(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6903006号
(P6903006)
(45)発行日　令和3年7月14日(2021.7.14)　(24)登録日　令和3年6月24日(2021.6.24)

(51)Int.Cl.　　F I
H04W 12/04 (2021.01)　H04W 12/04
H04L 9/08 (2006.01)　H04L 9/00　601C
H04L 9/14 (2006.01)　H04L 9/00　601E
H04W 88/16 (2009.01)　H04L 9/00　641
H04W 88/16

請求項の数 15　(全 58 頁)

(21)出願番号　特願2017-522621(P2017-522621)
(86)(22)出願日　平成27年10月27日(2015.10.27)
(65)公表番号　特表2017-534204(P2017-534204A)
(43)公表日　平成29年11月16日(2017.11.16)
(86)国際出願番号　PCT/US2015/057640
(87)国際公開番号　WO2016/069638
(87)国際公開日　平成28年5月6日(2016.5.6)
審査請求日　平成30年10月9日(2018.10.9)
審判番号　不服2020-6920(P2020-6920/J1)
審判請求日　令和2年5月21日(2020.5.21)
(31)優先権主張番号　62/072,388
(32)優先日　平成26年10月29日(2014.10.29)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　507364838
クアルコム，インコーポレイテッド
アメリカ合衆国　カリフォルニア　９２１２１　サン　ディエゴ　モアハウス　ドライブ　５７７５
(74)代理人　100108453
弁理士　村山　靖彦
(74)代理人　100163522
弁理士　黒田　晋平
(72)発明者　ソ・ブム・イ
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５

最終頁に続く

(54)【発明の名称】次世代セルラーネットワークのためのユーザプレーンセキュリティ

(57)【特許請求の範囲】
【請求項１】
デバイスにおいて動作可能な方法であって、
前記デバイスおよびコアネットワークエンティティによって共有される第1の共有鍵を前記デバイスにおいて取得するステップと、
前記デバイスとパケットデータネットワークゲートウェイ(P-GW)との間で通過中のデータトラフィックをセキュアにするために、前記第1の共有鍵に基づいて、前記デバイスおよび前記P-GWによって共有される第2の共有鍵を前記デバイスにおいて取得するステップと、
第1のセキュアにされたデータトラフィックを作成するために、前記第2の共有鍵に基づいてデータトラフィックをセキュアにするステップと、
前記第1のセキュアにされたデータトラフィックをアクセスノードを介して前記P-GWに送信するステップとを含み、前記コアネットワークエンティティ、前記P-GWおよび前記アクセスノードが別個のネットワークエンティティであり、前記第1の共有鍵が、前記アクセスノードに知られておらず、
前記デバイスとモビリティ管理エンティティ(MME)との間で送信される制御メッセージングをセキュアにするために、前記第1の共有鍵に基づいて第3の共有鍵を前記デバイスにおいて取得するステップをさらに含み、前記第3の共有鍵が前記デバイスおよび前記MMEによって共有され、前記P-GW、前記MMEおよび前記アクセスノードが別個のネットワークエンティティである、

方法。
【請求項２】
前記第1の共有鍵が、前記P-GWに知られていない、または、
前記第1の共有鍵および前記第2の共有鍵が前記デバイスにおいてローカルに導出され、前記デバイスに送信されない、または、
前記第2の共有鍵が、前記デバイスと、前記P-GWとの間のユーザプレーン通信のインターネットプロトコル(IP)層をセキュアにする一方で、異なる鍵が、前記デバイスと、前記MMEとの間の制御プレーン通信をセキュアにする、請求項1に記載の方法。
【請求項３】
前記デバイスと前記アクセスノードとの間のデータトラフィックおよび前記デバイスと前記MMEとの間の制御メッセージングをセキュアにするために、前記第3の共有鍵に基づいて、前記デバイスおよび前記アクセスノードによって共有される第4の共有鍵を前記デバイスにおいて取得するステップと、
第2のセキュアにされたデータトラフィックを作成するために、前記第4の共有鍵に基づいて、前記第1のセキュアにされたデータトラフィックをセキュアにするステップであって、前記第1のセキュアにされたデータトラフィックが、前記第2のセキュアにされたデータトラフィックの中にカプセル化される、セキュアにするステップと、
前記第1のセキュアにされたデータトラフィックの代わりに前記第2のセキュアにされたデータトラフィックを前記アクセスノードを介して前記P-GWに送信するステップとをさらに含み、前記P-GW、前記MMEおよび前記アクセスノードが別個のネットワークエンティティである、請求項1に記載の方法。
【請求項４】
前記第4の共有鍵が、ユーザプレーンのパケットデータ収束プロトコル(PDCP)層内の前記第2のセキュアにされたデータトラフィックを保護する、または、
前記第4の共有鍵が、ユーザプレーンのいくつかの層上のトラフィックのいくつかの送信を保護する一方で、前記第2の共有鍵が、前記ユーザプレーンの他の層上のトラフィックの他の送信を保護するために使用される、請求項3に記載の方法。
【請求項５】
前記コアネットワークエンティティが、前記第1の共有鍵をホーム加入者サーバ(HSS)から取得する、または、
前記デバイスが前記P-GWとは独立に前記第2の共有鍵を取得する、または、
前記第2の共有鍵を取得するステップが、
前記第2の共有鍵を、前記第1の共有鍵およびパケットデータネットワークゲートウェイ識別子(GW ID)の関数として前記デバイスにおいて導出するステップをさらに含む、請求項1に記載の方法。
【請求項６】
データトラフィックが制御メッセージングとは異なる、または、
データトラフィックがユーザプレーン上で送信され、制御メッセージングが制御プレーン上で送信され、前記ユーザプレーンおよび前記制御プレーンが別個の送信経路である、または、
前記データトラフィックをセキュアにするステップが、前記第2の共有鍵に基づいて前記データトラフィックを暗号化するステップを含む、または、
前記データトラフィックをセキュアにするステップが、前記第2の共有鍵に基づく認証署名を含めるステップを含む、請求項1に記載の方法。
【請求項７】
第3のセキュアにされたデータトラフィックを前記アクセスノードを介して前記P-GWから受信するステップであって、前記第3のセキュアにされたデータトラフィックが前記第2の共有鍵に基づいてセキュアにされている、受信するステップと、
セキュアでないデータトラフィックを作成するために、前記第2の共有鍵に基づいて、前記第3のセキュアにされたデータトラフィックを解読および/または認証するステップと

をさらに含む、請求項1に記載の方法。
【請求項８】
デバイスであって、
前記デバイスおよびコアネットワークエンティティによって共有される第1の共有鍵を取得するための手段と、
前記デバイスとパケットデータネットワークゲートウェイ(P-GW)との間で通過中のユーザプレーンデータトラフィックをセキュアにするために、前記第1の共有鍵に基づいて、前記デバイスおよび前記P-GWによって共有される第2の共有鍵を取得するための手段と、
第1のセキュアにされたデータトラフィックを作成するために、前記第2の共有鍵に基づいてデータトラフィックをセキュアにするための手段と、
前記第1のセキュアにされたデータトラフィックをアクセスノードを介して前記P-GWに送信するための手段とを含み、前記コアネットワークエンティティ、前記P-GWおよび前記アクセスノードが別個のネットワークエンティティであり、前記第1の共有鍵が、前記アクセスノードに知られておらず、
前記デバイスとモビリティ管理エンティティ(MME)との間で送信される制御メッセージングをセキュアにするために、前記第1の共有鍵に基づいて第3の共有鍵を取得するための手段をさらに含み、前記第3の共有鍵が前記デバイスおよび前記MMEによって共有され、前記P-GW、前記MMEおよび前記アクセスノードが別個のネットワークエンティティである、
デバイス。
【請求項９】
前記デバイスと前記アクセスノードとの間のデータトラフィックおよび前記デバイスと前記MMEとの間の制御メッセージングをセキュアにするために、前記第3の共有鍵に基づいて、前記デバイスおよび前記アクセスノードによって共有される第4の共有鍵を取得するための手段と、
第2のセキュアにされたデータトラフィックを作成するために、前記第4の共有鍵に基づいて前記第1のセキュアにされたデータトラフィックをセキュアにするための手段であって、前記第1のセキュアにされたデータトラフィックが、前記第2のセキュアにされたデータトラフィックの中にカプセル化される、セキュアにするための手段と、
前記第1のセキュアにされたデータトラフィックの代わりに前記第2のセキュアにされたデータトラフィックを前記アクセスノードを介して前記P-GWに送信するための手段とをさらに含み、前記P-GW、前記MMEおよび前記アクセスノードが別個のネットワークエンティティである、請求項8に記載のデバイス。
【請求項１０】
1つまたは複数の命令が記憶された非一時的機械可読記憶媒体であって、前記1つまたは複数の命令が、少なくとも1つのプロセッサによって実行されたときに、前記少なくとも1つのプロセッサに、請求項1または3に記載の方法を行わせる、非一時的機械可読記憶媒体。
【請求項１１】
パケットデータネットワークゲートウェイ(P-GW)において動作可能な方法であって、
データトラフィックをパケットデータネットワークから前記P-GWにおいて受信するステップと、
前記P-GWとデバイスとの間で通過中の前記データトラフィックをセキュアにするために、前記P-GWおよび前記デバイスによって共有される秘密の共有鍵をネットワークエンティティから前記P-GWにおいて取得するステップと、
セキュアにされたデータトラフィックを作成するために、前記秘密の共有鍵に基づいて前記データトラフィックをセキュアにするステップと、
前記セキュアにされたデータトラフィックをアクセスノードを介して前記デバイスに送信するステップとを含み、前記P-GW、前記アクセスノードおよび前記ネットワークエンティティが別個のネットワークエンティティであり、前記秘密の共有鍵が、前記アクセスノードに知られておらず、

前記秘密の共有鍵を取得するステップが、
ホーム加入者サーバ(HSS)とモビリティ管理エンティティ(MME)との間に位置する前記ネットワークエンティティから前記秘密の共有鍵を取得するステップをさらに含み、
前記秘密の共有鍵によってセキュアにされた、セキュアにされたアップリンクデータトラフィックを、前記アクセスノードを介して前記デバイスから前記P-GWにおいて受信するステップと、
アップリンクデータトラフィックを取得するために、前記秘密の共有鍵を用いて、前記セキュアにされたアップリンクデータトラフィックを解読および/または認証するステップと、
前記アップリンクデータトラフィックを前記パケットデータネットワークに送信するステップと、を含む
方法。

【請求項１２】
前記秘密の共有鍵が、前記ネットワークエンティティから、制御プレーンインターフェース上で前記P-GWに提供される、または、
前記秘密の共有鍵が、ユーザプレーンのインターネットプロトコル(IP)層内の前記データトラフィックを保護する、または、
前記P-GWが前記デバイスとは独立に前記秘密の共有鍵を取得する、または、
前記秘密の共有鍵が、P-GW識別子(GW ID)の関数である、または、
前記秘密の共有鍵が、前記P-GWと同じドメイン内の前記ネットワークエンティティから取得される、請求項11に記載の方法。

【請求項１３】
パケットデータネットワークゲートウェイ(P-GW)であって、
パケットデータネットワークおよびセルラーネットワークと通信するように構成されたネットワーク通信回路と、
前記ネットワーク通信回路に結合された処理回路とを備え、前記処理回路が、
データトラフィックを前記パケットデータネットワークから前記P-GWにおいて受信することと、
前記P-GWとデバイスとの間で通過中の前記データトラフィックをセキュアにするために、前記P-GWおよび前記デバイスによって共有される秘密の共有鍵を、ホーム加入者サーバ(HSS)とモビリティ管理エンティティ(MME)との間に位置するネットワークエンティティから前記P-GWにおいて取得することと、
セキュアにされたデータトラフィックを作成するために、前記秘密の共有鍵に基づいて前記データトラフィックをセキュアにすることと、
前記セキュアにされたデータトラフィックをアクセスノードを介して前記デバイスに送信することとを行うように構成され、前記P-GW、前記アクセスノードおよび前記ネットワークエンティティが別個のネットワークエンティティであり、前記秘密の共有鍵が、前記アクセスノードに知られておらず、
前記P-GWおよび前記ネットワークエンティティが1つのドメイン内にあり、
前記処理回路が、
セキュアにされたアップリンクデータトラフィックを前記アクセスノードを介して前記デバイスから受信することであって、前記セキュアにされたアップリンクデータトラフィックが前記秘密の共有鍵を用いてセキュアにされる、受信することと、
アップリンクデータトラフィックを取得するために、前記秘密の共有鍵を用いて前記セキュアにされたアップリンクデータトラフィックを解読および/または認証することと、
前記アップリンクデータトラフィックを前記パケットデータネットワークに送信することとを行うようにさらに構成される、パケットデータネットワークゲートウェイ(P-GW)。

【請求項１４】
請求項1から7のうちのいずれか一項に記載の方法を行わせるための命令を含む、コンピュータプログラム。

【請求項１５】
請求項11または12に記載の方法を行わせるための命令を含む、コンピュータプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本出願は、その内容全体が参照により本明細書に組み込まれる、2014年10月29日に米国特許庁に出願された米国仮出願第62/072,388号および2015年10月26日に米国特許庁に出願された米国非仮出願第14/923,223号の優先権および利益を主張する。
【０００２】
本開示は、全般に通信システムに関し、より詳細には、ワイヤレス通信システムにおけるユーザプレーンメッセージングを保護するためのシステムに関する。
【背景技術】
【０００３】
図1は、従来技術による第4世代(4G)セルラーネットワーク100の要素の図である。4Gセルラーネットワーク100は、本明細書では発展型ユニバーサル地上波無線アクセスネットワーク(E-UTRAN)102と呼ばれることがあるアクセス部分(たとえば、無線アクセスネットワーク(RAN))と、本明細書では発展型パケットコア(EPC)104と呼ばれることがあるコア部分(たとえば、コアネットワーク)とを含んでよい。E-UTRAN102およびEPC104はともに、発展型パケットシステム(EPS)を形成する。
【０００４】
EPSは、クライアントデバイス106(たとえば、モバイルデバイス、モバイル端末、ユーザ機器(UE)、端末)と通信してよい。クライアントデバイス106は、ユニバーサル加入者識別モジュール(USIM)108(通常、SIMカードと呼ばれる)を含んでよい。USIM108は、たとえば、国際移動体加入者識別(IMSI)番号およびそれに関連する鍵、Kをセキュアに記憶する集積回路チップであってよい。鍵、Kはルート鍵であってよい。
【０００５】
EPSにおける通信は、プレーンに、すなわちユーザプレーン(UP)と制御プレーン(CP)とに分割される。図1では、1つの特定の制御プレーンシグナリング経路が、アクセスノード112(たとえば、eノードB)とモビリティ管理エンティティ(MME)114との間の破線110によって識別される一方で、1つの特定のユーザプレーンデータトラフィック経路が、アクセスノード112とサービングゲートウェイ(S-GW)118との間の実線116によって識別される。当業者は、制御プレーンシグナリングおよびユーザプレーンデータトラフィックに対する追加のおよび代替の経路を認識している。図1の図は例であり、限定を意味するものではない。
【０００６】
E-UTRAN102は、クライアントデバイス106とワイヤレスに通信するハードウェアを含むアクセスノード112を含む。ロングタームエボリューション(LTE)ネットワークでは、アクセスノード112は、発展型ノードB(eノードB)と呼ばれることがある。例として、単一のLTEアクセスノードは、1つまたは複数のE-UTRAN102セルの働きをすることがある。
【０００７】
EPC104は、パケットデータネットワーク(PDN)ゲートウェイ(P-GW)120を含む。P-GW120は、インターネットおよび/または民間企業ネットワークなど、パケットデータネットワーク122へのゲートウェイとしての働きをする。P-GW120は、パケットデータネットワーク122への通路と見なされてよく、P-GW120は、ネットワークポリシー実施点である。アクセスノード112は、コアネットワーク(たとえば、EPC104)への、クライアントデバイス106のオーバージエアアクセスのための通路と見なされてよい。アクセスノード112は、P-GW120とコロケートされてよいが、アクセスノード112の機能は、P-GW120の機能とは異なる。言い換えれば、アクセスノード112およびP-GW120は、それらがコロケートされる場合でも、別個の機能を有する別個のエンティティである。

