示するように、これらのソフトウエア命令は、特に、オペレーティングシステム８７及び暗号化エンジン８９を含む。

メモリ８５は、移動電話３のための開始リスト９１も含み、現在の送信シーケンス番号及び受信シーケンス番号並びに現在の送信ハイパーフレーム番号及び受信ハイパーフレーム番号９３も含む。通常、開始リスト９１は、ＳＩＭカード（図示せず）等の不揮発性メモリに記憶される。暗号化エンジン８９は、ＵＴＡＮ５と同じ暗号化アルゴリズムを使用して、ＵＴＲＡＮ５へ送信されるアップリンクデータを暗号化し、ＵＴＲＡＮ５から受信されたダウンリンクデータを解読するように動作可能である。

【００２８】

理解するのを容易にするために、上記の説明では、ＵＴＲＡＮ５及び移動電話３は、複数の個別のモジュール（暗号化エンジン３３及び８９等）を有するものとして説明される。たとえば、既存のシステムが本発明を実施するように変更されている特定のアプリケーションに対して、このようにこれらのモジュールが提供される場合があるが、他のアプリケーション、たとえば、最初から本発明の特徴を念頭において設計されたシステムでは、これらのモジュールは、オペレーティングシステム又はコード全体の中に構成することができるので、これらのモジュールは個別のエンティティとして区別することができない場合がある。

【００２９】

ＨＳＰＡによるＣＳ音声の暗号化－第１の実施形態

図６は、ＨＳＰＡ（高速パケットアクセス）により移動電話３とＵＴＲＡＮ５との間でＣＳ音声データを運ぶ無線ベアラのセットアップ手順中のデータに関する交換の第１の提案を示すフロー図である。図示するように、ＣＳ領域の開始値は、移動電話３に記憶され（ステップｓ１）、この場合、ＵＳＩＭモジュール（図示せず）に記憶される。移動電話３及びＵＴＲＡＮ５は、ＲＲＣ接続確立手順に続き、ステップｓ３において「ＲＲＣ＿Ｃｏｎｎｅｃｔｅｄ」モードに入る。ステップｓ５に示すように、このＲＲＣ接続確立手順中、ＵＴＲＡＮ５は、移動電話３からＣＳ領域の開始値を取り出す。ステップｓ７において、ＵＴＲＡＮ５は、ＭＳＣ（コアネットワーク７のＣＳ領域８の一部を形成する移動交換局：Ｍｏｂｉｌｅ　Ｓｗｉｔｃｈｉｎｇ　Ｃｅｎｔｅｒ）からセットアップ又は変更されるＲＡＢ（無線アクセスベアラ）を識別するＲＡＢ　ａｓｓｉｇｎｍｅｎｔ　ｒｅｑｕｅｓｔ（ＲＡＢ割り当て要求）を受信する。ＵＴＲＡＮ５は、次に、ステップｓ９において、受信された要求を処理し、適切な資源割り当て及び構成データを求める。この実施形態では、ＵＴＲＡＮ５は、ステップｓ９において、ＲＢ　ＤＬ暗号化アクティブ化時刻及びアクティブ化時刻も求める。アクティブ化時刻は、移動電話３及びＵＴＲＡＮ５が、新しい無線ベアラ構成の使用を開始する時を規定する。アクティブ化時刻は、移動電話がそのシステムフレーム番号（ＣＦＮ：接続フレーム番号）を受信すると、新しい構成をアクティブ化するようなＣＦＮによって規定される。ＲＢ　ＤＬ暗号化アクティブ化時刻は、ＵＴＲＡＮ５が、移動電話３から受信される新しい開始値を使用してカウントｃ値（暗号入力パラメータ）を変更した結果として生成された新しい鍵ストリームブロックを使用してダウンリンクデータの暗号化を開始する時を規定する。ＲＢ　ＤＬ暗号化アクティブ化時刻は、ダウンリンクデータのためのＲＬＣシーケンス番号（ＳＮ）の点から規定される。上述したように、無線ベアラがセットアップされると、ダウンリンクデータのためのＲＬＣ　ＳＮは、０に初期化され、送信されるＲＬＣ　ＰＤＵごとにインクリメントされる。この実施形態では、ＲＢ　ＤＬ暗号化アクティブ化時刻は、新しい鍵ストリームブロックで暗号化される最初のＲＬＣ　ＤＬ　ＰＤＵのシーケンス番号を識別する。

【００３０】

ステップｓ１１において、ＵＴＲＡＮ５は、ＲＲＣ：ＲＡＤＩＯ　ＢＥＡＲＥＲ　ＳＥＴＵＰ（無線ベアラセットアップ）メッセージを移動電話３へ送信する。このメッセージは、アクティブ化時刻、セットアップ用のＲＡＢ情報、及びＲＢ　ＤＬ暗号化アクティブ化時刻を別個の情報要素（ＩＥ）内に含む。これに応答して、移動電話３のＲＲＣ層１６は、ステップｓ１３において、関連のある無線ベアラ１８を構成する。ステップｓ１５において、移動電話３のＲＲＣ層１６は、３ＧＰＰ標準規格ＴＳ２５．３３１のセクション８．５．９によって規定された方法で新しい開始値を求める。移動電話３のＲＲＣ層１６は

、次に、ステップｓ１７において、移動電話３が、ステップｓ１５において求められた新しい開始値を使用してカウントｃ値を変更した結果として生成された新しい鍵ストリームブロックを使用してアップリンクデータの暗号化を開始する時を規定するＲＢ ＵＬ暗号化アクティブ化時刻を求める。ＲＢ ＤＬ暗号化アクティブ化時刻と同様に、ＲＢ ＵＬ暗号化アクティブ化時刻は、新しい鍵ストリームブロックで暗号化される最初のＲＬＣ ＵＬ ＰＤＵのシーケンス番号（ＳＮ）を識別する。