【０００８】
EPC104は、ホーム加入者サーバ(HSS)124をさらに含む。HSS124は、各クライアントデバイス106の一意の識別情報を記憶する。認証センター(AuC)126は、HSS124に結合されてよい。AuC126は、クライアントデバイス106がEPC104への接続を試みるとき、USIM108を認証する働きをすることがある。AuC126は、USIM108に記憶された鍵と同じ鍵(たとえば、ルート鍵K)を記憶してよい。言い換えれば、AuC126は、USIM108に記憶されたルート鍵Kの第2のインスタンスを記憶してよい。ルート鍵は、オーバージエアで送信されない。AuC126によるUSIM108の認証は、一般に、クライアントデバイス106が電源投入されるときに発生してよい。
【０００９】
EPC104はまた、S-GW118を含む。S-GW118は、クライアントデバイス106へのおよびそこからのユーザプレーンIPメッセージの移送に関連する機能を実行する。メッセージは1つまたは複数のパケットを含んでよいことが、全般的に理解される。パケットおよびメッセージは異なるフォーマットを有してよく、異なるヘッダによってカプセル化されてよい。本明細書における参照を容易にするために、用語メッセージが、全体にわたって使用される。
【００１０】
EPC104はまた、MME114を含む。MME114は、様々な物理チャネルをセットアップ、維持、および解放することに関連する機能を実行する。MME114は、メッセージ通信に対するベアラを準備することがある。MME114は制御プレーンに関連する一方で、クライアントデバイス106、アクセスノード112、S-GW118、P-GW120、およびHSS124は制御プレーンとユーザプレーンの両方に関連する。
【００１１】
クライアントデバイス106がネットワーク(たとえば、EPC104)と通信するとき、クライアントデバイス106は、アタッチ手順の間にMME114によって割り振られる一時的移動体加入者識別情報(TMSI)を使用して識別される。クライアントデバイス106はまた、クライアントデバイス106が電源投入されるとすぐにP-GW120によって割り振られるIPアドレスによって識別される。
【００１２】
制御プレーン
制御プレーンにおいて、クライアントデバイス106がネットワークへのアタッチを求めるとき、クライアントデバイス106は、アクセスノード112と接触することになる。アクセスノード112は、クライアントデバイス106に対するMME114を選択することになる。MME114は、S-GW118およびP-GW120を選択することになる。P-GW120は、一般に、ユーザまたはユーザの事業者によって提供されるアクセスポイント名(APN)に従って選択されてよい。クライアントデバイス106は、選択されたP-GW120からのIPアドレスを割り振られ、したがって、セルラーネットワーク100にアタッチされる。
【００１３】
ユーザプレーン
ひとたびアタッチされると、クライアントデバイス106は、メッセージ(たとえば、音声およびデータに対するデータトラフィック)を、ユーザプレーン上でアクセスノード112を介してP-GW120へ送信し、P-GW120から受信することができる。クライアントデバイス106とアクセスノード112との間のユーザプレーンリンクをセキュアにするために、これらの2つのノードは、K_{UPenc}鍵として知られている暗号化鍵をすぐに導出する。K_{UPenc}鍵の導出の説明は、図3で説明する鍵階層の中で提示されるK_{UPenc}鍵316に関連して与えられる。アクセスノード112とP-GW120との間のユーザプレーンバックホールリンクをセキュアにするために、これら2つのノードは、インターネットプロトコルセキュリティ(IPSEC)に依存する。IPSECは、通信セッションの各IPパケットを認証して暗号化することによってインターネットプロトコル(IP)通信をセキュアにするためのプロトコルスイートである。バックホールセキュリティは、ベアラベースで定義されるのではなく、ネットワークドメインセ

キュリティ(NDS)によって定義されることに留意されたい。

【００１４】

セルラーネットワーク100は、ダウンリンクとアップリンクの両方向でアクセスノード112へ、またはアクセスノード112から移動するユーザプレーンデータトラフィックに対するセキュリティを提供する。ダウンリンク方向において、ユーザデータトラフィックを搬送するIPメッセージが(たとえば、インターネットなどのパケットデータネットワーク122から)P-GW120に到達すると、メッセージは、IPSECを使用して暗号化され、アクセスノード112にセキュアに転送され得る。メッセージは、アクセスノード112において解読されてよい。そのために、暗号化されていないメッセージデータが、アクセスノード112上に存在することがある。次いで、メッセージは再び暗号化され、K_{UPenc}鍵を使用してアクセスノード112からクライアントデバイス106にセキュアに転送され得る。アップリンク方向において、ユーザデータを搬送するIPメッセージがクライアントデバイス106からアクセスノード112にオーバージエアで送信されるように設定されるとき、メッセージは暗号化され、K_{UPenc}鍵を使用してアクセスノード112にセキュアに転送され得る。メッセージは、アクセスノード112において解読されてよい。そのために、再び、暗号化されていないメッセージデータが、アクセスノード112上に存在することがある。次いで、メッセージは再び暗号化され、IPSECを使用してアクセスノード112からP-GW120にセキュアに転送され得る。

【００１５】

好ましくは、暗号化によってもたらされるセキュリティは、第三者による、またはさらに、危険にさらされたもしくは信頼できない場所に配置されたアクセスノードによる攻撃から安全にメッセージを保持すべきである。後で説明するように、クライアントデバイス106およびアクセスノード112はともに、クライアントデバイス106とアクセスノード112との間をアップリンクおよびダウンリンクの方向にオーバージエアで移動するデータトラフィックをセキュアにするために使用されるK_{UPenc}鍵を導出する。ユーザプレーンセキュリティは、アクセスノード112において終了する。ユーザプレーンセキュリティは、アクセスノード112の正しい振舞いに依存し、アクセスノード112は、説明したように、暗号化されていないメッセージデータが、途中で、アクセスノード112からP-GW120またはクライアントデバイス106のいずれかに転送されるべき順番を待っているときに、暗号化されていないメッセージデータを保持している。

【００１６】

セキュリティは、非アクセス層(NAS)とアクセス層(AS)との間で別々に定義されることに留意されたい。NASは、MME114などのコアネットワークノードとクライアントデバイス106との間の通信の処理を提供する。ASは、アクセスノード112とクライアントデバイス106との間の通信を提供する。加えて、制御プレーン上のセキュリティは、ユーザプレーン上のセキュリティとは別々に定義される。

【００１７】

いくつかの例は、ユーザプレーン上のセキュリティを維持することの重要性を示す。たとえば、第三者がアクセスノード112のセキュリティを損なう場合、第三者は、アクセスノード112から暗号化されていないデータを直接取り込むことができることがある。第2の例として、攻撃者は、ユーザのデータを攻撃者自身のデータと入れ替えることができる。受信者は、そのデータがユーザからのものではなかったものと確認することはできないことになる。第3の例として、攻撃者は、ユーザのメッセージ中のビットを反転することがあり、そのことで、適切に解読され得ないメッセージの送信がもたらされ、それによって貴重な資源が無駄になる。

【００１８】

アクセスノード112は公共の場(たとえば、信頼できないかまたはセキュアでない場所)に位置することがあるので、アクセスノード112は攻撃の対象となることがあり、アクセスノード112は敵対的攻撃に対してより脆弱になる。加えて、(たとえば、アクセスノード112と同様の)多くのアクセスノードは、複数のモバイルネットワーク事業者(MNO)によっ

て共有されている。モバイルネットワーク事業者はそれぞれ、同レベルのセキュリティおよび監視に従って運営するわけではないので、悪意のある一エンティティがゆるいセキュリティ活動のモバイルネットワーク事業者を介してアクセスノード112にアクセスを得ることが可能になる。

【００１９】

4Gネットワークでは、ユーザプレーンセキュリティは、クライアントデバイス106のメッセージが送受信される場所であるアクセスノード112において終了する。その結果として、ユーザプレーンデータにおけるクライアントデバイス106のプライバシーは、アクセスノード112の保全性(またはセキュリティの状況)に依存する。アクセスノード112が危険にさらされるかまたは信頼できない場所に配置される場合、クライアントデバイス106のユーザプレーンデータトラフィックのセキュリティは損なわれる恐れがある。

【００２０】

ユーザプレーンセキュリティに対するアクセスノード112へのこの依存は、アクセスノード112にあまり信頼を置かず、それゆえあまり依存しないことを追求する4Gセキュリティアーキテクチャの設計理念と相反することがある。提案されている次世代セルラーネットワーク(5Gなど)では、より高度な容量および/または帯域幅、メッシュノード、あるいはアクセスノードまたはアクセスノード機能を包含する中継ノードをサポートするためのネットワーク高密度化の必要性によって、アクセスノード112は、4Gネットワークにおけるよりもいっそう、信頼性が低くなり得る。

【発明の概要】

【発明が解決しようとする課題】

【００２１】

したがって、P-GW120とクライアントデバイス106との間のセキュアな通信のために、信頼できるエンティティとしてのアクセスノード112を取り除くことが有益であろう。

【課題を解決するための手段】

【００２２】

一態様によれば、デバイスにおいて動作可能な方法は、第1の共有鍵をデバイスにおいて取得するステップと、第1の共有鍵に基づいて第2の共有鍵をデバイスにおいて取得するステップとを含んでよい。第2の共有鍵は、デバイスとパケットデータネットワークゲートウェイ(P-GW)との間で通過中のデータトラフィックをセキュアにするためのものである。デバイスおよびP-GWは第2の共有鍵を共有してよいが、デバイスおよびP-GWは、第2の共有鍵を互いに独立に取得する。

【００２３】

デバイスは、第1のセキュアにされたデータトラフィックを作成するために、第2の共有鍵に基づいてデータトラフィックをセキュアにしてよい。次いで、デバイスは、第1のセキュアにされたデータトラフィックをアクセスノードを介してP-GWに送信してよく、P-GWおよびアクセスノードは別個のネットワークエンティティである。

【００２４】

第1の共有鍵は、P-GWに知られていないことがある。第1の共有鍵および第2の共有鍵はデバイスにおいてローカルに導出されてよく、デバイスに送信されることはない。第2の共有鍵が、ユーザプレーン通信の少なくともいくつかの層をセキュアにする一方で、異なる鍵が、制御プレーン通信をセキュアにすることができる。

【００２５】

いくつかの態様によれば、デバイスは、デバイスとモビリティ管理エンティティ(MME)との間で送信される制御メッセージングをセキュアにするために、第1の共有鍵に基づいて第3の共有鍵を取得してよく、第3の共有鍵はデバイスおよびMMEによって共有され、P-GW、MMEおよびアクセスノードは別個のネットワークエンティティである。デバイスは、デバイスとアクセスノードとの間のデータトラフィックおよびデバイスとMMEとの間の制御メッセージングをセキュアにするために、第3の共有鍵に基づいて第4の共有鍵を取得してよく、第4の共有鍵はデバイスおよびアクセスノードによって共有される。次いで、デバ

イスは、第2のセキュアにされたデータトラフィックを作成するために、第4の共有鍵に基づいて第1のセキュアにされたデータトラフィックをセキュアにしてよく、第1のセキュアにされたデータトラフィックは、第2のセキュアにされたデータトラフィックの中にカプセル化される。次いで、デバイスは、第1のセキュアにされたデータトラフィックの代わりに第2のセキュアにされたデータトラフィックをアクセスノードを介してP-GWに送信してよく、P-GW、MMEおよびアクセスノードは別個のネットワークエンティティである。

【００２６】

いくつかの態様によれば、第2の共有鍵が、ユーザプレーンのインターネットプロトコル(IP)層内の第2のセキュアにされたデータトラフィックを保護する一方で、第4の共有鍵が、ユーザプレーンのパケットデータ収束プロトコル(PDCP)層内の第2のセキュアにされたデータトラフィックを保護する。いくつかの態様によれば、第4の共有鍵が、ユーザプレーンのいくつかの層上のいくつかのトラフィックの送信を保護する一方で、第2の共有鍵が、ユーザプレーンの他の層上のトラフィックの他の送信を保護するために使用される。

【００２７】

第1の共有鍵は、デバイスとネットワークエンティティとの間で共有されてよい。ネットワークエンティティは、第1の共有鍵をホーム加入者サーバ(HSS)から取得してもよい。デバイスはP-GWとは独立に、第2の共有鍵を取得してもよい。第2の共有鍵を取得するステップは、第2の共有鍵を、第1の共有鍵およびパケットデータネットワークゲートウェイ識別子(GW ID)の関数としてデバイスにおいて導出するステップをさらに含む。

【００２８】

本明細書で説明する態様では、データトラフィックは、制御メッセージングとは異なる。データトラフィックはユーザプレーン上で送信されてよく、制御メッセージングは制御プレーン上で送信されてよく、ユーザプレーンおよび制御プレーンは別個の送信経路である。

【００２９】

いくつかの態様では、データトラフィックをセキュアにするステップは、第2の共有鍵に基づいてデータトラフィックを暗号化するステップを含む。データトラフィックをセキュアにするステップは、第2の共有鍵に基づく認証署名を含めるステップを含んでよい。

【００３０】

いくつかの態様によれば、本明細書で説明する方法は、第3のセキュアにされたデータトラフィックをアクセスノードを介してP-GWから受信するステップをさらに含んでよく、第3のセキュアにされたデータトラフィックは第2の共有鍵に基づいてセキュアにされている。方法は、セキュアでないデータトラフィックを作成するために、第2の共有鍵に基づいて、第3のセキュアにされたデータトラフィックを解読および/または認証するステップをさらに含んでよい。

【００３１】

上記で例示する方法を実行するためのデバイスについて、本明細書で説明する。加えて、少なくとも1つのプロセッサによって実行されたときに、少なくとも1つのプロセッサに、上記で例示する方法のステップを実行させる1つまたは複数の命令が記憶された非一時的機械可読記憶媒体についても、本明細書で説明する。

【００３２】

別の態様によれば、パケットデータネットワークゲートウェイ(P-GW)において動作可能な方法は、パケットデータネットワークからのデータトラフィックをP-GWにおいて受信するステップを含んでよい。P-GWは、P-GWとデバイスとの間で通過中のデータトラフィックをセキュアにするために、秘密の共有鍵をネットワークエンティティから取得してよく、秘密の共有鍵はP-GWおよびデバイスによって共有される。次いで、P-GWは、第1のセキュアにされたデータトラフィックを作成するために、秘密の共有鍵に基づいてデータトラフィックをセキュアにしてよい。次いで、P-GWは、第1のセキュアにされたデータトラフィックをアクセスノードを介してデバイスに送信してよく、P-GW、アクセスノードおよびネ

ットワークエンティティは、別個のネットワークエンティティである。
【００３３】
いくつかの態様によれば、秘密の共有鍵は、アクセスノードに知られていない。秘密の共有鍵は、ネットワークエンティティから、制御プレーンインターフェース上でP-GWに提供されてよい。いくつかの態様によれば、秘密の共有鍵が、ユーザプレーン通信の少なくともいくつかの層をセキュアにする一方で、異なる共有鍵が、制御プレーン通信をセキュアにする。たとえば、秘密の共有鍵は、ユーザプレーンのインターネットプロトコル(IP)層内のデータトラフィックを保護してよい。P-GWは、デバイスとは独立に、秘密の共有鍵を取得してもよい。秘密の共有鍵は、P-GW識別子(GW ID)の関数であってよい。秘密の共有鍵を取得するステップは、ホーム加入者サーバ(HSS)とモビリティ管理エンティティ(MME)との間に位置するネットワークエンティティから秘密の共有鍵を取得するステップをさらに含んでよい。好ましくは、秘密の共有鍵は、P-GWと同じドメイン内のネットワークエンティティから取得される。すなわち、P-GWおよびネットワークエンティティは1つのドメイン内にある。
【００３４】
P-GWにおいて動作可能な方法は、秘密の共有鍵によってセキュアにされた、セキュアにされたアップリンクデータトラフィックを、アクセスノードを介してデバイスからP-GWにおいて受信するステップをさらに含んでよい。P-GWは、アップリンクデータトラフィックを取得するために、秘密の共有鍵を用いてセキュアにされたアップリンクデータトラフィックを解読および/または認証してよい。次いで、P-GWは、アップリンクデータトラフィックをパケットデータネットワークに送信してよい。
【００３５】
P-GWにおいて実施され、上記で例示される方法を実行するためのデバイスについて、本明細書で説明する。
【００３６】
ネットワークエンティティ(たとえば、セッション鍵管理エンティティ)において動作可能な方法は、第1の共有鍵をネットワークエンティティにおいて取得するステップを含んでよい。第2の共有鍵もまた、第1の共有鍵に基づいて、ネットワークエンティティにおいて取得されてよい。第2の共有鍵は、デバイスとパケットデータネットワークゲートウェイ(P-GW)との間で通過中のデータトラフィックをセキュアにするためのものであってよい。デバイスおよびP-GWは第2の共有鍵を共有してよいが、デバイスおよびP-GWは、第2の共有鍵を互いに独立に取得する。方法は、第2の共有鍵をP-GWに送信するステップをさらに含んでよい。方法は、デバイスとモビリティ管理エンティティ(MME)との間で送信される制御メッセージングをセキュアにするために、第1の共有鍵に基づいて第3の共有鍵をネットワークエンティティにおいて取得するステップをさらに含んでよい。第3の共有鍵は、デバイスおよびMMEによって共有される。第3の共有鍵は、MMEに送信されてよい。ネットワークエンティティ、P-GWおよびMMEは、別個のネットワークエンティティであってよい。
【００３７】
いくつかの態様によれば、第2の共有鍵を取得するステップは、第2の共有鍵を、第1の共有鍵およびパケットデータネットワークゲートウェイ識別子(GW ID)の関数として導出するステップを含んでよい。
【００３８】
本明細書で説明する態様によれば、データトラフィックは、制御メッセージングとは異なる。たとえば、データトラフィックはユーザプレーン上で送信されてよく、制御メッセージングは制御プレーン上で送信されてよく、ユーザプレーンおよび制御プレーンは別個の送信経路である。
【００３９】
いくつかの態様によれば、ネットワークエンティティは、ホーム加入者サーバ(HSS)とMMEとの間に位置し、ネットワークエンティティは、HSSおよびMMEとは異なる。