【００３１】

ステップｓ１９において、ＲＲＣ層１６は、無線ベアラセットアップメッセージに規定されたアクティブ化時刻から、ステップｓ５においてＵＴＲＡＮへ送信された古い開始値を使用して導出された古いカウントｃ値から生成された鍵ストリームブロックを使用したアップリンクデータの暗号化及びダウンリンクデータの解読をステップｓ２１において実行できるように、対応するＲＬＣエンティティ１５を構成する。同様に、ステップｓ２１において、ＵＴＲＡＮ５は、ステップｓ５においてＵＴＲＡＮへ送信された古い開始値を使用する古いカウントｃ値を使用して生成された鍵ストリームブロックを使用したダウンリンクデータの暗号化及びアップリンクデータの解読を開始するように、対応する無線ベアラを（アクティブ化時刻において）アクティブ化する。

【００３２】

その後、ステップｓ２３において、ＲＲＣ層１６は、ＲＲＣ：ＲＡＤＩＯ ＢＥＡＲＥＲ ＳＥＴＵＰ ＣＯＭＰＬＥＴＥ（無線ベアラセットアップ完了）メッセージをＵＴＲＡＮ５へ送信する。このメッセージは、新しい開始値（ステップｓ１５において求められたもの）及びＲＢ ＵＬ暗号化アクティブ化時刻を含む。これに応答して、ＵＴＲＡＮ５は、ステップｓ２５において、無線ベアラの構成の成功を確認するＲＡＢ ＡＳＳＩＧＮＭＥＮＴ ＲＥＳＰＯＮＳＥ（ＲＡＢ割り当て応答）メッセージをＭＳＣへ送信する。最後に、ステップｓ２７において、移動電話３は、ｉ）ＲＬＣ ＵＬ ＳＮが、ＲＢ ＵＬ暗号化アクティブ化時刻によって規定された数に達すると、新しい開始値（ステップｓ１５において求められたもの）を使用してカウントｃ値を変更した結果として生成された新しいアップリンク（送信）鍵ストリームブロックを使用した自身のアップリンクデータの暗号化を開始し、ｉｉ）ＲＬＣ ＤＬ ＳＮが、ＲＢ ＤＬ暗号化アクティブ化時刻によって規定された数に達すると、新しい開始値を使用してカウントｃ値を変更した結果として生成された新しいダウンリンク（受信）鍵ストリームブロックを使用した受信されたダウンリンクデータの解読を開始し；ＵＴＲＡＮ５は、ｉ）ＲＬＣ ＤＬ ＳＮが、ＲＢ ＤＬ暗号化アクティブ化時刻によって規定された数に達すると、新しい開始値を使用してカウントｃ値を変更した結果として生成された新しいダウンリンク（送信）鍵ストリームブロックを使用した自身のダウンリンクデータの暗号化を開始し、ｉｉ）ＲＬＣ ＵＬ ＳＮが、ＲＢ ＵＬ暗号化アクティブ化時刻によって規定された数に達すると、新しい開始値を使用してカウントｃ値を変更した結果として生成された新しいアップリンク（受信）鍵ストリームブロックを使用した受信されたアップリンクデータの解読を開始する。

【００３３】

当業者が認識するように、上述した実施形態の利点は、移動電話３及びＵＴＲＡＮ５が、少なくとも、アクティブ化時刻と、ＲＲＣ：ＲＡＤＩＯ ＢＥＡＲＥＲ ＳＥＴＵＰ ＣＯＭＰＬＥＴＥメッセージがＵＴＲＡＮ５へ送信される時刻との間、データを交換できるということである。しかしながら、当業者が認識するように、この実施形態では、理想的には、移動電話３及びＵＴＲＡＮ５の双方が、それぞれ新しい開始値及び当該新しい開始値が対応するＲＬＣ ＳＮを使用できるときを正確に推定できることが必要とされる。ＲＬＣ ＳＮは、トラフィックフローに基づいてインクリメントされるので、これには、理想的には、移動電話３及びＵＴＲＡＮ５の双方が、コーデックレート、チャネル状態等をできるだけ正確に推定することが必要とされる。これは、Ｌ２／ＭＡＣ層で実行されるセグメンテーションによってさらに複雑化される。

【００３４】

加えて、ＲＬＣ ＳＮは７ビット長であるので、コーデックレートに応じて、ロールオ

ーバが起こる可能性があることに留意すべきである。アクティブ化時刻と、ＲＢ ＤＬ暗号化アクティブ化時刻によって規定された時刻との間の時間差が、２回以上のＲＬＣ ＳＮロールオーバを含む場合、ＲＲＣ：ＲＡＤＩＯ ＢＥＡＲＥＲ ＳＥＴＵＰメッセージには、ロールオーバの回数を示す追加のＩＥが必要とされる。これは、アクティブ化時刻と、ＲＢ ＵＬ暗号化アクティブ化によって規定された時刻との間の時間差が２回以上のＲＬＣ ＳＮロールオーバを含む場合に、ＲＲＣ：ＲＡＤＩＯ ＢＥＡＲＥＲ ＳＥＴＵＰ ＣＯＭＰＬＥＴＥメッセージにも同様に当てはまる。

【００３５】

ＨＳＰＡによるＣＳ音声の暗号化－第２の実施形態

図７は、ＨＳＰＡ（高速パケットアクセス）により移動電話（ＭＴ）３とＵＴＲＡＮ５との間でＣＳ音声データを運ぶ無線ベアラのためのセットアップ手順中のデータの交換に関する第２の提案を示すフロー図である。この提案と第１の提案との間の主な相違は、この提案では、移動電話３が、ＲＢ ＵＬ暗号化アクティブ化時刻とＲＢ ＤＬ暗号化アクティブ化時刻との双方を求め、これらのＲＢ ＵＬ暗号化アクティブ化時刻及びＲＢ ＤＬ暗号化アクティブ化時刻がその後ＵＴＲＡＮ５へシグナリングされるということである。図６と図７とを比較することによって分かるように、この結果、ステップが、ステップｓ９’（ＵＴＲＡＮ５は、ＲＢ ＤＬ暗号化アクティブ化時刻を計算しない）、ステップｓ１１’（ＲＲＣ：ＲＡＤＩＯ ＢＥＡＲＥＲ ＳＥＴＵＰメッセージは、ＲＢ ＤＬ暗号化アクティブ化時刻を含まない）、ステップＳ１７’（移動電話３は、ＲＢ ＤＬアクティブ化時刻を計算する）、及びステップｓ２３’（移動電話３は、ＲＲＣ：ＲＡＤＩＯ ＢＥＡＲＥＲ ＳＥＴＵＰ ＣＯＭＰＬＥＴＥメッセージを、新しい開始値及びＲＢ ＵＬ暗号化アクティブ化時刻だけでなく、計算されたＲＢ ＤＬ暗号化アクティブ化時刻をも伴って送信する）に変更される。残りのステップは変更されず、再び説明しない。

【００３６】

当業者が認識するように、この実施形態による１つの利点は、アクティブ化時刻とＲＢ ＤＬ暗号化アクティブ化時刻との間のＤＬ ＲＬＣ ＳＮロールオーバの危険性が（上記で論述した第１の提案と比較して）低減されるということである。この理由は、第１の実施形態では、ＵＴＲＡＮ５が、自身の直接制御外にある新しい開始値を受信する時を推定しなければならなかったからである。したがって、適切なオペレーションを保証するために、ＵＴＲＡＮ５は、新しい開始値を使用して暗号化する準備ができる前に要する時間を過大に見積もらなければならない。これとは対照的に、新しい開始値を求めるのは移動電話３であるので、移動電話３及びＵＴＲＡＮ５が新しい開始値を使用して暗号化を開始できる時をより正確に計算することが可能になる。移動電話３は、したがって、アクティブ化時刻とＲＢ ＤＬ暗号化アクティブ化時刻との間の時間期間をより短く規定することができる。

【００３７】

移動電話３は、暗号化アクティブ化ＲＬＣ－ＳＮを計算するときに、ＲＲＣ：ＲＡＤＩＯ ＢＥＡＲＥＲ ＳＥＴＵＰ ＣＯＭＰＬＥＴＥメッセージをスケジューリングする少なくとも１つの送信時間間隔（ＴＴＩ）に、ラウンドトリップ時間／２（一方向通信リンク時間）を加え、ＵＴＲＡＮがメッセージを処理するのに要する時間間隔を加えた時間を要することを考慮する。ＴＴＩは、ＨＳＰＡの場合に２ミリ秒又は１０ミリ秒のいずれかとなり得る可能性があるので、２ミリ秒のＴＴＩが使用される場合には、ＲＲＣ：ＲＡＤＩＯ ＢＥＡＲＥＲ ＳＥＴＵＰ ＣＯＭＰＬＥＴＥメッセージは、より速くＵＴＲＡＮ５に達することができ、新しい構成もより迅速にアクティブになることができる。

【００３８】

変更形態及び代替形態

詳細な実施形態が上記で説明されてきた。当業者には理解されるように、該実施形態において具現される本発明から依然として利益を享受しながら、上記の実施形態に対する複数の変更形態及び代替形態を実施できる。例示にすぎないが、ここで、いくつかのこれらの代替形態及び変更形態を説明する。

【００３９】
上記実施形態では、暗号化アクティブ化時刻の前に１２８個以上のＲＬＣ ＰＤＵが送信される場合（移動電話３又はＵＴＲＡＮ５のいずれか）、対応するＨＦＮが、ロールオーバを反映するようにインクリメントされる。結局のところ、現在提案されているＵＴＲＡＮ標準規格の場合、１２７個のＲＬＣ ＰＤＵは、約２．５秒に対応する可能性があり、移動電話３及びＵＴＲＡＮは、ロールオーバが起こり得る前に新しい開始値を適切に使用していると予想されるので、この初期期間中にロールオーバが行われる可能性は低い。それにもかかわらず、（ロールオーバの可能性がはるかに高い場合）ＤＣＨによるＣＳ音声との一貫性を維持するために、標準規格は、ＨＦＮがこの初期期間中はインクリメントされないことを規定する場合がある。

【００４０】
上述した第２の実施形態では、移動電話３は、アップリンク及びダウンリンクの双方の暗号化アクティブ化時刻を規定していた。別の実施形態では、ＵＲＴＡＮが、アップリンク及びダウンリンクの双方の暗号化アクティブ化時刻を求め、これらの時刻をＲＲＣ：ＲＡＤＩＯ ＢＥＡＲＥＲ ＳＥＴＵＰメッセージで移動電話へシグナリングするように構成することができる。

【００４１】
上記実施形態では、暗号化は、更新された開始値に基づいて変更されていた。当業者が認識するように、このような開始値が使用も記憶もされないシステムでは、代わりに、ＵＥが供給する他の或るデータを使用して、２つの段階間の暗号化の変更を制御することができる。

【００４２】
上記実施形態では、暗号化アクティブ化時刻は、ＲＬＣ ＳＮによって規定されていた。代替的な一実施形態では、ＣＦＮ番号等による他の或る時間依存パラメータによってアクティブ化時刻を規定することができる。

【００４３】
上記実施形態は、ＨＳＰＡによるＣＳ音声の無線ベアラをセットアップするための技法を説明している。当業者が認識するように、上記技法は、他のタイプのＣＳデータ及びＰＳデータにも同様に使用することができる。