【００４０】
上記で例示する方法を実行するためのデバイスについて、本明細書で説明する。加えて、少なくとも1つのプロセッサによって実行されたときに、少なくとも1つのプロセッサに、上記で例示する方法のステップを実行させる1つまたは複数の命令が記憶された非一時的機械可読記憶媒体についても、本明細書で説明する。
【図面の簡単な説明】
【００４１】
【図１】従来技術による第4世代(4G)セルラーネットワークの要素の図である。
【図２】図1の4Gセルラーネットワークのユーザプレーン内で実施される様々なプロトコルスタックのブロック図である。
【図３】図1の4Gセルラーネットワーク内で実施される鍵階層の図である。
【図４】従来技術による、制御プレーンおよびユーザプレーンに従って要素をグループ化する4G(たとえば、LTE(リリース8))セルラーネットワークの要素を示す図である。
【図５】本開示の態様による、例示的な次世代(たとえば、5G)セルラーネットワークの要素を示す図である。
【図６】図5の次世代セルラーネットワークのユーザプレーン内で実施される様々なプロトコルスタックのブロック図である。
【図７】図5の例示的な次世代セルラーネットワーク内で実施される鍵階層の図である。
【図８】本開示の態様による、制御プレーンおよびユーザプレーンに従って要素をグループ化する例示的な次世代(たとえば、5G)セルラーネットワークの要素を示す図である。
【図９】本開示の態様による、パケットデータネットワーク(PDN)接続セットアップ中の制御プレーン内の、K_{P-GW}鍵と本明細書において呼ばれる共有鍵の初期のプロビジョニングに関連付けられたコールフロー、およびユーザプレーン内のK_{P-GW}鍵を用いて暗号化/認証されたメッセージの後続の通信の一例を示す図である。
【図１０Ａ】P-GWがホームネットワーク内にあってH-P-GWとして識別される制御プレーンおよびユーザプレーンに従って、要素をグループ化する例示的な次世代セルラーネットワークの要素を示す図である。
【図１０Ｂ】P-GWが訪問先ネットワーク内にあってV-P-GWとして識別される制御プレーンおよびユーザプレーンに従って、要素をグループ化する例示的な次世代セルラーネットワークの要素を示す図である。
【図１１】本明細書で説明する態様による、次世代セルラーネットワーク内でユーザプレーンメッセージ(たとえば、ユーザプレーンデータトラフィック)のセキュリティおよび/または保全性を保護するための、クライアントデバイスにおいて動作可能な例示的な方法を示す図である。
【図１２】本明細書で説明する態様による、次世代セルラーネットワーク内でユーザプレーンメッセージ(たとえば、ユーザプレーンデータトラフィック)のセキュリティおよび/または保全性を保護するための、クライアントデバイスにおいて動作可能な例示的な方法を示す図である。
【図１３】本明細書で説明する態様による、次世代セルラーネットワーク内でユーザプレーンメッセージ(たとえば、ユーザプレーンデータトラフィック)のセキュリティおよび/または保全性を保護するための、クライアントデバイスにおいて動作可能な例示的な方法を示す図である。
【図１４】本明細書で説明する態様による、次世代セルラーネットワーク内でユーザプレーンメッセージ(たとえば、ユーザプレーンデータトラフィック)のセキュリティおよび/または保全性を保護するための、クライアントデバイスにおいて動作可能な例示的な方法を示す図である。
【図１５】本明細書で説明する態様による、次世代セルラーネットワーク内でユーザプレーンメッセージ(たとえば、ユーザプレーンデータトラフィック)のセキュリティおよび/または保全性を保護するための、クライアントデバイスにおいて動作可能な例示的な方法を示す図である。

【図１６】本明細書で説明する態様による、次世代セルラーネットワーク内でユーザプレーンメッセージ(たとえば、ユーザプレーンデータトラフィック)のセキュリティおよび/または保全性を保護するための、デバイス(たとえば、チップ構成要素、クライアントデバイス)において動作可能な例示的な方法を示す図である。
【図１７】本明細書で説明する態様による、次世代セルラーネットワーク内でユーザプレーンメッセージ(たとえば、ユーザプレーンデータトラフィック)のセキュリティおよび/または保全性を保護するための、たとえばアクセスノードにおいて動作可能な例示的な方法を示す図である。
【図１８】本明細書で説明する態様による、セルラーネットワーク内でユーザプレーンメッセージ(たとえば、ユーザプレーンデータトラフィック)を保護するための、アクセスノード(たとえば、eノードB)において動作可能な例示的な方法を示す図である。
【図１９】本明細書で説明する態様による、次世代セルラーネットワーク内でユーザプレーンメッセージのセキュリティおよび/または保全性を保護するための、P-GWにおいて動作可能な例示的な方法を示す図である。
【図２０】本明細書で説明する態様による、セルラーネットワーク内でユーザプレーンメッセージ(たとえば、ユーザプレーンデータトラフィック)を保護するための、パケットデータネットワークへのゲートウェイ(たとえば、P-GW)において動作可能な例示的な方法を示す図である。
【図２１】本明細書で説明する態様による、次世代セルラーネットワーク内でユーザプレーンメッセージ(たとえば、ユーザプレーンデータトラフィック)のセキュリティおよび/または保全性を保護するための、セッション鍵管理エンティティ(SKME)と本明細書で呼ばれるネットワークエンティティにおいて動作可能な例示的な方法を示す図である。
【図２２】本明細書で説明する態様による、セルラーネットワーク内でユーザプレーンメッセージ(たとえば、ユーザプレーンデータトラフィック)を保護する鍵を導出するための、SKMEにおいて動作可能な例示的な方法を示す図である。
【図２３】本明細書で説明する方法を実行するように構成されたデバイスの例示的なハードウェア実装形態のブロック図である。
【図２４】本明細書で説明する態様による、セルラーネットワーク内でユーザプレーンメッセージ(たとえば、ユーザプレーンデータトラフィック)を保護するための、デバイス(たとえば、チップ構成要素、クライアントデバイス)において動作可能な例示的な方法を示す図である。
【図２５】本明細書で説明する方法を実行するように構成されたパケットデータネットワークゲートウェイ(P-GW)の例示的なハードウェア実装形態のブロック図である。
【図２６】本明細書で説明する態様による、セルラーネットワーク内でユーザプレーンメッセージ(たとえば、ユーザプレーンデータトラフィック)を保護するための、P-GWにおいて動作可能な例示的な方法を示す図である。
【図２７】本明細書で説明する方法を実行するように構成されたセッション鍵管理エンティティ(SKME)と本明細書で呼ばれるネットワークエンティティの例示的なハードウェア実装形態のブロック図である。
【図２８】本明細書で説明する態様による、セルラーネットワーク内でのユーザプレーンメッセージ(たとえば、ユーザプレーンデータトラフィック)の保護に関連する、SKMEにおいて動作可能な例示的な方法を示す図である。
【発明を実施するための形態】
【００４２】
添付の図面に関して以下に記載する詳細な説明は、様々な構成の説明として意図されており、本明細書において説明する概念が実践される場合がある唯一の構成を表すことは意図されていない。詳細な説明は、様々な概念を完全に理解してもらうために具体的な詳細を含む。しかしながら、これらの概念がこれらの具体的な詳細なしに実践される場合があることは当業者に明らかであろう。場合によっては、そのような概念を曖昧にするのを避けるために、よく知られている構造および要素がブロック図の形で示される。

【００４３】
本明細書で使用する「取得するステップ」という用語は、ローカルに導出するステップまたは別のエンティティから取得するステップを意味することがある。本明細書で使用する「デバイス」という用語は、チップ構成要素、および/またはクライアントデバイス(たとえば、デバイスの中でも、モバイルデバイス、ユーザ機器、ユーザデバイス、端末、モバイルフォン、モバイル通信デバイス、モバイルコンピューティングデバイス、デジタルタブレット、スマートフォン、ウェアラブルスマートデバイス)などのユーザデバイスを記述することがある。本明細書で使用する「Bに基づいてAを導出するステップ」という句および類似の構文は、Bから直接的または間接的にAを導出/生成するステップを意味するために使用されることがある。本明細書で使用する「セキュアにするステップ」という用語は、ユーザプレーンデータトラフィック内のパケットまたはメッセージを認証することに関連する何らかのアクションを暗号化/解読すること、および/または実行することを意味することがある。

【００４４】
知られているシステム内に存在する問題および欠点を克服するために、クライアントデバイス106とP-GW120との間のセキュアな通信のための、アクセスノード112の保全性(またはセキュリティの状況)への依存を低減する態様が、本明細書に提示される。

【００４５】
概要
次世代セルラーネットワーク(たとえば、4Gネットワークに対して)において向上したセキュリティを提供するために、第1の共有鍵が、クライアントデバイスによって、およびパケットデータネットワークへのセルラーネットワークゲートウェイ(以後、パケットデータネットワーク(PDN)ゲートウェイ(P-GW)と呼ばれる)によって認識、取得および/または導出される。クライアントデバイスは、セルラーネットワークに対するアクセスノードを介してP-GWと通信する。クライアントデバイスおよびP-GWは、独立して、第1の共有鍵を認識、取得、生成および/または導出する。すなわち、第1の共有鍵を認識、取得、生成および/または導出することに関して、2つのエンティティ間の交渉は存在しない。2つのエンティティ間で鍵関連情報を交換することはない。言い換えれば、独立して認識、取得、生成および/または導出することは、2つのエンティティが、それら自体の間で何も交換することなく、同じ鍵の2つのインスタンスを別々に認識、取得、生成および/または導出することを意味する。第1の共有鍵は、クライアントデバイスとP-GWとの間で送信されるメッセージを暗号化および/または認証する働きをしてよい。第1の共有鍵はアクセスノードに知られていないので、アクセスノードを介してクライアントデバイスとP-GWとの間で送信されたメッセージは、改ざんおよび/またはアクセスノードへのアクセス不能に対してセキュアにされる。

【００４６】
第2の共有鍵は、クライアントデバイスおよびアクセスノードによって認識、取得、生成および/または導出されてよく、ここで第2の共有鍵は第1の共有鍵とは異なる。第2の共有鍵は、クライアントデバイスとアクセスノードとの間で送信されるオーバージエアメッセージを暗号化および/または認証する働きをしてよい。

【００４７】
一例では、アクセスノードを介してクライアントデバイスとP-GWとの間で送信された第1のメッセージは、最初に第1の共有鍵を使用して暗号化および/または認証されてよく、次いで、第2の共有鍵を使用して暗号化および/または認証される第2のメッセージの中にカプセル化される。

【００４８】
4Gセルラーネットワークユーザプレーンセキュリティ
図2は、図1の4Gセルラーネットワークのユーザプレーン内で実施される様々なプロトコルスタック200のブロック図である。様々なプロトコルスタック200は、クライアントデバイス202、アクセスノード204、P-GW206およびアプリケーションサーバ(APPサーバ)208内

に実装されるように示されている。標準の運用支援システム(OSS)モデルに従って、クライアントデバイス202内に実装されたプロトコルスタックは、インターネットプロトコル層(IP層)210、パケットデータ収束プロトコル(PDCP)層212、無線リンク制御(RLC)層214、媒体アクセス制御(MAC)層216、および物理(PHY)層218を含んでよい。アクセスノード204内に実装されたプロトコルスタックは、クライアントデバイス106のプロトコルスタックに対応する層を含んでよい。たとえば、アクセスノード204層は、PDCP層220、RLC層222、MAC層224、およびPHY層226を含んでよい。加えて、ユーザプレーンに対する汎用パケット無線サービス(GPRS)トンネリングプロトコル(GTP-U)層228、ユーザデータグラムプロトコル(UDP)層230、インターネットプロトコル層(IP層)232、MAC層234、およびイーサーネット層236が、パケットデータネットワークゲートウェイ(P-GW)206との通信のために含まれる。P-GW206内に実装されたプロトコルスタックは、アクセスノード204と通信するための対応する(GTP-U)層238、ユーザデータグラムプロトコル(UDP)層240、IP層242、MAC層244、およびイーサーネット層246を含んでよい。APPサーバ208内に実装されたプロトコルスタックは、IP層248を含んでよい。APPサーバ208のIP層248は、P-GW206のIP層250と通信するためのものである。P-GW206のIP層250は、クライアントデバイス202のIP層210と通信してよい。ここで確認された層(just-identified layer)は、当技術分野において知られている。これらの層の詳細な説明は当業者にとって入手可能であり、簡明にするために本明細書では説明しない。

【００４９】

図2は、クライアントデバイス202のPDCP層212とアクセスノード204のPDCP層220との間の通信が、共有鍵、K_{eNB}鍵252に基づいて暗号化/解読されることを示し、ここでK_{eNB}鍵252は、共有されるユーザプレーン暗号化鍵、K_{UPenc}を導出するために使用されてよい。言い換えれば、クライアントデバイス202のPDCP層212とアクセスノード204のPDCP層220との間の通信は、共有鍵、K_{eNB}鍵252に基づいてセキュアにされてよい。加えて、図2は、アクセスノード204のIP層232とP-GW206のIP層242との間の通信が、インターネットプロトコルセキュリティ(IPSEC)254を使用してセキュアにされることの表示を与える。

【００５０】

図1および図2を参照すると、4Gでは、クライアントデバイス106がユーザプレーンメッセージをパケットデータネットワーク122(たとえば、インターネット)に送信する場合、クライアントデバイス106は、最初に、ユーザプレーンメッセージをアクセスノード112に送信しなければならない。ユーザプレーンメッセージを保護するために、クライアントデバイス106は、K_{eNB}鍵252に基づいて(すなわち、K_{UPenc}鍵を導出するためにK_{eNB}鍵252を使用して)メッセージを暗号化してよい。暗号化されると、クライアントデバイス106は、メッセージをアクセスノード112に送信してよい。アクセスノード112は、K_{eNB}鍵252に基づいて(すなわち、K_{UPenc}鍵を導出するためにK_{eNB}鍵252を使用して)ユーザプレーンメッセージを解読してよい。したがって、ユーザプレーンメッセージの暗号化されていないコンテンツが、アクセスノード112に対して利用可能である。したがって、アクセスノード112を通過する通信のセキュリティを保護することは、アクセスノード112に大きく依存している。上記のように、セキュリティ問題にかかわらず、アクセスノード112は、4G通信に対して信頼できるエンティティであると見なされてよい。

【００５１】

解読の後、アクセスノード112は、ユーザプレーンメッセージをP-GW120に転送してよい。アクセスノード112は、IPSEC254を使用して、アクセスノード112のIP層からP-GW120の対応するIP層に転送される各IPメッセージをセキュアにすることができる。アクセスノード112は、セキュアにされると、IPSECプロトコルに従って各IPメッセージをP-GW120に送信してよい。IPSECプロトコルは、従来技術において知られている。IPSECプロトコルの詳細な説明は当業者にとって入手可能であり、簡明にするために本明細書では説明しない。

【００５２】

図3は、図1の4Gセルラーネットワーク内で実施される鍵階層300である。K302鍵として本明細書で識別されるルート鍵は、クライアントデバイスのユニバーサル加入者識別モジ

ュール(USIM)上に記憶されてよく、同様に、コアネットワークの認証センター(AuC)において記憶されてもよい。クライアントデバイスとコアネットワークとの間の認証セッションの間、USIMおよびAuCはそれぞれ独立に、K302鍵に基づいて、保全性鍵(IK)、暗号鍵(CK)304鍵と本明細書で総称されるIKおよびCKを導出してよい。IK、CK304鍵は、セッション鍵と呼ばれることがある。

【００５３】

認証および鍵合意(AKA)手順の間、IK、CK304鍵は、AuCからHSSに送信されてよい。言い換えれば、HSSは、AuCからIK、CK304鍵を取得してよい。クライアントデバイスは、すでに、(クライアントデバイスにおいてUSIMによって導出されたIKおよびCK鍵によって)IK、CK304鍵を有する。

【００５４】

クライアントデバイスおよびHSSはそれぞれ、IK、CK304鍵に基づいてアクセスセキュリティ管理エンティティ(ASME)鍵(K_{ASME}鍵)306を独立に導出してよい。K_{ASME}鍵306は、HSSからMMEに送信されてよい。言い換えれば、MMEは、HSSからK_{ASME}鍵306を取得してもよい。クライアントデバイスは、すでに、(クライアントデバイスにおけるIK、CK304鍵に基づいてK_{ASME}鍵306を導出することによって)K_{ASME}鍵306を有する。MMEは、信頼できる鍵エンティティと見なされてよい。

【００５５】

クライアントデバイスおよびMMEはそれぞれ、K_{ASME}鍵306に基づいて非アクセス層暗号化鍵(K_{NASenc}鍵)308および非アクセス層保全性鍵(K_{NASint}鍵)310を独立に導出してよい。K_{NASenc}鍵308およびK_{NASint}鍵310は、クライアントデバイスとMMEとの間の制御プレーンメッセージを保護することを意図している。そのような保護は、他の要素が、制御プレーン内のメッセージを解読または修正することを防止する。

【００５６】

同じく、クライアントデバイスおよびMMEはそれぞれ、K_{ASME}鍵306に基づいて、K_{eNB}鍵312と本明細書で呼ばれるアクセスノード鍵を独立に導出してよい。K_{eNB}鍵312は、MMEからアクセスノードに送信されてよい。言い換えれば、アクセスノードは、MMEからK_{eNB}鍵312を取得してもよい。この点において、クライアントデバイスおよびアクセスノードはそれぞれ、K_{eNB}鍵312として識別される鍵を所有する。言い換えれば、クライアントデバイスおよびアクセスノードは、K_{eNB}鍵312を共有する。

【００５７】

K_{eNB}鍵312を含むブロックの中で、ネクストホップ(NH)カウンタへの参照がなされる。MMEは、アクセスノードに対する第1のK_{eNB}鍵を導出する。クライアントデバイスが、第1のアクセスノードから第2のアクセスノードに「前方に」移動するときはいつでも、MMEは、新しいK_{eNB}鍵を導出して、第1のK_{eNB}鍵を置き換える。次いで、MMEは、前のアクセスノードからの接続を保護するために、新しいK_{eNB}鍵を第2のアクセスノードに送信する。したがって、NHカウンタは、MMEおよびクライアントデバイス内で導出されるべき中間K_{eNB}鍵のための方法を提供する。これは、前方セキュリティ手順として知られている。前方セキュリティ手順のおかげで、第1の鍵が、第1のアクセスノードから第2のアクセスノードへのクライアントデバイスのハンドオーバに関連して新しい鍵に交換されるとき、第1のアクセスノードは、第2のアクセスノードを介して送信されたメッセージを解読または修正するために第1のK_{eNB}鍵を使用することはできない。

【００５８】

K_{ASME}鍵306に基づいて導出されたK_{eNB}鍵312を使用して、クライアントデバイスおよびアクセスノードは、4つの異なる鍵を独立して導出してよいが、実際には通常、3つの鍵が導出される。4つの可能性のある鍵には、K_{UPint}鍵314と呼ばれるユーザプレーン保全性鍵、K_{UPenc}鍵316と呼ばれるユーザプレーン暗号化鍵、K_{RRCint}鍵318と呼ばれる制御プレーン(無線リソース制御)保全性鍵、およびK_{RRCenc}鍵320と呼ばれる制御プレーン(無線リソース制御)暗号化鍵が含まれる。下付き文字「enc」を有する鍵は、暗号化のために使用される。下付き文字「int」を有する鍵は、保全性のために使用される。4Gでは、ユーザプ

レーン保全性は考慮されず、したがって一般に、K_{UPint}鍵314は導出されない。

【００５９】

4Gセルラーネットワークのユーザプレーンプロトコルスタックの図2に戻ると、クライアントデバイス202のPDCP層212とアクセスノード204のPDCP層220との間で転送されるメッセージは、K_{eNB}鍵252に基づいて(すなわち、K_{UPenc}鍵を導出するためにK_{eNB}鍵252を使用して)暗号化されてよい。K_{UPenc}鍵(図3のK_{UPenc}鍵316に類似する)を使用する暗号化は、メッセージの方向を顧慮することなく、クライアントデバイス202のPDCP層212とアクセスノード204のPDCP層220との間で転送されるメッセージに対して実行されてよい。保全性は、4Gユーザプレーンメッセージにおいて、クライアントデバイス202とアクセスノード204との間で制御されることはない。

【００６０】

図2に示すように、ユーザプレーンメッセージ暗号化ステップを説明する。クライアントデバイス202が、メッセージをAPPサーバ208に送信することを求めているシナリオを想定する。クライアントデバイス202およびAPPサーバ208は、送信制御プロトコル/インターネットプロトコル(TCP/IP)またはユーザデータグラムプロトコル/インターネットプロトコル(UDP/IP)のプロトコルを使用して通信してよい。ユーザプレーン内でメッセージを送信するために、クライアントデバイス202は、プロトコルスタックに従って、PDCP層212を利用してよい。第3世代パートナーシッププロジェクト(3GPP)として知られる規格設定団体が、PDCP層212を定義し得る。PDCP層212は、クライアントデバイス202からアクセスノード204に送信されたメッセージを暗号化(たとえばサイファー化)および認証(たとえば、保全性保護)を行う役目を果たすことができる。メッセージを暗号化するために、クライアントデバイス202は、K_{eNB}鍵252に基づいてクライアントデバイス202によって導出されたK_{UPenc}鍵を使用してよい。アクセスノード204は、K_{eNB}鍵252の共有されたコピーに基づいて、同じK_{UPenc}鍵を独立に導出している。クライアントデバイス202とアクセスノード204の両方が同じ鍵を保有するという点で、K_{UPenc}鍵は共有鍵である。K_{UPenc}鍵は、クライアントデバイス202とアクセスノード204との間においてのみ有益である。K_{UPenc}鍵は、クライアントデバイス202と任意の他のアクセスノードとの間のメッセージを暗号化または解読するために使用することはできない。

【００６１】

クライアントデバイス202のPDCP層212は、K_{UPenc}鍵(ここでK_{UPenc}鍵はK_{eNB}鍵252に基づいて導出された)を使用してユーザプレーンメッセージを暗号化し、暗号化されたメッセージを、下位層(RLC層214、MAC層216、PHY層218)のヘッダがメッセージに追加されてそのメッセージがアクセスノード204に送信され得るように、下位層に送信する。メッセージを上位層から受信した後、下位層は、3GPPによって確立された規格に従ってメッセージを処理し、処理されたメッセージをアクセスノード204に送信する。

【００６２】

アクセスノード204のPDCP層220は、受信すると、共有鍵、K_{eNB}鍵252に基づいてアクセスノード204によって導出されたK_{UPenc}鍵を使用して、メッセージを解読することができる。次いで、アクセスノード204は、メッセージが転送されるべきP-GW(たとえば、P-GW206)のIPアドレスを(解読されたデータから)決定することができる。次いで、メッセージは、IPSEC254を使用してカプセル化される。IPSECトンネルが、アクセスノード204とP-GW206との間で確立される。次いで、IPSECトンネルによって確立された相互接続に基づいて、アクセスノード204は、追加のヘッダを追加した後、全IPメッセージをカプセル化し、カプセル化されたメッセージをP-GW206に送信する。IPSEC254は、アクセスノード204とP-GW120との間の接続を保護し、それゆえ、その接続はセキュアであるものと見なされてよい。P-GW206が、IPSEC254によって保護されたメッセージを受信すると、P-GW206は、そのメッセージを検証してよい。検証が正常であると、P-GW206は、アクセスノード204によって追加されたヘッダのすべてを取り除いてよく、最終的に、クライアントデバイス202から受信されたメッセージをAPPサーバ208に送信する。

【００６３】

メッセージは、クライアントデバイスからP-GWまで通して保護されているように見える。しかしながら、クライアントデバイス202の視点からすれば、4Gユーザプレーンセキュリティは、アクセスノード204において終了していることがある。4Gでは、クライアントデバイス202は、ユーザプレーンセキュリティをアクセスノード204に依存している。なぜならば、クライアントデバイス202は、アクセスノード204がP-GW206とのセキュアな接続を有しているかどうかを決定することはできないからである。アクセスノード204は、メッセージがアクセスノード204にセキュアに到達したのであれば、アクセスノード204はメッセージをP-GW206にセキュアに送信するであろう、と当てにしなければならない。アクセスノード204はまた、メッセージがP-GW206に正常に到達したのであれば、インターネットサービスプロバイダ(ISP)はメッセージをP-GW206からAPPサーバ208にセキュアに送信するであろう、と当てにしなければならない。そのために、4Gセルラーネットワークでは、クライアントデバイス202は、たとえば、オーバージエア盗聴者がメッセージを解読できないように、クライアントデバイス202自体とアクセスノード204との間にメッセージのセキュリティを与えるために、メッセージの暗号化のみに関心が払われている。

【００６４】

図4は、従来技術による、制御プレーンおよびユーザプレーンに従って要素をグループ化する4G(たとえば、LTE(リリース8))セルラーネットワーク400の要素を示す。図4では、トンネルまたはパイプラインの図式表現が、セキュアな信号経路を表すために使用される。図4は、コアネットワーク402の要素を示す。図4はまた、クライアントデバイス406とワイヤレスに通信中であり得るアクセスノード404を示す。コアネットワーク402は、HSS408、MME410、S-GW412、およびP-GW414を含む。アクセスノード404は、RRC416エンティティ(制御プレーン内で発見されるエンティティ)、PDCP/RLCエンティティ418、およびIPエンティティ420(PDCP/RLCおよびIPのエンティティはユーザプレーン内で発見される)を含む。

【００６５】

したがって、上記で説明したように、4Gセルラーネットワーク内のユーザプレーンセキュリティは、アクセスノード404(たとえば、eノードB)の正しい振舞いに依存する。アクセスノード404は4GにおけるMME410よりも信頼できないエンティティであるので、MME410は、ローカルトラストアンカーまたはローカル鍵アンカーと見なされる。必要なときはいつでも、MME410は、K_{eNB}鍵をアクセスノード404に配信することができる。K_{UPenc}鍵は、K_{eNB}鍵に基づいて導出されてよい。

【００６６】

図4は、いくつかの導出された暗号化鍵の使用と、IPSECトンネル426の使用とを視覚的に示す。図4の態様によれば、MME410は、K_{ASME}鍵に対するローカルトラストアンカーまたはローカル鍵アンカーである。MME410とクライアントデバイス406との間のパイプライン422は、MME410とクライアントデバイス406との間の制御プレーンメッセージが、K_{NASenc}鍵およびK_{NASint}鍵のセキュリティを用いて送信されることを示す。図3に関して上記で説明したように、クライアントデバイス406およびMME410はそれぞれ、K_{ASME}鍵に基づいて非アクセス層暗号化K_{NASenc}鍵および非アクセス層保全性K_{NASint}鍵を独立に導出してよい。アクセスノード404のPDCP/RLCエンティティ418とクライアントデバイス406との間のパイプライン424は、PDCP/RLCエンティティ418とクライアントデバイス406との間のユーザプレーンメッセージが、K_{UPenc}鍵のセキュリティを用いて送信されることを示す。図3に関して上記で説明したように、クライアントデバイス406およびアクセスノード404は、K_{UPenc}鍵(すなわち、ユーザプレーン暗号化鍵)を独立に導出してよい。アクセスノード404のIPエンティティ420とコアネットワーク402のP-GW414との間のIPSECトンネル426は、IPエンティティ420とP-GW414との間のユーザプレーンメッセージが、IPSECのセキュリティを用いて送信されることを示す。

【００６７】

次世代セルラーネットワークのユーザプレーンセキュリティ

上記で説明した4Gシナリオは、4Gセルラーセキュリティアーキテクチャの問題のある設計理念を例示する。ユーザプレーンのセキュリティまたはプライバシーがアクセスノード

の保全性(またはセキュリティの状況)に依存するという問題は、次世代(たとえば、5G)セルラーネットワークにおいて矯正され得る。本明細書で具現化される次世代セルラーネットワークでは、クライアントデバイスとP-GWとの間の直接的セキュリティ関係が確立され、アクセスノードの保全性(またはセキュリティの状況)への依存が低減され得る。本明細書で使用する直接的セキュリティ関係は、クライアントデバイスとP-GWとの間の(たとえば、通信/メッセージ/パケットの交換のための)セキュアな接続が、中間のエンティティまたはノードを信頼する必要なしに提供され得ることを意味することがある。直接的セキュリティ関係は、クライアントデバイスおよびP-GWによって共有される鍵の使用によって確立されてよく、しかも、その鍵は、クライアントデバイスとP-GWとの間の交渉または交換の結果もたらされるものではない。言い換えれば、クライアントデバイスは共有鍵をP-GWとは独立に取得し、同様に、P-GWは、共有鍵をクライアントデバイスとは独立に取得する。

【００６８】

図5は、本開示の態様による、例示的な次世代(たとえば、5G)セルラーネットワーク500の要素の図である。セルラーネットワーク500は、発展型ユニバーサル地上波無線アクセスネットワーク(E-UTRAN)502として説明されることがあるアクセス部分(たとえば、無線アクセスネットワーク(RAN))と、発展型パケットコア(EPC)504と本明細書で呼ばれることがあるコア部分(たとえば、コアネットワーク)とを含んでよい。E-UTRAN502およびEPC504はともに、発展型パケットシステム(EPS)を形成する。

【００６９】

EPSは、クライアントデバイス506(たとえば、モバイルデバイス、モバイル端末、ユーザ機器(UE)、端末)と通信してよい。クライアントデバイス506は、ユニバーサル加入者識別モジュール(USIM)508(通常、SIMカードと呼ばれる)を含んでよい。USIM508は、たとえば、国際移動体加入者識別(IMSI)番号およびそれに関連する鍵、Kをセキュアに記憶する集積回路チップであってよい。鍵、Kはルート鍵であってよい。ルート鍵、Kは、本明細書で説明する任意の態様から逸脱することなく、限定はしないが、USIM508上にセキュアなストレージを含む任意の数の方法でクライアントデバイス506においてセキュアに記憶されてよい。

【００７０】

EPSにおける通信は、プレーン、すなわちユーザプレーン(UP)と制御プレーン(CP)とに分割される。図5では、1つの特定の制御プレーンシグナリング経路が、アクセスノード512(たとえば、eノードB)とモビリティ管理エンティティ(MME)514との間の破線510によって識別される一方で、1つの特定のユーザプレーンデータ経路が、アクセスノード512とサービングゲートウェイ(S-GW)518との間の実線516によって識別される。制御プレーンシグナリングおよびユーザプレーンデータに対する追加で代替の経路が、当業者に知られている。図5の図は例であり、限定を意味するものではない。

【００７１】

E-UTRAN502は、クライアントデバイス506とワイヤレスに通信するハードウェアを含むアクセスノード512を含む。ロングタームエボリューション(LTE)ネットワークでは、たとえば、アクセスノード512は、発展型ノードB(eノードB)と呼ばれることがある。例として、単一のLTEアクセスノードは、1つまたは複数のE-UTRAN502セルの働きをすることがある。

【００７２】

EPC504は、パケットデータネットワーク(PDN)ゲートウェイ(P-GW)520など、様々なネットワークエンティティを含む。P-GW520は、インターネットおよび/または民間企業ネットワークなどのパケットデータネットワーク522へのゲートウェイとしての働きをする。P-GW520は、パケットデータネットワーク522に対するネットワークポリシー実施の通路および点と見なされてよく、一方で、アクセスノード512は、クライアントデバイス506の、パケットデータネットワーク522が接続されるコアネットワーク(たとえば、EPC504)へのオーバージエアアクセスのための通路と見なされてよい。アクセスノード512は、P-GW520と

コロケートされてよいが、アクセスノード512の機能は、P-GW520の機能とは異なる。言い換えれば、アクセスノード512およびP-GW520は、それらがコロケートされる場合でも、別個の機能を有する別個のエンティティである。

【００７３】

EPC504は、ホーム加入者サーバ(HSS)524などのネットワークエンティティをさらに含む。HSS524は、各クライアントデバイス506の一意の識別情報を記憶する。認証センター(AuC)526は、HSS524に結合されてよい。AuC526は、クライアントデバイス506がEPC504(たとえば、コアネットワーク)への接続を試みるとき、USIM508を認証する働きをすることがある。AuC526は、USIM508に記憶された鍵と同じ鍵を記憶してよい。USIM508カードの認証は、一般に、クライアントデバイス506が電源投入されるときに発生し得る。

【００７４】

EPC504はまた、S-GW518などのネットワークエンティティを含む。S-GW518は、ユーザプレーンIPメッセージのクライアントデバイス506への移送およびそこからの移送に関連する機能を実行する。概して、メッセージは1つまたは複数のパケットを含んでよいことを理解されたい。パケットおよびメッセージは異なるフォーマットを有してよく、異なるヘッダによってカプセル化されてよい。本明細書における参照を容易にするために、用語メッセージが、全体にわたって使用される。EPC504はまた、MME514を含む。MME514が制御プレーンに関連する一方で、クライアントデバイス506、アクセスノード512、S-GW518、P-GW520、およびHSS524は、制御プレーンとユーザプレーンの両方に関連する。MME514は、様々な物理チャネルをセットアップ、維持、および解放することに関連する機能を実行する。

【００７５】

EPC504は、セッション鍵管理エンティティ(SKME)528と本明細書で呼ばれることがあるネットワークエンティティをさらに含んでよい。ローカル鍵アンカー、ローカルトラストアンカー、鍵導出および維持ストアなど、SKME528に対する代替名称が容認されている。1つまたは複数のSKMEが、所与のドメイン/ネットワーク/サービングネットワーク内に位置することがある。たとえば、本明細書で説明する態様では、1つのSKMEがクライアントデバイスのホームネットワーク内に存在していると見なされるとき、そのSKMEは、ホームセッション鍵管理エンティティ(H-SKME)528と呼ばれることがある。さらなる例として、本明細書で説明する態様では、1つのSKMEがクライアントデバイスの訪問先ネットワーク内に存在していると見なされるとき、そのSKMEは、訪問先セッション鍵管理エンティティ(V-SKME)530と呼ばれることがある。H-SKME528および/またはV-SKME530は、HSS524とMME514との間に位置することがある。いくつかの態様では、H-SKME528および/またはV-SKME530は、論理エンティティであるものとして説明されてよく、それらの機能は、H-SKME528および/またはV-SKME530のタスクを実行するように特別に構成されたハードウェア内に実装されてよい。V-SKME530は、H-SKME528を介してHSS524に直列に接続されているように示されているが、V-SKME530は、HSS524と直接通信することができる。いくつかの態様では、1つのSKMEは、H-SKME528とV-SKME530の両方の機能を実行することができる。次世代セルラーネットワークのEPC504は、訪問先P-GW(V-P-GW532とも呼ばれる)をさらに含んでよい。本明細書で開示する次世代セルラーネットワークでは、H-SKME528および/またはV-SKME530は、ローカルトラストアンカーまたはローカル鍵アンカーとしての働きをすることがある。H-SKME528とP-GW520との間の破線は、第1の制御プレーンシグナリング経路534を識別する。V-SKME530とV-P-GW532との間の破線は、第2の制御プレーンシグナリング経路536を識別する。第1の制御プレーンシグナリング経路534および/または第2の制御プレーンシグナリング経路536は、第1の共有鍵(たとえば、図7のK_{P-GW}鍵724)を、必要に応じて、ローカルトラストアンカーまたはローカル鍵アンカー、H-SKME528、V-SKME530からP-GW520、V-P-GW532に配信するために使用されることがある。