【００４４】
上記２つの実施形態では、ＲＡＢセットアップメッセージは、ＨＳＰＡによりＣＳ音声データを運ぶための新しい無線ベアラをセットアップするのに使用されていた。本発明は、無線ベアラ（複数可）がすでにセットアップされ、再構成が行われていく場合にも適用することができる。例えば、（移動電話は、ＤＣＨサービスのみを提供するセル内に現在存在し、その後、ＨＳＰＡサービスを提供するように構成されたセル内に移動するため）当初の無線ベアラは、初期的には、ＤＣＨによりＣＳトラフィックを運ぶように構成することができる。この場合、上位層は、データを連続的に送信しており、トランスポートチャネルの切り替えは、下位層で行われる。上述した技法は、この遷移期間中の暗号化を引き受けるのに使用することができる。この手順は、トリガがＲＡＢ割り当て要求メッセージだけでなく、セルの変化によっても引き起こされることを除いて、ＵＴＲＡＮ５がＲＲＣ：ＲＡＤＩＯ ＢＥＡＲＥＲ ＳＥＴＵＰメッセージを送信し、移動電話３がＲＲＣ：ＲＡＤＩＯ ＢＥＡＲＥＲ ＳＥＴＵＰ ＣＯＭＰＬＥＴＥメッセージで応答することと同じである。当業者が認識するように、他の再構成の状況を他のトリガイベントによってトリガすることもできる。

【００４５】
上記の実施形態において、移動電話を基にする通信システムが説明された。当業者には理解されるように、本出願において説明される技法は任意の通信システムにおいて利用できる。詳細には、これらの技法の多くは、データを搬送するために電磁信号又は音響信号のいずれかを用いる有線系通信システム又は無線系通信システムにおいて用いることができる。一般的な事例において、ＵＴＲＡＮ及び移動電話は、互いに通信する通信ノード又

はデバイスと見なすことができる。他の通信ノード又はデバイスは、たとえば、携帯情報端末、ラップトップコンピュータ、ウエブブラウザ等のようなユーザデバイスを含み得る。

【００４６】

上記の実施形態では、複数のソフトウエアモジュールが説明された。当業者には理解されるように、それらのソフトウエアモジュールはコンパイルされた形で又はコンパイルされない形で与えられる場合があり、コンピュータネットワークを介した信号として又は記録媒体において、ＵＴＲＡＮ又は移動電話に供給される場合がある。さらに、このソフトウエアの一部又は全てによって実行される機能は、１つ又は複数の専用のハードウエア回路を用いて実行されてもよい。しかしながら、ソフトウエアモジュールを用いることが好ましい。これは、ソフトウエアモジュールが、それらの機能を更新するために、ＵＴＲＡＮ５及び移動電話３を更新することを容易にするためである。

【００４７】

当業者には種々の他の変更形態が明らかになり、ここでは、さらに詳しくは説明しない。

【００４８】

３ＧＰＰ用語の用語集

ＮｏｄｅＢ　ＵＴＲＡＮ基地局
ＣＮ　コアネットワーク
ＵＥ　ユーザ機器　移動通信デバイス
ＤＬ　ダウンリンク　基地局から移動局へのリンク
ＵＬ　アップリンク　移動局から基地局へのリンク
ＵＰＥ　ユーザプレーンエンティティ
ＲＮＳ　無線ネットワークサブシステム
ＲＬＣ　無線リンク制御
ＲＲＣ　無線資源制御
ＰＤＣＰ　パケットデータユニバージェンスプロトコル
Ｃ－ｐｌａｎｅ　制御プレーン
Ｕ－ｐｌａｎｅ　ユーザプレーン
ＨＳＰＡ　高速パケットアクセス
ＣＦＮ　接続フレーム番号
ＣＳ　回路交換
ＰＳ　パケット交換
ＳＮ　シーケンス番号
ＤＣＨ　専用チャネル
ＰＤＵ　プロトコルデータユニット
ＴＴＩ　送信時間間隔
ＲＡＢ　無線アクセスベアラ
ＵＳＩＭ　汎用加入者識別モジュール
ＩＥ　情報要素
ＨＦＮ　ハイパーフレーム番号

【００４９】

以下において、現在提案されている３ＧＰＰ　ＵＴＲＡＮ標準規格において本発明を実施することができる方法を詳細に説明する。種々の特徴が不可欠であるか又は必要であるように説明される場合があるが、これは、たとえばその標準規格によって課せられる他の要件に起因して、提案されている３ＧＰＰ　ＬＴＥ標準規格の場合にのみ当てはまり得る。それゆえ、これらの記載は、いかなる形においても本発明を制限するものと解釈されるべきではない。

【００５０】

ＨＳＰＡによるＣＳ音声のための２段階暗号化

ＨＳＰＡによるＣＳ音声は、ＲＬＣ－ＵＭ無線ベアラを使用し、ＲＬＣ－ＵＭ無線ベアラのための暗号化は、現在、ＲＬＣ層内で実行される。アップリンクのための暗号化は、アクティブ化時刻に開始され、ダウンリンクのための暗号化は、ＵＴＲＡＮがＲＲＣ完了メッセージをＵＥから受信した後に開始される。したがって、アクティブ化時刻とＲＲＣ再構成応答メッセージの受信との間にＵＴＲＡＮにおいて受信されるいかなるデータも、適切に解読することができない。本発明者は、この問題を解決する以下の３つの提案を提案する。これは、ＤＣＨからＨＳＰＡへのＨＳＰＡによるＣＳ音声のセットアップ及び再構成に適用される。

【００５１】

提案される変更

本発明の背後にある動機：

ユーザデータを暗号化する必要がある場合、ユーザデータを転送するＲＬＣ－ＵＭを使用した無線ベアラの暗号化は、ＲＬＣ副層において実行される。暗号化に使用される暗号化アルゴリズムは、いくつかの入力パラメータを必要とする。入力パラメータのうちの１つは、ＣＯＵＮＴ－Ｃ（カウントＣ）値である。このＣＯＵＮＴ－Ｃ値は、暗号化シーケンス番号であり、３２ビット長である。

【００５２】

ＣＯＵＮＴ－Ｃ値は、無線ベアラの確立時にＳＴＡＲＴ（開始）値で初期化される。ＳＴＡＲＴ値は、ＵＥによって計算され、無線ベアラ確立手順中にＵＥからＵＴＲＡＮへ通知される。

【００５３】

送信される最初のＲＬＣ ＰＤＵからの暗号化及び受信された最初のＲＬＣ ＰＤＵからの解読を行うには、無線ベアラは、無線ベアラ確立手順中に計算されたＳＴＡＲＴ値によって初期化されたＣＯＵＮＴ－Ｃ値の使用を開始する必要がある。

【００５４】

暗号化構成を有するこの既存の無線ベアラ確立手順は、以下の問題を有する。

【００５５】

ＵＥ及びＵＴＲＡＮは、無線ベアラを確立し、アクティブ化時刻における対応する資源及びエンティティを割り当てて構成する。このアクティブ化時刻は、ＲＲＣ：ＲＡＤＩＯ ＢＥＡＲＥＲ ＳＥＴＵＰメッセージによってＵＴＲＡＮからＵＥへ送信され、ＵＥ及びＵＴＲＡＮが、ＲＲＣメッセージによって与えられた新しい構成の使用を開始する時を示す。この時点で、無線ベアラは、一時停止もされなければ停止もされない。したがって、無線ベアラは、ユーザデータを転送することができる。しかしながら、暗号化構成については、ＵＥ及びＵＴＲＡＮは、同じＳＴＡＲＴ値を使用する必要があり、このＳＴＡＲＴ値は、ＲＲＣ：ＲＡＤＩＯ ＢＥＡＲＥＲ ＳＥＴＵＰ ＣＯＭＰＬＥＴＥメッセージを使用することによってＵＥからＵＴＲＡＮへ送信され、ＲＲＣメッセージが、アクティブ化時刻後に送信される。これは、ＵＥ及びＵＴＲＡＮが、アクティブ化時刻及びＲＲＣ：ＲＡＤＩＯ ＢＥＡＲＥＲ ＳＥＴＵＰ ＣＯＭＰＬＥＴＥメッセージのＵＴＲＡＮにおける受信から有効な暗号化も有効な解読も実行できない時間ギャップがあることを意味する。

【００５６】

この現在のメカニズムの仕様を定めた３ＧＰＰ仕様は、その時間期間中にユーザデータを転送することを禁止している。

【００５７】

本発明は、２段階暗号化を導入して、ＵＥ及びＵＴＲＡＮが有効な暗号化によりユーザデータの転送を開始できるようにする。

【００５８】

［提案１］

１． ＵＴＲＡＮは、ＲＢ ＤＬアクティブ化時刻情報ＩＥを有するＲＲＣ再構成メッセージにおいて新しい再構成を提供する。ＲＢ ＤＬアクティブ化時刻情報ＩＥは、ＵＴＲＡＮが暗号化のための新しいＳＴＡＲＴ値を使用する時を示すＲＬＣ ＵＭ ＳＮを含む

。新しいＩＥ「ＲＢ ＤＬアクティブ化時刻情報」は、ＲＲＣ再構成メッセージにおいて提案されることに留意されたい。
２． ＵＥは、ＲＲＣ再構成メッセージを受信する。
２．１ ＵＥは、新しいＳＴＡＲＴ値を計算し、ＵＥが新しいＳＴＡＲＴ値の使用を開始する時を決定する（すなわち、ＲＢ ＵＬアクティブ化時刻を規定する）。ＵＥは、新しいＳＴＡＲＴ値及びＲＢ ＵＬアクティブ化時刻をＲＲＣ再構成完了メッセージに含める。
２．２ ＵＥは、アクティブ化時刻（暗号化アクティブ化時刻ではない）において、所与の新しい構成の使用を開始し、古いＳＴＡＲＴ値を使用することによる暗号化及び解読を開始する。この時点で、ＵＴＲＡＮも、アクティブ化時刻において、新しい構成の使用を開始し、古いＳＴＡＲＴ値を使用することによる暗号化及び解読を開始する。（注１）
２．３ ＵＥは、ＲＲＣ再構成完了メッセージをＵＴＲＡＮへ送信する。
３． ＵＴＲＡＮは、ＲＲＣ再構成完了メッセージを受信する。ＵＴＲＡＮは、新しいＳＴＡＲＴ値及びＲＢ ＵＬアクティブ化時刻を得る。ＵＥは、ＤＬ ＲＬＣ ＳＮが、ＲＲＣ再構成メッセージによって与えられたＲＢ ＤＬアクティブ化時刻に達すると、新しいＳＴＡＲＴ値を使用することによる解読を開始し、ＵＬ ＲＬＣ ＳＮがＲＲＣ再構成完了メッセージにおいて送信されたＲＢ ＵＬアクティブ化時刻に達すると、新しいＳＴＡＲＴ値を使用することによる暗号化を開始する。ＵＴＲＡＮについても同様である。
長所：
１． 暗号化は、アクティブ化時刻及びＲＲＣ再構成メッセージが受信される時間の間アクティブである。
短所：
１． ＲＬＣ－ＳＮカウンタは、トラフィックに基づいてインクリメントされる。したがって、ＵＬ ＲＬＣ－ＳＮ及びＤＬ ＲＬＣ－ＳＮを決定する前に、対応するエンティティは、理想的には、コーデックレート、チャネル状態等をできるだけ正確に推定しなければならない。これは、可変のＲＣＬ－ＰＤＵサイズ及びセグメンテーションのＭＡＣ層内部への導入によってより複雑になる。
２． ＲＬＣ－ＳＮは７ビット長であり、ロールオーバは、コーデックレートに応じて、頻繁に行われる可能性がある。ＲＲＣ：ＲＡＤＩＯ ＢＥＡＲＥＲ ＳＥＴＵＰメッセージの送信と、ＤＬ ＲＬＣ－ＳＮによって示される暗号化の開始との間の時間差が、ＲＬＣ－ＳＮロールオーバの２つ以上のサイクルを含む場合、ロールオーバの回数を示す追加のＩＥが必要とされる。
３． ＡＳＮ．１を変更する必要がある。
【００５９】
［提案２］
１． ＵＴＲＡＮは、アクティブ化時刻情報ＩＥを有するＲＲＣ再構成メッセージにおいて新しい構成を提供する。新しいＩＥは必要とされないことに留意されたい。
２． ＵＥは、ＲＲＣ再構成メッセージを受信する。
２．１ ＵＥは、新しいＳＴＡＲＴ値を計算し、ＵＥが新しいＳＴＡＲＴ値の使用を開始する時を決定する（すなわち、ＲＢ ＵＬアクティブ化時刻及びＲＢ ＤＬアクティブ化時刻を規定する）。ＵＥは、新しいＳＴＡＲＴ値、ＲＢ ＵＬアクティブ化時刻、及びＲＢ ＤＬアクティブ化時刻をＲＲＣ再構成完了メッセージに含める。
２．２ ＵＥは、アクティブ化時刻（暗号化アクティブ化時刻ではない）において、所与の新しい構成の使用を開始し、古いＳＴＡＲＴ値を使用することによる暗号化及び解読を開始する。この時点で、ＵＴＲＡＮも、アクティブ化時刻において、新しい構成の使用を開始し、古いＳＴＡＲＴ値を使用することによる暗号化及び解読を開始する。（注１）
２．３ ＵＥは、ＲＲＣ再構成完了メッセージをＵＴＲＡＮへ送信する。
３． ＵＴＲＡＮは、ＲＲＣ再構成完了メッセージを受信する。ＵＴＲＡＮは、新しいＳＴＡＲＴ値、ＲＢ ＵＬアクティブ化時刻、及びＲＢ ＤＬアクティブ化時刻を得る。ＵＥは、ＤＬ ＲＬＣ ＳＮがＲＢ ＤＬアクティブ化時刻に達すると、新しいＳＴＡＲＴ値