【００７６】

クライアントデバイス506からP-GW520まで通して次世代セルラーネットワーク内でユー

ザプレーンセキュリティを提供するために、H-SKME528および/またはV-SKME530が、HSS524とMME514との間に導入される。H-SKME528および/またはV-SKME530は、共有鍵を導出、維持、および/または記憶する役目を果たすことができる。クライアントデバイス506およびP-GW520(および/またはV-P-GW532)は、共有鍵を共有してよい。H-SKME528は、共有鍵を、それのホームネットワーク内のP-GW520に提供してよい。V-SKME530は、共有鍵を、訪問先ネットワークのV-P-GW532に提供してよい。共有鍵は、次世代セルラーネットワーク内のユーザプレーンデータを保護するために使用されてよい。共有鍵は、K_{P-GW}鍵(たとえば、図7、K_{P-GW}鍵724)と呼ばれることがある。クライアントデバイスならびにP-GW520および/またはV-P-GW532は、第1の共有鍵を独立して認識、取得および/または導出する。すなわち、第1の共有鍵の認識、取得、および/または導出に関して、クライアントデバイス506とP-GW520および/またはV-P-GW532との間の交渉は存在しない。クライアントデバイス506とP-GW520および/またはV-P-GW532との間で鍵関連情報の交換は存在しない。

【００７７】

ホームネットワークの場合、H-SKME528の機能は、場合によっては、HSS524内に実装され得る。

【００７８】

本明細書で説明するいくつかの態様によれば、ローカルトラストアンカーまたはローカル鍵アンカーの役割(4Gセルラーネットワーク内のMMEによって果たされる役割)は、次世代セルラーネットワーク内でH-SKME528および/またはV-SKME530に割り当てられてよい。

【００７９】

図6は、図5の次世代セルラーネットワークのユーザプレーン内で実装される様々なプロトコルスタック600のブロック図である。様々なプロトコルスタック600が、クライアントデバイス602、アクセスノード604、パケットデータネットワークゲートウェイ(P-GW)606およびアプリケーションサーバ(APPサーバ)608内に実装されるように示されている。標準OSSモデルに従って、クライアントデバイス602内に実装されたプロトコルスタックは、インターネットプロトコル層(IP層)610、パケットデータ収束プロトコル(PDCP)層612、無線リンク制御(RLC)層614、媒体アクセス制御(MAC)層616、および物理(PHY)層618を含んでよい。アクセスノード604内に実装されるプロトコルスタックは、クライアントデバイス106と通信するために、対応するPDCP層620、RLC層622、MAC層624、およびPHY層626を含んでよい。加えて、ユーザプレーンに対するGPRSトンネリングプロトコル(GTP-U)層628、ユーザデータグラムプロトコル(UDP)層630、インターネットプロトコル(IP)層632、MAC層634、およびイーサーネット層636が、P-GW606との通信のために含まれる。P-GW606内に実装されたプロトコルスタックは、アクセスノード604と通信するために、対応する(GTP-U)層638、ユーザデータグラムプロトコル(UDP)層640、インターネットプロトコル(IP)層642、MAC層644、およびイーサーネット層646を含んでよい。APPサーバ608内に実装されたプロトコルスタックは、P-GW606のIP層650と通信するためのIP層648を含んでよい。P-GW606のIP層650は、クライアントデバイス602のIP層610と通信してよい。今識別された層は、従来技術において知られている。これらの層の詳細な説明は当業者にとって入手可能であり、簡明にするために本明細書では説明しない。

【００８０】

図6は、クライアントデバイス602およびP-GW606内に実装されたプロトコルスタック内の新しい層をさらに示す。すなわち、クライアントデバイス602内のユーザプレーンセキュリティ(UP-SEC)層656およびP-GW606内のUP-SEC層658は新しい。これらの層に対する代替名称が容認されている。UP-SEC層656は、K_{P-GW}鍵660に基づいて(たとえば、$K_{P-GWenc}$、$K_{P-GWint}$を使用して)導出された鍵を使用して、クライアントデバイス602のIPパケット(たとえば、IPメッセージ)を暗号化および/または認証する役目を果たしてよい。アクセスノード604は、暗号化および/または保全性保護されると、IPメッセージを解読することはできず、メッセージをP-GW606に転送することだけしかできない。K_{P-GW}鍵660に基づいて導出された鍵は、クライアントデバイス602およびP-GW606によってのみ共有され、アクセスノード604に対して利用可能ではないので、P-GW606だけが、メッセージを解読および/

または認証することができる。同じことが、反対の方向においても当てはまる。クライアントデバイス602内に実装されたUP-SEC層656は、クライアントデバイス602内に実装されたPDCP層612より高い。P-GW606のUP-SEC層658は、P-GW606のGTP-U層638より高い。アクセスノード604とP-GW606との間にIPSECトンネルの必要性はないが、ネットワークは、UP-SEC層656、658内のK_{P-GW}鍵660を用いてメッセージを保護することに加えて、IPSECトンネルを随意に実装してもよい。たとえば、P-GW606は、受信されるメッセージが所与のアクセスノード604から受信されていることを検証するためにIPSECを使用してよい。しかしながら、IPSECは、ユーザプレーンセキュリティのために依存される必要はない。したがって、クライアントデバイス602およびP-GW606は、共有されるK_{P-GW}鍵660に基づいて導出された共有鍵(たとえば、$K_{P-GWenc}$、$K_{P-GWint}$)を使用してユーザプレーントラフィック内のメッセージに対する暗号化(機密保持)および/または保全性保護を提供することができる。

【００８１】

本明細書で説明する態様では、アクセスノード604は、クライアントデバイス602とP-GW606との間のユーザプレーンセキュリティ(UP-SEC)保護の新しい態様が有効にされているかどうかに基づいて、メッセージの暗号化および/または認証を行わせられてよく、または行うように構成されてもよい。オーバーヘッドは、このオプションの使用によって回避され得る。より正確には、クライアントデバイス602とP-GW606との間のUP-SEC保護の新しい態様が有効にされていない場合、アクセスノード604は、現在の4Gのやり方と同様の振舞いを実行してよい。クライアントデバイス602とP-GW606との間のUP-SEC保護の新しい態様が有効にされる場合、IP層内のメッセージは、第1の共有鍵、K_{P-GW}鍵660(ここでK_{P-GW}鍵660は、共有鍵、$K_{P-GWenc}$および$K_{P-GWint}$を導出するために使用されてよい)に基づいて暗号化/解読されてよく、および/または認証/保全性検証されてよい。加えて、PDCP層内のメッセージは、第2の共有鍵、K_{eNB}鍵652(ここでK_{eNB}鍵652は、共有鍵、K_{UPenc}およびK_{UPint}を導出するために使用されてよい)に基づいて随意に、暗号化/解読されてよく、および/または認証/保全性検証されてよい。上記で説明したように、K_{eNB}鍵652の導出は、MMEに知られているK_{ASME}鍵に基づく。しかしながら、本明細書で説明する態様では、MMEは、K_{P-GW}鍵660を提供されない(すなわち、MMEはK_{P-GW}鍵660を認識しない)。実際には、K_{eNB}鍵652およびK_{P-GW}鍵660は相関を持たない-それらは無相関である。K_{P-GW}鍵660の使用に基づくUP-SEC、およびK_{eNB}鍵652の使用に基づくクライアントデバイスとアクセスノードとの間の随意の追加のユーザプレーンセキュリティの特徴は、たとえば、ネットワークごとの構成、またはクライアントデバイス602ごとのベアラごとの構成に基づいて有効/無効にされてよい。

【００８２】

次世代(たとえば、5G)セルラーネットワークの例示的な実際的使用では、暗号化されていないIPメッセージは、4Gセルラーネットワーク内で現在発見される暗号化されていないIPメッセージと同じであってよい。しかしながら、鍵生成ならびにクライアントデバイス602内のUP-SEC層656およびP-GW606内のUP-SEC層658の追加の方法が、本明細書で説明する例示的な次世代セルラーネットワークの態様の中に導入されてよい。クライアントデバイス602内のUP-SEC層656およびP-GW606内のUP-SEC層658は、K_{P-GW}鍵660に基づいて導出された共有鍵(たとえば、$K_{P-GWenc}$、$K_{P-GWint}$)を使用してクライアントデバイス602のIPメッセージを暗号化および/または認証する役目を果たしてよい。本明細書で例示される次世代セルラーネットワークでは、IPメッセージが第1の共有鍵(たとえば、K_{P-GW}鍵660)に基づいて暗号化および/または保全性保護されると、アクセスノード112は、IPメッセージを解読および/または認証することはできない。本明細書で例示される次世代態様では、P-GW606だけが、第1の共有鍵(たとえば、K_{P-GW}鍵660)に基づいて、鍵を使用して暗号化および/または保全性保護されたメッセージを解読および/または認証することができることが好ましい。これは、次世代セルラーネットワークにおいて可能になり得る、4Gセルラーネットワークをしのぐセキュリティの改善を表すことができる。なぜならば、次世代セルラーネットワークでは、クライアントデバイス602およびP-GW606は、K_{P-GW}鍵660に基づいて1つまたは複数の鍵(たとえば、$K_{P-GWenc}$、$K_{P-GWint}$)を共有し得るからである。K_{P-GW}鍵66

0に基づいて、クライアントデバイス602およびP-GW606は、ユーザプレーンのメッセージに機密性および/または保全性を提供することができる。上記で例示したように、アクセスノード604は、第2の共有鍵(たとえば、K_{eNB}鍵652)の使用による第1の共有鍵(K_{P-GW}鍵660)に基づいて、共有鍵を用いて暗号化および/または保全性保護されたメッセージに追加のセキュリティを加えるために随意に使用されてよいことにさらに留意されたい。すなわち、アクセスノード604は、第1の共有鍵(K_{P-GW}鍵660)に基づく鍵を用いて暗号化および/または保全性保護されたメッセージを、第2の共有鍵(K_{eNB}鍵652)に基づく鍵を用いて暗号化および/または保全性保護してよい。次いで、アクセスノード112は、セキュアにされたメッセージをP-GW606に送信してよい。

【００８３】

図7は、図5の例示的な次世代セルラーネットワーク内で実施される鍵階層700である。K鍵702として本明細書で識別されるルート鍵は、クライアントデバイスのユニバーサル加入者識別モジュール(USIM)上に記憶されてよく、また、コアネットワークの認証センター(AuC)において記憶されてもよい。本明細書で説明する態様では、K鍵702は、オーバージエアで送信されない。クライアントデバイスとコアネットワークとの間の認証セッションの間、USIMおよびAuCがそれぞれ所有しているK鍵702に基づいて、USIMおよびAuCはそれぞれ、保全性鍵(IK)、暗号鍵(CK)鍵704と本明細書で総称されるIKおよびCKを独立に導出してよい。IK、CK鍵704は、セッション鍵、より具体的には認可セッション鍵と呼ばれることがある。

【００８４】

認証および鍵合意(AKA)手順の間、IK、CK鍵704は、AuCからHSSに送信されてよい。本明細書で説明する態様では、IK、CK鍵704は、オーバージエアで送信されない。言い換えれば、HSSは、AuCからIK、CK鍵704を取得してよい。クライアントデバイスはすでに、(クライアントデバイスにおいてUSIMによって導出されるIKおよびCK鍵によって)IK、CK鍵704を有する。

【００８５】

クライアントデバイスおよびHSSがそれぞれ(現在の4Gセルラーネットワークにおけるように)K_{ASME}鍵を独立に導出するのではなく、クライアントデバイスおよびHSSはそれぞれ、K_{SKME}鍵706と本明細書で呼ばれる新しい鍵を独立に導出してよく、ここでSKMEは、IK、CK鍵704に基づくセッション鍵管理エンティティを表すことがある。K_{SKME}鍵706は、HSSからMMEに送信されない。代わりに、K_{SKME}鍵706は、HSSからSKME(たとえば、図5、H-SKME528)に送信されてよい。言い換えれば、SKMEは、HSSからK_{SKME}鍵706を取得してよい。本明細書で説明する態様では、K_{SKME}鍵706は、オーバージエアで送信されない。クライアントデバイスはすでに、(クライアントデバイスにおけるIK、CK鍵704に基づいて導出されるK_{SKME}鍵706によって)K_{SKME}鍵706を有する。

【００８６】

クライアントデバイスおよびSKMEはそれぞれ、K_{SKME}鍵706に基づいてK_{ASME}鍵708を独立に導出してよい。K_{ASME}鍵708は、SKMEからMMEに送信されてよい。言い換えれば、MMEは、SKMEからK_{ASME}鍵708を取得してもよい。本明細書で説明する態様では、K_{ASME}鍵708は、オーバージエアで送信されない。今述べたSKMEは、クライアントデバイスがホームネットワークにアタッチされているか、または訪問先ネットワークにアタッチされているかにかかわらず、ローカルSKMEであることに留意されたい。K_{ASME}鍵708は、4GにおけるK_{ASME}鍵と同様であってもよいが、本明細書で説明する態様におけるK_{ASME}鍵708の導出はK_{SKME}鍵706に基づいており、IK、CK鍵704には基づいていないことにも留意されたい。クライアントデバイスはすでに、(クライアントデバイスにおけるK_{SKME}鍵706に基づいてK_{ASME}鍵708を導出することによって)K_{ASME}鍵708を有する。

【００８７】

本明細書で説明する態様におけるSKMEの導入は、(図3に例示する)4G鍵階層の層と比較して、HSSとMMEとの間に追加の鍵階層の層を提供する。

【００８８】

クライアントデバイスおよびMMEはそれぞれ、K_{ASME}鍵708に基づいて非アクセス層暗号化鍵、K_{NASenc}鍵710および非アクセス層保全性鍵、K_{NASint}鍵712を独立に導出してよい。K_{NASenc}鍵710およびK_{NASint}鍵712は、クライアントデバイスとMMEとの間の制御プレーンメッセージを保護することを意図している。そのような保護は、他の要素が、制御プレーン内のメッセージを解読または修正することを防止する。

【００８９】

同じく、クライアントデバイスおよびMMEはそれぞれ、K_{ASME}鍵708に基づいて、K_{eNB}鍵714と本明細書で呼ばれるアクセスノード鍵を独立に導出してよい。K_{eNB}鍵714は、MMEからアクセスノードに送信されてよい。言い換えれば、アクセスノードは、MMEからK_{eNB}鍵714を取得してもよい。クライアントデバイスはすでに、(クライアントデバイスにおけるK_{ASME}鍵708に基づいてK_{eNB}鍵714を導出することによって)K_{eNB}鍵714を有する。本明細書で説明する態様では、K_{eNB}鍵714は、オーバージエアで送信されない。

【００９０】

この点において、クライアントデバイスおよびアクセスノードはそれぞれ、K_{eNB}鍵714として識別される鍵を所有する。言い換えれば、クライアントデバイスおよびアクセスノードは、K_{eNB}鍵714を共有する。

【００９１】

K_{eNB}鍵714を含むブロック内で、ネクストホップ(NH)カウンタへの参照がなされる。NHカウンタの機能は上記で説明されており、簡明さのために繰り返さない。

【００９２】

K_{eNB}鍵714を使用して、クライアントデバイスおよびアクセスノードは、4つの異なる鍵を独立に導出してよい。4つの可能性のある鍵は、K_{UPint}鍵716と呼ばれるユーザプレーン保全性鍵、K_{UPenc}鍵718と呼ばれるユーザプレーン暗号化鍵、K_{RRCint}鍵720と呼ばれる制御プレーン保全性鍵、およびK_{RRCenc}鍵722と呼ばれる制御プレーン暗号化鍵を含む。下付き文字「enc」を有する鍵は、暗号化のために使用される。下付き文字「int」を有する鍵は、保全性のために使用される。K_{UPint}鍵716およびK_{UPenc}鍵718はそれぞれ、クライアントデバイスとアクセスノードとの間でオーバージエアで転送されるメッセージに対するユーザプレーンデータの、保全性保護および暗号化のために使用される。K_{UPint}鍵716およびK_{UPenc}鍵718は、クライアントデバイスとアクセスノードとの間のPDCP層内のメッセージを暗号化/保全性保護するために使用されてよい。K_{RRCint}鍵720およびK_{RRCenc}鍵722はそれぞれ、無線リソース制御(RRC)データの、保全性保護および暗号化のために使用される。

【００９３】

加えて、別の鍵が、K_{SKME}鍵706に基づいて導出されてよい。図7の右側に示す追加の鍵は、K_{P-GW}鍵724と呼ばれることがある。K_{P-GW}鍵724およびK_{SKME}鍵706は、4Gセルラーネットワークの特徴と比較して、次世代セルラーネットワークにおける新しい特徴であってよい。クライアントデバイスおよびSKMEはそれぞれ、K_{SKME}鍵706に基づいてK_{P-GW}鍵724を独立に導出してよい。SKMEは、K_{P-GW}鍵724をP-GWに提供してよい。本明細書で説明する態様では、K_{P-GW}鍵724は、オーバージエアで送信されない。K_{P-GW}鍵724は、クライアントデバイスとP-GWの両方が同じ鍵を所有するという点で、共有鍵である。言い換えれば、その鍵が共有されるのは、両エンティティが、それら自体で独立に導出または取得された鍵のコピーを所有するからであり、一方のエンティティが他方のエンティティにその鍵のコピーを分配したからではなく、またはその鍵の導出もしくは生成について他方のエンティティと交渉したからでもない。K_{P-GW}鍵724の共有は、クライアントデバイスとP-GWとの間のシグナリング、交渉、または対話を必要としない。K_{P-GW}鍵724は、クライアントデバイスが、訪問先ドメイン(たとえば、V-P-GW)内のP-GWを介してパケットデータネットワーク(たとえば、インターネット)に接続される場合、訪問先SKME(V-SKME)によって提供されることに留意されたい。クライアントデバイスがホームP-GW(たとえば、H-P-GW)を介してパケットデータネットワークに接続される場合、K_{P-GW}はホームSKME(H-SKME)によって提供されるべきである。H-P-GW(すなわち、ホームドメイン/ホームネットワークP-GW)を使用す