を使用することによる解読を開始し、ＵＬ ＲＬＣ ＳＮがＲＲＣ再構成完了メッセージにおいて送信されたＲＢ ＵＬアクティブ化時刻に達すると、新しいＳＴＡＲＴ値を使用することによる暗号化を開始する。

４． ＵＴＲＡＮは、ＵＬ ＲＬＣ ＳＮがＲＢ ＵＬアクティブ化時刻に達すると、新しいＳＴＡＲＴ値を使用した解読を開始し、ＤＬ ＲＬＣ－ＳＮがＲＢ ＤＬアクティブ化時刻に達すると解読を開始する。

長所：

１． ＤＬ ＲＬＣ－ＳＮのロールオーバが２回以上になる危険性が低減される。

しかしながら、これが実際のネットワークではどれくらい速く起こる可能性があるのかはあまり明らかではない。理論的には、ＡＭＲフレームタイミングは２０ミリ秒であり、１つのＲＣＬ ＰＤＵが１つのＰＤＣＰ ＰＤＵにマッピングされる場合、ＲＬＣ－ＳＮロールオーバの最大時間は２０ミリ秒×１２７＝２．５秒である。

２． ２ミリ秒のＴＴＩが使用される場合、ＲＲＣ：ＲＢセットアップ完了をより速く送信することができ、新しい構成をより迅速にアクティブにすることができる。

短所：

１． 暗号化アクティブ化時刻とアクティブ化時刻との間の関係がない。２つの構成は、異なる時刻にアクティブになる。

２． ＵＥは、新しい構成がアクティブとなる正確な時刻を計算しなければならない。すなわち、それほど長くもなく且つ短か過ぎない値を計算しなければならない。

３． ＡＳＮ．１を変更する必要がある。

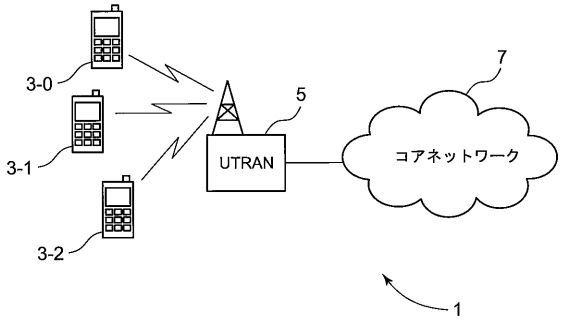
【００６０】

注１：暗号化は、この段階では、ＨＦＮ値をインクリメントすることによって開始することができる。ＤＣＨによるＣＳ音声中、ＣＦＮロールオーバが起こる可能性があり、これは、ＵＥに保持されたカウントｃ値とＵＴＲＡＮに保持されたカウントｃ値との間の不一致につながる可能性があるので、ＨＦＮ値は、この段階ではインクリメントされなかった。この可能性を回避するために、ＨＦＮは、ＤＣＨによるＣＳ音声の場合にはインクリメントされなかった。しかしながら、ＨＳＰＡによるＣＳ音声の場合には、ＲＬＣ－ＳＮは、常に０から開始し、ロールオーバは、１２７個のＲＬＣ－ＰＤＵが受信された後に起こる可能性があり、ＵＥとＵＴＲＡＮとの間のＨＦＮ値の不一致の可能性は存在しない。しかし、ＤＣＨによるＣＳ音声との一貫性を提供するために、３ＧＰＰは、ＨＦＮをインクリメントすることのない暗号化を選択することができる。したがって、本発明では、ＨＦＮをインクリメントする場合及びＨＦＮをインクリメントしない場合の双方が含まれることを含めたい。