るかまたはV-P-GW(すなわち、訪問先ドメイン/訪問先ネットワークP-GW)を使用するかは、たとえば、クライアントデバイスの加入情報(たとえば、加入プロファイルから)、ならびに/あるいはホームドメインのサービスポリシーおよび/または何らかの他のネットワークアクセスポリシーに基づいてネットワーク事業者によって構成されてよい。

【００９４】

したがって、K_{P-GW}鍵724は、クライアントデバイスとP-GWとの間で共有されてよい。クライアントデバイスおよびP-GWは、K_{P-GW}鍵724に基づいて$K_{P-GWint}$鍵726(保全性鍵)および$K_{P-GWenc}$鍵728(暗号化鍵)を独立に導出してよい。保全性鍵、$K_{P-GWint}$鍵726は、メッセージ認証コードを生成するために使用されてよい。暗号化鍵、$K_{P-GWenc}$鍵728は、暗号化のために使用されてよい。

【００９５】

ネットワークの観点から、アクセスノードは、層2(L2)接続点であってよく、すなわち、MAC/PHY層をサポートする一方で、P-GWは、層3(L3)接続点、すなわちIP層であってよい。アクセスノードおよびP-GWの2つはコロケートされる必要はなく、L2接続点は変化し得るが、L3接続点は同じままである。

【００９６】

本明細書のいくつかの態様において第2の共有鍵と呼ばれることがあるK_{P-GW}鍵714は、ユーザプレーン層2のオーバージエアメッセージを保護するために使用されてよい。ユーザプレーン層2のオーバージエアメッセージは、パケットデータ収束プロトコル(PDCP)層内に存在してよい。本明細書のいくつかの態様において第1の共有鍵と呼ばれることがあるK_{P-GW}鍵724は、ユーザプレーン層3のメッセージを保護するために使用されてよい。ユーザプレーン層3のメッセージは、インターネットプロトコル層(IP層)(たとえば、図6、IP層610、650)、またはユーザプレーンセキュリティ(UP-SEC)層(たとえば、図6、656、658)の中に存在してよい。

【００９７】

いくつかの態様では、K_{P-GW}鍵724は、たとえば、K_{SKME}鍵706と、特定のゲートウェイの識別子(GW ID)との関数(たとえば、$K_{P-GW}=F(K_{SKME}、GW\ ID)$)であってよい。MMEは、セッション確立中に、クライアントデバイスにGW IDを通知する。関数Fは、鍵導出関数であってよい。

【００９８】

図8は、本開示の態様による、制御プレーンおよびユーザプレーンに従って要素をグループ化する例示的な次世代(たとえば、5G)セルラーネットワーク800の要素を示す。図8では、トンネルまたはパイプライン822、824、826の図式表現が、セキュアな信号経路を表すために使用されている。図8は、コアネットワーク802の要素を示す。図8はまた、クライアントデバイス806とワイヤレスに通信中であり得るアクセスノード804を示す。コアネットワーク802は、HSS808、SKME809、MME810、S-GW812、およびP-GW814を含む。アクセスノード804は、RRC816エンティティ(制御プレーン内で発見されるエンティティ)、PDCP/RLCエンティティ818、およびIPエンティティ820(PDCP/RLCおよびIPのエンティティはユーザプレーン内で発見される)を含む。図8は、ホームネットワーク接続シナリオにおけるクライアントデバイスに関する。

【００９９】

図8は、いくつかの導出された暗号化鍵の使用を視覚的に示す。図8の態様によれば、SKME809は、セッション鍵管理エンティティ鍵(K_{SKME}鍵811)に対するローカルトラストアンカーまたはローカル鍵アンカーである。MME810は、K_{ASME}鍵813に対するローカルトラストアンカーまたはローカル鍵アンカーである。

【０１００】

MME810とクライアントデバイス806との間のパイプライン822は、MME810とクライアントデバイス806との間の制御プレーンメッセージが、K_{NASenc}鍵およびK_{NASint}暗号化鍵のセキュリティを用いて送信されることを示す。図7に関して上記で説明したように、クライアントデバイス806およびMME810はそれぞれ、K_{ASME}鍵813に基づいて非アクセス層暗号化K

K_{NASenc}鍵および非アクセス層保全性K_{NASint}鍵を独立に導出してよい。具体的には、HSS808は、K_{SKME}鍵811をSKME809に送信し、SKME809は、K_{SKME}鍵811に基づいてK_{ASME}鍵813を導出してK_{ASME}鍵813をMME810に送信し、MME810は、K_{ASME}鍵813に基づいてK_{NASenc}およびK_{NASint}暗号化鍵(パイプライン822参照)を導出する。

【０１０１】

クライアントデバイス806とP-GW814との間のパイプライン824は、クライアントデバイス806とP-GW814との間のユーザプレーンメッセージが、K_{P-GW}暗号化鍵のセキュリティを用いて送信されることを示す。図7に関して上記で説明したように、クライアントデバイス806およびSKME809はそれぞれ、K_{SKME}鍵811に基づいてK_{P-GW}鍵を独立に導出してよい。SKMEは、P-GW814にK_{P-GW}鍵を提供してよい。具体的には、HSS808は、K_{SKME}鍵811をSKME809に送信し、SKME809は、K_{SKME}鍵811に基づいてK_{P-GW}鍵を導出して、K_{P-GW}鍵をP-GW814に送信する。クライアントデバイス806とP-GW814との間のメッセージは、第1の共有鍵、K_{P-GW}鍵(パイプライン824参照)のセキュリティを用いて送信される。

【０１０２】

クライアントデバイス806とアクセスノード804のPDCP/RLCエンティティ818との間のパイプライン824を取り巻くパイプライン826は、第2の共有鍵、K_{eNB}鍵が、K_{P-GW}鍵に基づいてすでに暗号化および/または認証されているメッセージを暗号化および/または認証するために随意に使用されてよいことを示す。随意の第2の暗号化および/または認証は、メッセージがアクセスノード804とクライアントデバイス806との間でアップリンクまたはダウンリンクのいずれかの方向で送信されるときに、そのメッセージに対して利用可能であり得る。

【０１０３】

上記のように、SKME809は、K_{P-GW}鍵と呼ばれる鍵を導出する役目を果たすことができる。クライアントデバイス806は、場合によっては、それ自体とAuCとの間で共有されるルート鍵、Kに基づいてあらゆる鍵を導出することができ、そのゆえクライアントデバイス806は、K_{P-GW}も導出し得るが、P-GW814は、クライアントデバイス806のデータ接続のためにK_{P-GW}鍵を導出することはできない。そのために、SKME809は、K_{SKME}鍵811に基づいてK_{P-GW}鍵を導出して、K_{P-GW}鍵を、たとえば制御プレーン信号経路828を介してP-GW814に送信してよい。したがって、クライアントデバイス806およびP-GW814は、鍵、K_{P-GW}鍵を共有する。2つのエンティティが鍵を共有するとき、2つのエンティティは、何らかの手段によって接続をセキュアにすることができることが理解されよう。

【０１０４】

4GネットワークにおけるK_{ASME}鍵とは異なり、K_{P-GW}鍵は、MME810に提供されない。K_{P-GW}鍵は、クライアントデバイス806がハンドオーバ中に異なるMMEに移転することがあるので、MME810に提供されない。そのような場合、K_{P-GW}鍵は、第1のMME810から第2のMME(図示せず)に転送される必要がある。しかしながら、次世代セルラーネットワークでは、セキュリティアーキテクチャは、MME810をあまり信頼できないエンティティと見なすように設計されてよい。

【０１０５】

現在4Gセルラーネットワークを使用しているモバイルデバイスよりずっと多くのモバイルデバイスが、次世代セルラーネットワークを使用することになるものと予期されている。一推定によれば、そのモバイルデバイスの数は、10年で100倍に増加する。そのように多数のクライアントデバイスを仮定すれば、MMEの数は劇的に増加する可能性がある。今日、4Gネットワークでは、MMEは、信頼できるエンティティと見なされている。今日、大規模な全国的電話会社は、それらのネットワーク全体をカバーするために、4つのMMEしか必要としない。この数は小さいので、強力なセキュリティが、各MMEに対して確立され得る。たとえば、今日のMMEは、制限されたアクセスを有するセキュアな設備の中に収容され得る。しかしながら、MMEの数が数百まで増加する場合、同レベルのセキュリティを維持することが困難になる可能性が高い。次世代(5G)セルラーネットワークが広く使用されるようになると、MMEの数が増加することが見込まれる。加えて、作業は、「再配置可能

な」MME上で行われていることを理解されたい。これらのタイプのMMEは、速やかなハンドオーバをサポートするために、アクセスノードの近くに配置されることがある。したがって、これは、再配置可能なMMEが公共の場に配置されることがあり、そのことが、攻撃に対するMMEの脆弱性を高めることになることを意味する。これらおよび他の理由で、MME810をあまり信頼できないエンティティとして取り扱うことが望ましい。これは、鍵導出および鍵管理(たとえば、メンテナンス、ストレージ)のために利用され得るSKME809を導入することに対する別の理由であり得る。鍵導出関数には、長さXのハッシュメッセージ認証コード(HMAC)(HMAC-X)が含まれることがあり、ここでXは鍵長さであることに留意されたい。

【０１０６】

したがって、K_{P-GW}は、SKME809によって導出されてP-GW814に提供されてよく、こうして、クライアントデバイス806は、共有鍵、K_{P-GW}に基づいてP-GW814と直接的セキュリティ関係を有することができる。これによって、ユーザプレーンの信頼が、(4Gにおけるアクセスノード804においてではなく)P-GW814においてアンカリングされるという結果がもたらされ得る。言い換えれば、ユーザプレーンデータを保護するために、クライアントデバイス806は、それ自体とP-GW814との間のエンティティ/要素を信頼する必要はなく、または信頼することを要求されることもない。今日、4Gにおいては当然であるように、クライアントデバイス806は、それとP-GW814との間の経路上に存在するアクセスノード804または任意の他のデバイスもしくはルータを信頼する必要はない。

【０１０７】

それにもかかわらず、いくつかの態様では、第1の共有鍵(クライアントデバイス806およびP-GW814によって共有されるK_{P-GW}鍵)に基づくユーザプレーンメッセージの暗号化および/または認証に加えて、クライアントデバイス806はまた、それ自体と次世代(たとえば、5G)セルラーネットワークの他の要素またはエンティティとによって共有される他の鍵を使用して追加の暗号化および/または認証を利用することがある。これらの方法のうちの1つまたは複数において、本明細書で説明する態様は、4Gと比較して、5Gにおいてより良好なユーザプレーンセキュリティを提供することができる。改善されたユーザプレーンセキュリティは、少なくとも第1の共有鍵、K_{P-GW}鍵を共有することによって実現されてよく、それによって、次世代セルラーネットワークは、クライアントデバイス806およびP-GW814におよびそこから伝えられるメッセージに、機密性および保全性保護を提供することができる。

【０１０８】

4Gセルラーネットワークと次世代セルラーネットワークとの間の別の差異は、4Gネットワークでは、K_{UPenc}鍵がK_{eNB}鍵に基づいて導出されることである。K_{UPenc}鍵は、クライアントデバイスとアクセスノードとの間のオーバージエアトラフィックを暗号化するために使用される。これは、オーバージエアトラフィックが保全性保護されないことを意味する。保全性保護のこの欠如は、4G仕様の設計期間中の帯域幅の不足に起因している。次世代(たとえば、5G)セルラーネットワークは、4Gセルラーネットワークのこれらおよび他の欠陥を克服し、全体的に、4Gより良好なセキュリティを提供するように設計され得る。これは、(4Gでは提供されない)ユーザプレーンメッセージに対する保全性保護を提供することを伴う。したがって、ユーザプレーントラフィックに対する保全性保護を提供する特徴などの有用な特徴が、次世代セルラーネットワークにおいて使用され得る。保全性保護は、たとえば暗号化がいくつかの国ではオプションであるのと同様に、オプションであってもよい。いくつかの態様では、クライアントデバイス806およびP-GW814は、それらが、それらの間で伝えられるメッセージを暗号化するべきか、それらの間で伝えられるメッセージに対して保全性保護を与えるべきか、または両方を行うべきかについて取り決めることがある。

【０１０９】

保全性保護

機密性のために、メッセージが暗号化されることがある。受信者がメッセージを暗号化

するために使用した鍵を有する場合、受信者はそのメッセージを解読することができる。受信者が鍵を持たない場合、メッセージは解読され得ず、メッセージの機密性は維持される。しかしながら、いくつかのシナリオでは、中間の攻撃者が、暗号化されたメッセージ中の数ビットだけを変更することがある。中間の攻撃者は、メッセージのコンテンツについて何も知らないが、暗号化されたメッセージを取り込み、1つまたは複数のビットを変更し、そのメッセージを予定受信者に送信することは可能であり得る。次に、受信者はメッセージを解読するが、ビットのうちのいくつかが変更されていることを知らず、受信者はメッセージを信頼する。メッセージをセキュアにするために、(メッセージを暗号化するために使用される)暗号文(cipher)に加えて、メッセージが通過中に修正されているかどうかを受信者が判断することができるように、メッセージが保護されてよい。

【０１１０】

そのような保護を達成するために、メッセージ認証コードが計算/生成/導出/取得されてよく、メッセージが受信者に送信される前に、メッセージの最後に追加されてよい。メッセージ認証コードは、メッセージに対する保全性および真正性の保証を与えるために使用されてよい。保全性保証は偶発的および意図的メッセージ変化(たとえば、メッセージの保全性)を検出する一方で、真正性の保証はメッセージの出所(たとえば、メッセージ創作者の識別情報検証)を確言する。メッセージ認証コードの計算/生成/導出/取得は、$K_{P\text{-}GWint}$などの保全性保護鍵を用いてメッセージを暗号化することを伴うことがある。本明細書で説明するように、$K_{P\text{-}GWint}$は、クライアントデバイスおよびP-GWによって独立に導出されてよい。$K_{P\text{-}GWint}$は、$K_{P\text{-}GW}$鍵に基づいて導出されてよい。$K_{P\text{-}GWint}$は、クライアントデバイスにおいて導出された$K_{P\text{-}GW}$鍵に基づいて、クライアントデバイスによってローカルに導出されてよい。$K_{P\text{-}GWint}$は、SKMEからP-GWによって取得された$K_{P\text{-}GW}$鍵に基づいて、P-GWによってローカルに導出されてよい。したがって、クライアントデバイスとP-GWの両方は、$K_{P\text{-}GWint}$鍵を共有してよい。受信者は送信者によって使用された保全性保護鍵を有する(たとえば、クライアントデバイスとP-GWの両者が$K_{P\text{-}GWint}$を有する)ので、受信者(たとえば、クライアントデバイスまたはP-GW)は、メッセージ認証コードを検証することができる。したがって、受信者は、受信されたメッセージからメッセージ認証コードを計算/生成/導出/取得し、それを、メッセージとともに受信されたメッセージ認証コードと比較することができる。保全性および真正性は、受信者のメッセージ認証コードが送信者のメッセージ認証コードと一致するかどうかを検証されてよい。メッセージ認証は、保全性アルゴリズムを使用して実行されてよいことに留意されたい。保全性アルゴリズムの例には、暗号文ベースのメッセージ認証コード(CMAC)、暗号文ブロック連鎖メッセージ認証コード(CBC-MAC)、鍵付きハッシュメッセージ認証コード(HMAC)、ガロアメッセージ認証コード(GMAC)、および3GPPにおける発展型パケットシステム保全性アルゴリズム1、2または3(EIA1/EIA2/EIA3)が含まれる。

【０１１１】

メッセージの保全性がアクセスノードにおいて検証され得る場合、アクセスノードは、保全性が不足しているメッセージをP-GWに送信する必要はない。メッセージの保全性がP-GWにおいて検証され得る場合、P-GWは、保全性が不足しているメッセージをパケットデータネットワークに送信する必要はない。これは、さもなければ破損したメッセージの送信に使用されることがあるリソースの量を低減することができる。したがって、本明細書で説明する次世代セルラーネットワークのいくつかの態様では、ユーザプレーンにおいて機密性のみを保護する4Gセルラーネットワークをしのぐ、ユーザプレーンにおいて機密性と保全性の両方を保護する利点が実現され得る。

【０１１２】

制御プレーン/ユーザプレーンコールフロー

図9は、本開示の態様による、パケットデータネットワーク(PDN)接続セットアップ中の制御プレーン内の、$K_{P\text{-}GW}$鍵と本明細書で呼ばれる共有鍵の初期のプロビジョニングに関連付けられたコールフロー900、およびユーザプレーン内のKP-GW鍵に基づいて暗号化/認証されたメッセージの後続の通信の一例を示す。図9は、3GPP TS 23.401、図5.10.2-1に

基づく。しかしながら、UP鍵要求918およびUP鍵応答920として識別される新しいコールが、3GPP TS 23.401、図5.10.2-1に示す図に追加されている。

【０１１３】

図9は、デバイス902(たとえば、チップ構成要素、クライアントデバイス)、アクセスノード904(たとえば、eノードB、eNB)、MME906、P-GW908、およびセッション鍵管理エンティティ(SKME)910を示す。デバイスは、PDN接続要求をMMEに送信してよい、912。MMEは、セッション生成要求をP-GWに送信してよい、914。P-GWは、ポリシー制御および課金ルール関数(PCRF)と対話してよい、916。たとえば、P-GWは、IPアドレスを割り当てて、ベアラを準備してよい。PCRFとの対話に伴うステップの詳細な説明は、簡明のために省略されている。P-GWは、(たとえば、P-GWがデバイス902に対するK_{P-GW}を持たない場合)ユーザプレーン(UP)鍵要求をSKMEに送信してよい、918。UP鍵要求は、たとえば、図7のK_{P-GW}鍵724などの鍵を取得するために使用されてよい。次いで、SKMEは、UP鍵応答をP-GWに送信してよい、920。UP鍵応答は、共有鍵、K_{P-GW}を含んでよい。このようにして、P-GWは、共有されたK_{P-GW}鍵をSKMEから取得してもよい。

【０１１４】

次に、P-GWは、セッション生成応答をMMEに送信してよい、922。MMEは、ベアラセットアップ要求/PDN接続受諾をアクセスノードに送信してよい、924。次いで、アクセスノードは、RRC接続再構成要求をデバイスに送信してよい、926。デバイスは、RRC接続再構成完了をアクセスノードに送信してよい、928。アクセスノードは、ベアラセットアップ応答をMMEに送信してよい、930。デバイスは、直接転送をアクセスノードに送信してよい、932。アクセスノードは、PDN接続完了をMMEに送信してよい、934。参照番号912～916および922～934で表されるコールは、当業者には理解されよう。それらのコールの詳細な説明は、簡明のために省略されている。

【０１１５】

UP鍵要求918およびUP鍵応答920として識別される新しいコールが、3GPP TS 23.401、図5.10.2-1に示す図に追加されている。新しいコール、UP鍵要求918およびUP鍵応答920が、本明細書で説明する開示の態様に従って、SKMEにおよびSKMEから行われる。

【０１１６】

P-GWが所与のデバイスに対する共有されたK_{P-GW}鍵を持たない場合、P-GWは、共有鍵をSKMEから要求してよい。要求は、UP鍵要求918の使用によって行われてよい。次いで、SKMEは、K_{P-GW}鍵をP-GWに送信してよい。K_{P-GW}鍵は、UP鍵応答920を使用してP-GWに提供されてよい。

【０１１７】

デバイスが、K_{P-GW}鍵のそれのコピーを導出した後、デバイスは、第1のメッセージをP-GWを介してユーザプレーン内のネットワークに送信してよい、936。第1のメッセージは、共有されたK_{P-GW}鍵に基づいて暗号化および/または認証されてよい。加えて、デバイスは、第2のメッセージをP-GWを介してネットワークから受信してよく938、第2のメッセージは、共有されたK_{P-GW}鍵に基づいて暗号化および/または認証されてよい。デバイスはすでに、共有されたK_{P-GW}鍵のそれのコピーを有するので、デバイスは、受信された第2のメッセージを解読および/または認証することができる。

【０１１８】

いくつかの態様では、ユーザプレーンメッセージを保護するための方法は、メッセージをサイファー化および/または認証するための第1の共有鍵(K_{P-GW})をクライアントデバイスにおいて導出するステップを含んでよく、第1の共有鍵は、クライアントデバイスおよびP-GW(すなわち、パケットデータネットワークへのゲートウェイ)によって共有される。第1のメッセージは、第1の暗号化および/または認証されたメッセージを作成するために、第1の共有鍵を用いて暗号化または認証されてよい。第1の暗号化および/または認証されたメッセージは、クライアントデバイスからアクセスノードにオーバージエアで送信されてよい。さらに他の態様では、第1の共有鍵を用いて第1のメッセージを暗号化および/または認証するステップは、メッセージをサイファー化および/または認証するための第2

の共有鍵をクライアントデバイスにおいて導出するステップを付加的に含んでよく、クライアントデバイスおよびアクセスノードは、第2の共有鍵を共有する。第2の共有鍵は、第1の共有鍵とは異なる。第2の共有鍵と第1の共有鍵とは無相関である。方法は、第2の暗号化および/または認証されたメッセージを作成するために、第1の暗号化および/または認証された第1のメッセージを第2の共有鍵を用いて暗号化および/または認証するステップをさらに含んでよい。第2の暗号化および/または認証されたメッセージは、クライアントデバイスからアクセスノードにオーバージエアで送信されてよい。

【０１１９】

訪問先ネットワーク

図10Aは、制御プレーンおよびユーザプレーンに従って要素をグループ化する例示的な次世代セルラーネットワーク1000の要素を示しており、ユーザプレーンにおいて、P-GWがホームネットワーク内にあり、H-P-GW1010として識別される。図10Aでは、クライアントデバイス1002は、訪問先ネットワーク1015内でMME1018にアタッチされているが、ユーザプレーン内のデータ接続は、クライアントデバイス1002とホームネットワークのH-P-GW1010との間で行われる。ホームネットワーク内のH-SKME1012とH-P-GW1010との間の破線は、制御プレーンインターフェース1034を表す。制御プレーンインターフェース1034は、ユーザプレーン(UP)鍵要求(たとえば、図9、918)およびUP鍵応答(K_{P-GW}を含む)(たとえば、図9、920)を、H-P-GW1010とH-SKME1012との間で移送するために使用されてよい。

【０１２０】

図10Aは、ホームネットワーク1014内のHSS1008、H-P-GW1010、およびホームSKME(H-SKME)1012を示す。図10Aはまた、すべてが訪問先ネットワーク1015内にある訪問先SKME(V-SKME)1016、MME1018、およびS-GW1020を示す。クライアントデバイス1002は、アクセスノード1022を通って訪問先ネットワーク1015に至るワイヤレス通信を有してよい。

【０１２１】

図10Aでは、クライアントデバイス1002は、訪問先ネットワーク1015のMME1018と、訪問先ネットワーク1015に関連付けられたアクセスノード1022とにアタッチされてよい。しかしながら、クライアントデバイス1002は、H-P-GW1010から割り当てられたそれのIPアドレスを有していることがある。そのために、データ接続は、訪問先ネットワーク1015内のクライアントデバイス1002とそれのホームネットワーク1014内のH-P-GW1010との間で行われてよい。H-P-GW1010がクライアントデバイス1002に送信するためのメッセージを有するとき、H-P-GW1010は、そのメッセージを訪問先ネットワーク1015内のS-GW1020に送信してよく、訪問先ネットワーク1015内のS-GW1020は、そのメッセージをクライアントデバイス1002に送信してよい。

【０１２２】

一態様によれば、P-GW(H-P-GW1010)がホームネットワーク1014内にあるとき、クライアントデバイス1002が訪問先ネットワーク1015内にある間、K_{P-GW}鍵が、ホームネットワーク1014から取得されたK_{SKME}鍵1011に基づいて導出されてよい。言い換えれば、ホームネットワーク1014のHSS1008がK_{SKME}鍵1011を導出し、K_{SKME}鍵1011をホームネットワーク1014のH-SKME1012に提供する。次いで、H-SKME1012は、K_{SKME}鍵1011に基づいてK_{P-GW}鍵を導出する。次いで、H-SKME1012は、制御プレーンインターフェース1034を使用してH-P-GW1010にK_{P-GW}鍵を提供してよい。このようにして、ユーザプレーンメッセージは、訪問先ネットワーク1015内のクライアントデバイス1002とホームネットワーク1014内のH-P-GW1010との間の交換のために暗号化および/または認証され得る。その間に、ホームネットワーク1014のHSS1008がK_{SKME}'鍵1013を導出し、K_{SKME}'鍵1013を訪問先ネットワーク1015のV-SKME1016に提供する。K_{SKME}'鍵1013は、HSS1008から、図10Aに示すようにH-SKME1012を介してV-SKME1016に、または(HSS1008とV-SKME1016との間の、図10Bに示していない直接通信を介して)直接V-SKME1016に提供され得る。K_{SKME}'鍵1013は、K_{SKME}鍵1011とは異なる(たとえば、無相関であり、相関していない)。このようにして、各セッション鍵管理エンティティ鍵(たとえば、K_{SKME}鍵1011およびK_{SKME}'鍵1013)は、それ自体のネットワークに結合されるか、または言い換えれば、それ自体のドメインに結合される。K_{SKME}鍵1011は

ホームネットワーク1014に結合され、K_{SKME}'鍵1013は訪問先ネットワーク1015に結合される。K_{SKME}鍵1011およびK_{SKME}'鍵1013は、異なるネットワークに結合されるが、ともに、クライアントデバイス1002に関連して使用される。たとえば、図10Aのシナリオでは、V-SKME1016は、K_{SKME}'鍵1013に基づいてK_{ASME}鍵1019を導出し、K_{ASME}鍵1019を訪問先ネットワーク1015内のMME1018に提供する。ホームネットワーク1014と訪問先ネットワーク1015との間で無相関のセッション鍵管理エンティティ鍵(たとえば、K_{SKME}鍵1011およびK_{SKME}'鍵1013)を使用することで、訪問先ネットワーク1015が、ホームネットワーク1014によって使用されるK_{P-GW}を導出し得ない(すなわち、H-SKME1012によって導出され、制御プレーンインターフェース1034を介してH-P-GW1010に提供されるK_{P-GW}鍵を導出し得ない)ことになることが確実になる。

【０１２３】

図10Bは、制御プレーンおよびユーザプレーンに従って要素をグループ化する例示的な次世代セルラーネットワーク1004の要素を示しており、P-GWは訪問先ネットワーク1017内にあり、V-P-GW1024として識別される。図10Bでは、クライアントデバイス1006は、訪問先ネットワーク1017内のMME1028にアタッチされる。ユーザプレーン内のデータ接続は、クライアントデバイス1006と訪問先ネットワーク1017のV-P-GW1024との間で行われる。訪問先ネットワーク1017内のV-SKME1026とV-P-GW1024との間の破線は、制御プレーンインターフェース1036を表す。制御プレーンインターフェース1036は、ユーザプレーン(UP)鍵要求(たとえば、図9、918)およびUP鍵応答(K_{P-GW}を含む)(たとえば、図9、920)を、V-P-GW1024とV-SKME1026との間で移送するために使用されてよい。

【０１２４】

図10Bは、図10Aのホームネットワーク1014のHSS1008と同じものを示す。図10Bはまた、すべてが訪問先ネットワーク1017内にある訪問先P-GW(V-P-GW1024)、訪問先SKME(V-SKME1026)、MME1028、およびS-GW1030を示す。クライアントデバイス1006は、アクセスノード1032を通って訪問先ネットワーク1017に至るワイヤレス通信を有してよい。

【０１２５】

図10Bに示すように、クライアントデバイス1006が訪問先ネットワーク1017内にあるとき、ローカルSKME(たとえば、V-SKME1026)は、クライアントデバイス1006とローカルP-GW(たとえば、V-P-GW1024)との間の直接的セキュリティ関係を有効にすることを要求されることがある。V-SKME1026はK_{P-GW}を導出し、K_{P-GW}をV-P-GW1024に提供してよい。プロビジョニングは、制御プレーンインターフェース1036を介するものであってよい。この手順を踏むことによって、訪問先ネットワーク1017内のV-SKME1026は、ホームネットワーク1014内でH-P-GW1010を構成する必要がなくなる。これは、訪問先ネットワーク1017のV-SKME1026はH-P-GW1010のドメインとは異なるドメイン(訪問先ネットワーク1017のドメイン)の中にあるので、有利であり得る。訪問先ドメインからのSKME(V-SKME1026)が、どちらかといえば多分、別のドメインのP-GW(H-P-GW1010)を構成する特権を持たないことになる。これは、ホームSKME(H-SKME1012)および訪問先SKME(V-SKME1016、1026)の生成に対する別の有利な理由であり得、ホームSKMEおよび訪問先SKMEはそれぞれ、対応するP-GWを有するドメイン内にあり、同じドメイン内の対応するP-GWを提供することができる。

【０１２６】

一態様によれば、V-P-GW1024が訪問先ネットワーク1017内にあるとき、クライアントデバイス1006が同じく訪問先ネットワーク1017内にある間、K_{P-GW}鍵が、訪問先ネットワーク1017から取得されたK_{SKME}鍵1027に基づいて導出されてよい。言い換えれば、ホームネットワーク1014のHSS1008はK_{SKME}鍵1027を導出し、K_{SKME}鍵1027を訪問先ネットワーク1017のV-SKME1026に提供することになる(たとえば、図10Bのシナリオでは、HSS1008はV-SKME1026と直接通信してよい)。次いで、V-SKME1026は、K_{SKME}鍵1027に基づいてK_{P-GW}鍵を導出することになる。次いで、V-SKME1026は、制御プレーンインターフェース1036を介してV-P-GW1024にK_{P-GW}を提供することになる。このようにして、ユーザプレーンメッセージは、訪問先ネットワーク1017内のクライアントデバイス1006と訪問先ネットワーク1017内のV-P-GW1024との間の交換のために暗号化および/または認証され得る。

【０１２７】
要約すれば、H-P-GW1010がクライアントデバイス1002のユーザプレーントラフィックをアンカリングするために使用されるとき、H-SKME1012は、K_{P-GW}鍵をH-P-GW1010に(制御プレーンインターフェース1034を介して)提供するために使用される。V-P-GW1024がクライアントデバイス1006のユーザプレーントラフィックをアンカリングするために使用されるとき、V-SKME1026は、K_{P-GW}鍵をV-P-GW1024に(制御プレーンインターフェース1036を介して)提供するために使用される。ホームドメインおよび訪問先ドメインのK_{P-GW}鍵は、無相関の異なる鍵である。

【０１２８】
鍵の転送、たとえばK_{P-GW}の転送は、セッション生成要求の間に発生してよい。たとえば、図10Bにおいて、MME1028は、クライアントデバイス1006の訪問先ネットワーク1017への接続の間にベアラをセットアップするために、セッション生成要求を送信してよい。セッション生成要求は、V-P-GW1024(たとえば、訪問先ネットワーク1017のP-GW)まで進んでよい。V-P-GW1024がクライアントデバイス1006に対するK_{P-GW}鍵を持たない場合、V-P-GW1024は、ローカルSKME(たとえば、訪問先ネットワーク1017内のSKME、V-SKME1026)からK_{P-GW}を取得するための要求を送信してよい。この意味では、クライアントデバイス1006が、データ接続のためにホームネットワークを使用している(ここでH-P-GW1010はH-SKME1012からK_{P-GW}鍵を取得する)か、またはデータ接続のために訪問先ネットワーク1017を使用している(ここでV-P-GW1024はV-SKME1026からK_{P-GW}鍵を取得する)かの間に整合性が存在する。

【０１２９】
たとえば、図10Bでは、訪問先ネットワーク1017内のクライアントデバイス1006は、訪問先ネットワーク1017のV-P-GW1024を通してデータ接続を行うことを許容され得る。訪問先ネットワーク1017のV-P-GW1024は、訪問先ネットワーク1017のV-SKME1026からK_{P-GW}鍵を取得してよい。さらなる例として、それのプロバイダとして企業Yを有する一ユーザが欧州を旅行している場合、そのユーザは、(欧州における)企業Xのネットワークに接続されることがある。そのユーザは、企業XのP-GW(たとえば、V-P-GW1024)を通してメッセージを送信するためのオプションを有することがある。これは、クライアントデバイス1006が、ローミングパートナーのネットワーク(すなわち、訪問先ネットワーク1017)内でローミングする場合、訪問先ネットワーク1017のV-P-GW1024を使用し得るときに可能になる。クライアントデバイス1006が、旅行中に訪問先ネットワーク1017のV-P-GW1024を使用するように構成されている場合、ローカルSKME(たとえば、V-SKME1026)は、それのネットワークのV-P-GW1024を構成してよく、それによってクライアントデバイス1006とV-P-GW1024との間で、K_{P-GW}鍵に基づくセキュリティを用いたメッセージの交換が可能になる。図10Bの例では、H-SKME1012はユーザに対して利用可能でないので(たとえば、ユーザは外国を旅行中であるので)、H-SKME1012は含まれないことに留意されたい。

【０１３０】
そのために、図10Bでは、クライアントデバイス1006がアクセスノード1032から別のアクセスノード(図示せず)にハンドオフされている場合、訪問先ネットワーク1017内のMME1028は、各転送の間(およびクライアントデバイス1006接続の間)にベアラをセットアップしてよく、次いで、メッセージは、クライアントデバイス1006からV-P-GW1024まで進むことができる。しかしながら、V-P-GW1024がクライアントデバイス1006に関連付けられたK_{P-GW}を持たない場合、V-P-GW1024は、ローカルSKME、すなわちV-SKME1026を通してK_{P-GW}を要求してよい。

【０１３１】
本明細書で説明する態様を実施することによって、ユーザプレーンセキュリティは、余分なセキュリティメカニズム(たとえば、オーバージエアインターフェースセキュリティ(たとえば、K_{UPenc})およびクライアントデバイスとP-GWとの間のセキュリティトンネル(たとえば、IPSEC))に依存しなくてよい。危険にさらされたアクセスノードが、ユーザプレーンセキュリティを破ることはない。アクセスノードは、オーバージエアユーザプレーン

トラフィックの機密性および保全性の保護を維持する。HSSとMMEとの間のSKMEをローカルトラストアンカーまたはローカル鍵アンカーとして導入することで、将来の新しいネットワーク関数のための柔軟なさらなる鍵導出が可能になる。いくつかの態様によれば、SKMEは、鍵導出、維持、およびネットワーク要素(たとえば、MME、アクセスノード、P-GW)への鍵の提供に対してのみ、役目を果たすことができる。

【０１３２】

追加の態様

図11は、本明細書で説明する態様による、次世代セルラーネットワーク内でユーザプレーンメッセージ(たとえば、ユーザプレーンデータトラフィック)のセキュリティおよび/または保全性を保護するための、クライアントデバイスにおいて動作可能な例示的な方法1100を示す。