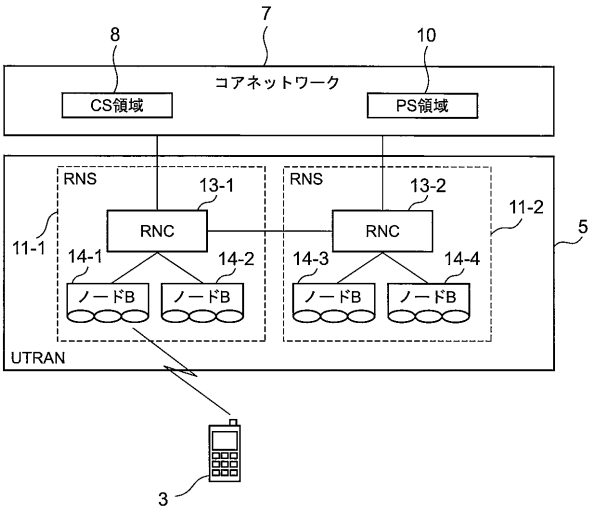
【００６１】

本出願は、２００８年１月３１日に出願の英国特許出願第０８０１８２５．１号に基づいており、その特許出願からの優先権の利益を主張し、その特許出願の開示は参照によりその全体が本明細書に援用される。

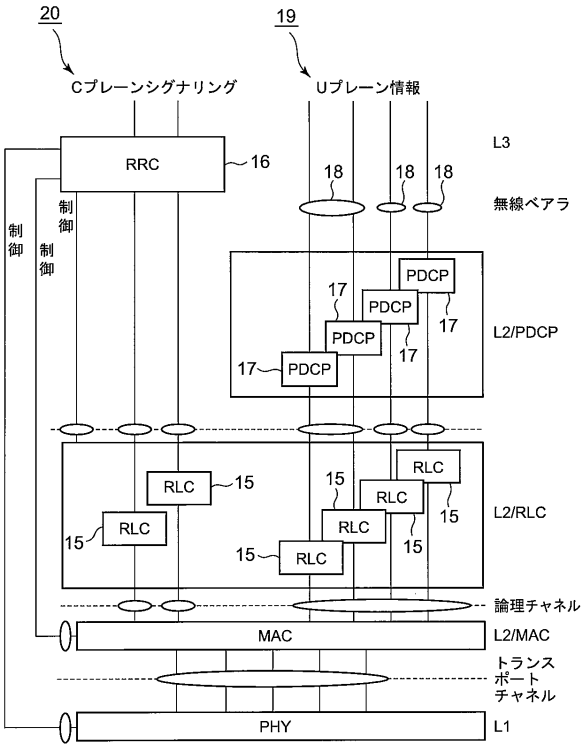
【図１】


3-0
3-1
3-2
5
UTRAN
7
コアネットワーク
1

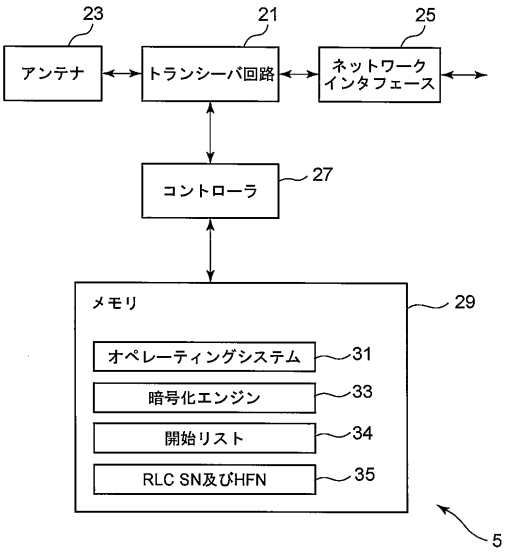
【図２】


7
8
10
コアネットワーク
CS領域
PS領域
RNS
13-1
RNC
11-1
14-1
14-2
ノードB
ノードB
RNS
13-2
RNC
11-2
5
14-3
14-4
ノードB
ノードB
UTRAN
3

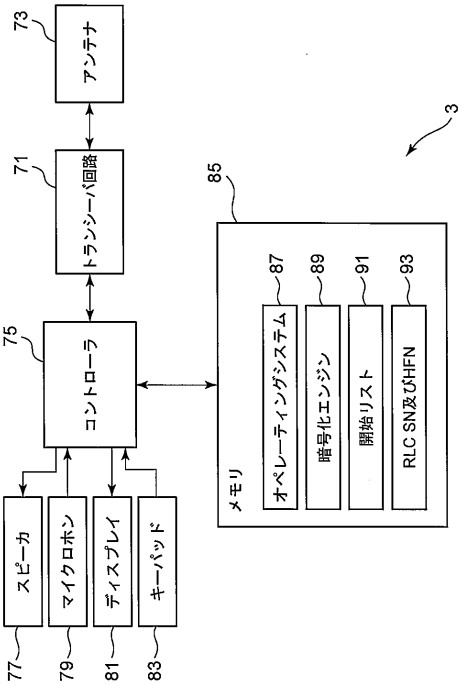
【図３】


20
19
Cプレーンシグナリング
Uプレーン情報
L3
RRC
16
18
18
18
無線ベアラ
制御
制御
制御
PDCP
17
PDCP
17
PDCP
17
17
PDCP
L2/PDCP
RLC
15
RLC
15
15
RLC
RLC
15
15
RLC
15
L2/RLC
論理チャネル
MAC
L2/MAC
トランスポートチャネル
PHY
L1

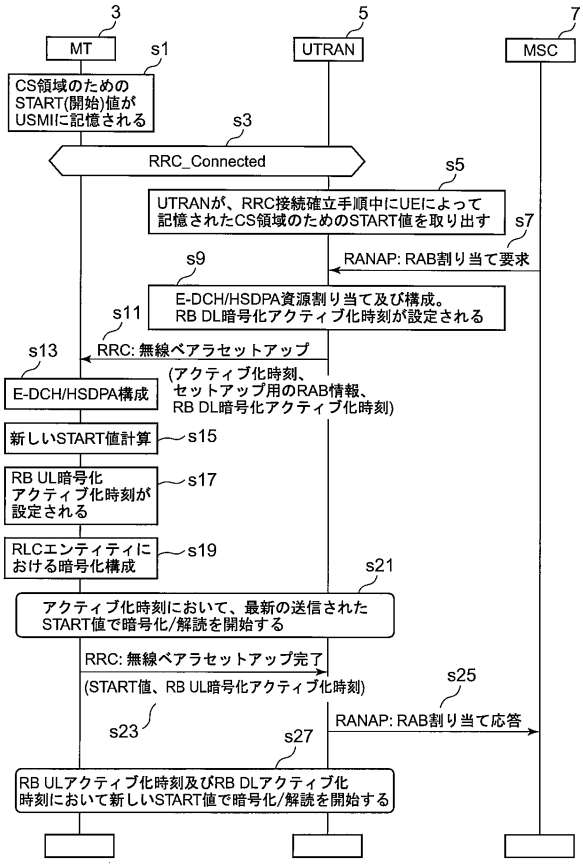
【図４】


23
21
25
アンテナ
トランシーバ回路
ネットワークインタフェース
コントローラ
27
メモリ
29
オペレーティングシステム
31
暗号化エンジン
33
開始リスト
34
RLC SN及びHFN
35
5

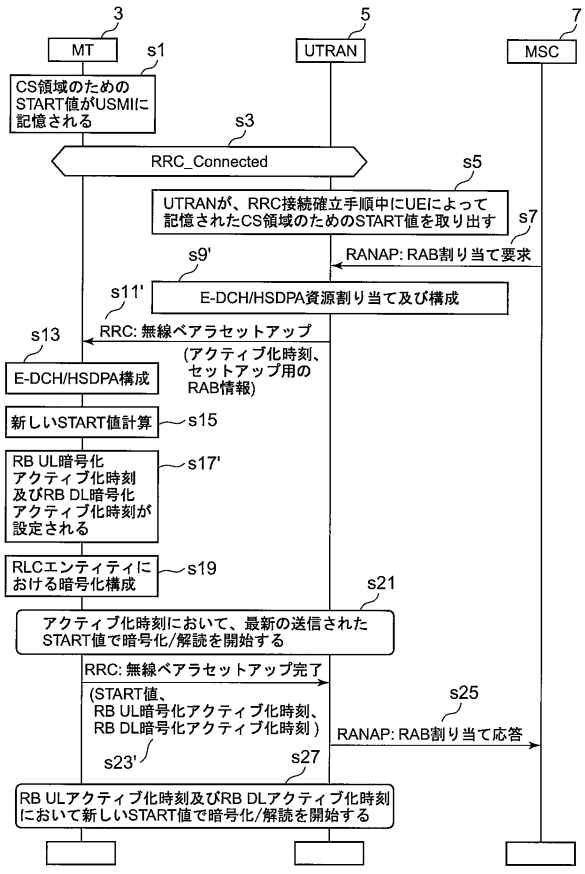
【図５】


73
アンテナ
71
トランシーバ回路
3
85
87
89
91
93
オペレーティングシステム
暗号化エンジン
開始リスト
RLC SN及びHFN
メモリ
75
コントローラ
スピーカ
マイクロホン
ディスプレイ
キーパッド
77
79
81
83

【図６】


3
MT
5
UTRAN
7
MSC
s1
CS領域のための
START(開始)値が
USMIIに記憶される
s3
RRC_Connected
s5
UTRANが、RRC接続確立手順中にUEによって
記憶されたCS領域のためのSTART値を取り出す
s7
RANAP: RAB割り当て要求
s9
E-DCH/HSDPA資源割り当て及び構成。
RB DL暗号化アクティブ化時刻が設定される
s11
RRC: 無線ベアラセットアップ
s13
E-DCH/HSDPA構成
(アクティブ化時刻、
セットアップ用のRAB情報、
RB DL暗号化アクティブ化時刻)
新しいSTART値計算
s15
RB UL暗号化
アクティブ化時刻が
設定される
s17
RLCエンティティに
おける暗号化構成
s19
s21
アクティブ化時刻において、最新の送信された
START値で暗号化/解読を開始する
RRC: 無線ベアラセットアップ完了
(START値、RB UL暗号化アクティブ化時刻)
s25
RANAP: RAB割り当て応答
s23
s27
RB ULアクティブ化時刻及びRB DLアクティブ化
時刻において新しいSTART値で暗号化/解読を開始する

【図７】


3
MT
5
UTRAN
7
MSC
s1
CS領域のための
START値がUSMIIに
記憶される
s3
RRC_Connected
s5
UTRANが、RRC接続確立手順中にUEによって
記憶されたCS領域のためのSTART値を取り出す
s7
RANAP: RAB割り当て要求
s9'
s11'
E-DCH/HSDPA資源割り当て及び構成
s13
RRC: 無線ベアラセットアップ
(アクティブ化時刻、
セットアップ用の
RAB情報)
E-DCH/HSDPA構成
新しいSTART値計算
s15
RB UL暗号化
アクティブ化時刻
及びRB DL暗号化
アクティブ化時刻が
設定される
s17'
RLCエンティティに
おける暗号化構成
s19
s21
アクティブ化時刻において、最新の送信された
START値で暗号化/解読を開始する
RRC: 無線ベアラセットアップ完了
(START値、
RB UL暗号化アクティブ化時刻、
RB DL暗号化アクティブ化時刻)
s25
RANAP: RAB割り当て応答
s23'
s27
RB ULアクティブ化時刻及びRB DLアクティブ化時刻
において新しいSTART値で暗号化/解読を開始する

フロントページの続き

(72)発明者　林　貞福
東京都港区芝五丁目７番１号　日本電気株式会社内

Ｆターム(参考) 5K067 AA35　DD17　HH36