【０１３３】

ユーザプレーン内のメッセージのサイファー化(暗号化/解読)および/または認証の根拠を置く共有鍵(たとえば、K_{P-GW})は、クライアントデバイスおよび第2のエンティティによって独立に導出されてよく、ここで第2のエンティティは、共有鍵をセルラーネットワークとパケットデータネットワークとの間のゲートウェイ(たとえば、P-GW)に提供する、1102。

【０１３４】

メッセージは、クライアントデバイスからセルラーネットワークに関連付けられたアクセスノードを介してゲートウェイに送信されてよく、ここでメッセージは、共有鍵(たとえば、K_{P-GW})に基づいて暗号化されたものおよび認証されたもののうちの少なくとも1つであり、共有鍵は、クライアントデバイスおよびゲートウェイによって共有される、1104。

【０１３５】

クライアントデバイスは、パケットデータネットワークからゲートウェイおよびアクセスノードを介してメッセージを受信してよく、ここでメッセージは、共有鍵を有するゲートウェイによって暗号化されたものおよび認証されたもののうちの少なくとも1つである、1106。

【０１３６】

図12は、本明細書で説明する態様による、次世代セルラーネットワーク内でユーザプレーンメッセージ(たとえば、ユーザプレーンデータトラフィック)のセキュリティおよび/または保全性を保護するための、クライアントデバイスにおいて動作可能な例示的な方法1200を示す。

【０１３７】

クライアントデバイスおよびHSSは、K_{SKME}鍵を独立に導出してよい、1202。

【０１３８】

HSSは、K_{SKME}鍵をSKMEに提供してよい、1204。

【０１３９】

クライアントデバイスおよびSKMEは、K_{SKME}鍵に基づいてK_{P-GW}鍵を独立に導出してよい、1206。共有されたK_{P-GW}鍵の導出は、K_{SKME}およびゲートウェイの識別子(GW ID)の関数であり得る。たとえば、$K_{P-GW}=F(K_{SKME}、GW\ ID)$。

【０１４０】

共有鍵、K_{P-GW}は、SKMEによってセルラーネットワークとパケットデータネットワークとの間のゲートウェイ(たとえば、GW IDによって識別されるゲートウェイ)に提供されてよい、1208。

【０１４１】

図13は、本明細書で説明する態様による、次世代セルラーネットワーク内でユーザプレーンメッセージ(たとえば、ユーザプレーンデータトラフィック)のセキュリティおよび/または保全性を保護するための、クライアントデバイスにおいて動作可能な例示的な方法1300を示す。

【０１４２】
クライアントデバイスのUSIM(またはクライアントデバイス内のセキュアなプロセス)は、それが保有する認証セッション鍵、Kに基づいて保全性鍵(IK)およびサイファー化鍵(CK)を導出する。認証センター(AuC)は、それが保有する認証セッション鍵、Kと同等のインスタンスを有する。AuCは、それが保有する同等の認証セッション鍵、Kに基づいて保全性鍵(IK)およびサイファー化鍵(CK)を独立に導出する。両認証鍵、Kは同等であり、そのためにIK鍵とCK鍵とは同等である。AuCは、IK、CK鍵をHSSに提供する。クライアントデバイスおよびHSSは、今や、共有された秘密(たとえば、IK、CK)を保有する、1302。
【０１４３】
クライアントデバイスおよびHSSは、共有された秘密(たとえば、IK、CK)に基づいてK_{SKME}鍵を独立に導出する、1304。K_{SKME}は、クライアントデバイスとHSSとの間の共有された秘密(SS)の、およびサービングネットワーク識別子(SN_ID)の関数Fであってよい。たとえば、K_{SKME}=F(SS、SN_ID)。関数Fは、HMAC-xなどの鍵導出関数であってよく、ここでxは鍵長さ、たとえばHMAC-256、HMAC-384であってよい。
【０１４４】
HSSは、K_{SKME}鍵をセッション鍵管理エンティティ(SKME)に提供してよい、1306。
【０１４５】
クライアントデバイスおよびSKMEは、K_{SKME}鍵に基づいてK_{ASME}鍵を独立に導出してよい、1308。並行して、クライアントデバイスおよびSKMEは、K_{SKME}鍵に基づいてK_{P-GW}鍵を独立に導出してよい、1310。
【０１４６】
SKMEは、K_{ASME}鍵をモビリティ管理エンティティ(MME)に提供してよい、1312。並行して、SKMEは、K_{P-GW}鍵をゲートウェイ(たとえば、P-GW)に提供してよい、1314。したがって、クライアントデバイスおよびゲートウェイ(たとえば、P-GW)は、K_{P-GW}鍵を共有する。
【０１４７】
クライアントデバイスおよびMMEは、K_{ASME}鍵に基づいてK_{eNB}鍵を独立に導出してよい、1316。MMEは、K_{eNB}鍵をアクセスノードに提供してよい、1318。したがって、クライアントデバイスおよびアクセスノードは、K_{eNB}鍵を共有する。
【０１４８】
図14は、本明細書で説明する態様による、次世代セルラーネットワーク内でユーザプレーンメッセージ(たとえば、ユーザプレーンデータトラフィック)のセキュリティおよび/または保全性を保護するための、クライアントデバイスにおいて動作可能な例示的な方法1400を示す。
【０１４９】
ユーザプレーン内のメッセージのサイファー化(暗号化/解読)および/または認証の根拠を置く共有鍵(たとえば、K_{P-GW})は、クライアントデバイスおよび第2のエンティティによって独立に導出されてよく、ここで第2のエンティティは、共有鍵をセルラーネットワークとパケットデータネットワークとの間のゲートウェイ(たとえば、P-GW)に提供する、1402。
【０１５０】
メッセージは、クライアントデバイスからネットワークに送信されてよく、ここでメッセージは、共有鍵(たとえば、K_{P-GW})に基づいて暗号化されたものおよび認証されたもののうちの少なくとも1つであり、メッセージの暗号化および認証は、たとえば、IPSEC、トランスポート層セキュリティ事前共有鍵(TLS-PSK)、またはデータグラムTLS-PSK(DTLS-PSK)を使用してよく、共有鍵は、クライアントデバイスおよびゲートウェイ(P-GW)によって共有される、1404。
【０１５１】
クライアントデバイスは、ネットワークからメッセージを受信してよく、ここでメッセージは、共有鍵に基づいて暗号化されたものおよび認証されたもののうちの少なくとも1つであり、メッセージの暗号化または認証は、IPSEC、DTLS-PSK、またはTLS-PSKを使用し

た、1406。加えて、暗号化および認証が有効にされるとき、暗号化および認証は、P-GWと共有される共有鍵(たとえば、K_{P-GW})を使用して実行されてよい。さらに、暗号化と認証の両方が有効にされる場合、追加データを有する認証暗号化(AEAD)暗号文が、ゲートウェイを伴う共有鍵(たとえば、K_{P-GW})を用いて使用されてよい。例示的なAEAD暗号文は、ガロア/カウンタモード(GCM)における高度暗号化規格(AES)(すなわち、AES-GCM)と、暗号文ブロック連鎖を有するカウンタ(CBC)-メッセージ認証コード(CBC-MAV)モード(CCM)における高度暗号化規格(AES)(すなわち、AES-CCM)とを含む。AEAD暗号文の記載およびそれの例は例示であって限定するものではなく、他の暗号文が使用されてよいことが理解されよう。さらに、IPSECは、データパケットの暗号化および認証のための1つのオプションである。IPSECは、鍵セットアップ段階中に2つの通信相手の間で共有鍵を確立する鍵合意プロトコルを含む。

【０１５２】

図15は、本明細書で説明する態様による、次世代セルラーネットワーク内でユーザプレーンメッセージ(たとえば、ユーザプレーンデータトラフィック)のセキュリティおよび/または保全性を保護するための、クライアントデバイスにおいて動作可能な例示的な方法1500を示す。

【０１５３】

ユーザプレーン内のメッセージ(たとえば、ユーザプレーンデータトラフィック)のサイファー化(暗号化/解読)および/または認証の根拠を置く第1の共有鍵(たとえば、K_{P-GW})は、クライアントデバイスおよび第2のエンティティ(たとえば、SKME)によって独立に導出されてよく、ここで第2のエンティティは、第1の共有鍵をセルラーネットワークとパケットデータネットワークとの間のゲートウェイ(たとえば、パケットデータネットワークゲートウェイ(P-GW))に提供する、1502。

【０１５４】

ユーザプレーン内のメッセージ(たとえば、ユーザプレーンデータトラフィック)のサイファー化(暗号化/解読)および/または認証の根拠を置く第2の共有鍵(たとえば、K_{eNB})は、クライアントデバイスおよび第3のエンティティ(たとえば、MME)によって独立に導出されてよく、ここで第3のエンティティは、第2の共有鍵をアクセスノード(たとえば、eノードB)に提供する、1504。

【０１５５】

第1のメッセージは、アクセスノード(たとえば、eノードB)を介してクライアントデバイスによってゲートウェイ(たとえば、P-GW)から受信されてよく、ここで第1のメッセージは、第1の共有鍵(たとえば、K_{P-GW})に基づいて暗号化されたものおよび認証されたもののうちの少なくとも1つであり、第1のメッセージは、第2の共有鍵(たとえば、K_{eNB})に基づいて暗号化されたものおよび認証されたもののうちの少なくとも1つである第2のメッセージの中にさらにカプセル化される、1506。

【０１５６】

第2のメッセージは解読されてよく、第2のメッセージの認証タグは、第2の共有鍵の使用に基づいて(たとえば、K_{UPenc}および/またはK_{UPint}はK_{eNB}に基づいて導出されてよい)検証されてよい、1508。

【０１５７】

したがって、(第2のメッセージが解読されたので)もはや第2のメッセージ内にカプセル化されていない第1のメッセージは、第1の共有鍵の使用に基づいて(たとえば、$K_{P-GWenc}$および/または$K_{P-GWint}$はK_{P-GW}に基づいて導出されてよい)解読および/または認証されてよい、1510。

【０１５８】

図16は、本明細書で説明する態様による、次世代セルラーネットワーク内でユーザプレーンメッセージ(たとえば、ユーザプレーンデータトラフィック)を保護するための、デバイス(たとえば、チップ構成要素、クライアントデバイス)において動作可能な例示的な方法1600を示す。

【０１５９】
方法は、ユーザプレーンメッセージの暗号化および/または認証の根拠を置く第1の共有鍵を、デバイスにおいて取得するステップを含んでよく、第1の共有鍵は、デバイスとパケットデータネットワークへのゲートウェイとによって共有され、デバイスは、ゲートウェイとは独立に、第1の共有鍵を取得する、1602。
【０１６０】
方法は、第1の暗号化および/または認証されたメッセージを作成するために、第1の共有鍵に基づいて第1のメッセージを暗号化および/または認証するステップをさらに含んでよい、1604。
【０１６１】
方法は、第1の暗号化および/または認証されたメッセージを、セルラーネットワークのアクセスノードを介してデバイスからゲートウェイにオーバージエアで送信するステップをさらに含んでよい、1606。
【０１６２】
場合によっては、方法は、メッセージの暗号化および/または認証の根拠を置く第2の共有鍵を、デバイスにおいて導出するステップをさらに含んでよく、第2の共有鍵はデバイスおよびアクセスノードによって共有され、第2の共有鍵は第1の共有鍵とは異なる、1608。デバイスは、アクセスノードとは独立に第2の共有鍵を取得してもよい。第1の共有鍵(たとえば、K_{P-GW})および第2の共有鍵(たとえば、K_{eNB})は無相関である。
【０１６３】
場合によっては、方法は、第2の暗号化および/または認証されたメッセージを作成するために、第2の共有鍵に基づいて第1の暗号化および/または認証されたメッセージを暗号化および/または認証するステップをさらに含んでよく、第1の暗号化および/または認証されたメッセージは、ゲートウェイに送信するために第2の暗号化および/または認証されたメッセージの中にカプセル化される、1610。
【０１６４】
図17は、本明細書で説明する態様による、次世代セルラーネットワーク内でユーザプレーンメッセージ(たとえば、ユーザプレーンデータトラフィック)のセキュリティおよび/または保全性を保護するための、たとえばアクセスノードにおいて動作可能な例示的な方法1700を示す。
【０１６５】
メッセージは、アクセスノードからクライアントデバイスに送信されてよく、メッセージは暗号化されたものおよび保全性保護されたもののうちの少なくとも1つであり、暗号化および認証は、クライアントデバイスと共有されている共有鍵を使用するクライアントデバイスと一致するアルゴリズムに基づく、1702。暗号化および認証は、追加または代替として、ネットワークごと、またはネットワーク事業者ごとの構成に基づいてよい。暗号化および認証は、追加または代替として、クライアントデバイスごとのベアラごとの構成に基づいてよい。暗号化および認証は、追加または代替として、たとえばベアラセキュリティ構成ごとのベアラ構成の一部に基づいてよい。
【０１６６】
メッセージは、クライアントデバイスからアクセスノードにおいて受信されてよく、メッセージは、暗号化されたものおよび保全性保護されたもののうちの少なくとも1つである、1704。
【０１６７】
メッセージが正しく解読されるか、または有効な認証タグを搬送する場合、メッセージは、ネットワーク上のノードからゲートウェイに転送されてよい、1706。
【０１６８】
図18は、本明細書で説明する態様による、セルラーネットワーク内でユーザプレーンメッセージ(たとえば、ユーザプレーンデータトラフィック)を保護するための、アクセスノード(たとえば、eノードB)において動作可能な例示的な方法1800を示す。

【０１６９】
方法は、パケットデータネットワークへのゲートウェイ(たとえば、P-GW)を介してパケットデータネットワークからデバイスに宛てられた、またはデバイスからP-GWに宛てられた第1のメッセージを、アクセスノードにおいて受信するステップを含んでよい、1802。第1のメッセージはすでに、デバイスおよびP-GWによって共有される第1の共有鍵を用いて、デバイスとP-GWとの間での送信中にセキュアにされていてもよい。方法は、デバイスとP-GWとの間にすでにセキュリティが存在するか否かに基づいて、第1のメッセージをさらにセキュアにするかどうかをアクセスノードに示す構成情報をMMEから受信するステップをさらに含んでよい、1804。
【０１７０】
たとえば、第1のメッセージがデバイスおよびゲートウェイによって共有される第1の共有鍵を用いてセキュアにされていない場合、MMEは、第1の暗号化されたメッセージを作成するために、第1のメッセージがデバイスおよびアクセスノードによって共有される第2の共有鍵を用いてセキュアにされるべきであることを、構成情報を通して示してよい。しかしながら、第1のメッセージがすでにデバイスおよびP-GWによって共有される第1の共有鍵を用いてセキュアにされている場合、MMEは、第1のメッセージが追加のセキュリティなしにアクセスノードからデバイスにオーバージエアで送信されてよいことを、構成情報を通して示してよい。さらなるセキュリティは、要求されないが随意に実施されてもよい。同様に、反対方向において、MMEは、デバイスとP-GWとの間にすでにセキュリティが存在するか否かに基づいて、第1のメッセージをさらにセキュアにするかどうかをアクセスノードに示してよい。次いで、第1のメッセージは、MMEからの構成情報に基づいて、さらなるセキュリティを伴ってまたは伴わずにアクセスノードから送信されてよい、1806。
【０１７１】
図19は、本明細書で説明する態様による、次世代セルラーネットワーク内でユーザプレーンメッセージのセキュリティおよび/または保全性を保護するための、P-GWにおいて動作可能な例示的な方法1900を示す。
【０１７２】
共有鍵(たとえば、K_{P-GW})の要求が、パケットデータネットワークゲートウェイ(たとえば、P-GW)からセッション鍵管理エンティティ(SKME)になされてよく、ここで鍵はクライアントデバイスと共有される、1902。
【０１７３】
共有鍵(たとえば、K_{P-GW})は、SKMEからP-GWにおいて受信されてよい、1904。
【０１７４】
P-GWは、メッセージをクライアントデバイスに送信してよく、メッセージは、共有鍵(たとえば、K_{P-GW})に基づいて暗号化および/または認証される、1906。言い換えれば、メッセージは、共有鍵に基づいて導出された鍵(たとえば、$K_{P-GWenc}$、$K_{P-GWint}$)を使用して暗号化および/または認証されてよい。
【０１７５】
P-GWは、メッセージをクライアントデバイスから受信してよく、メッセージは、共有鍵(たとえば、K_{P-GW})に基づいて暗号化および/または認証される、1908。言い換えれば、メッセージは、共有鍵に基づいて導出された鍵(たとえば、$K_{P-GWenc}$、$K_{P-GWint}$)を使用して暗号化および/または認証されてよい。
【０１７６】
図20は、本明細書で説明する態様による、セルラーネットワーク内でユーザプレーンメッセージ(たとえば、ユーザプレーンデータトラフィック)を保護するための、パケットデータネットワークへのゲートウェイ(たとえば、P-GW)において動作可能な例示的な方法2000を示す。
【０１７７】
方法は、パケットデータネットワークから第1のメッセージを、P-GWにおいて受信するステップによって開始してよい、2002。

【０１７８】
方法は、第1のメッセージの暗号化および/または認証の根拠を置く第1の共有鍵を、ゲートウェイにおいて取得するステップを含んでよく、第1の共有鍵はゲートウェイおよびデバイスによって共有され、ゲートウェイはデバイスとは独立に第1の共有鍵を取得する、2004。
【０１７９】
方法は、第1の暗号化および/または認証されたメッセージを作成するために、第1の共有鍵に基づいて第1のメッセージを暗号化および/または認証するステップをさらに含んでよい、2006。
【０１８０】
方法は、第1の暗号化および/または認証されたメッセージを、セルラーネットワークのアクセスノードを介してデバイスに送信するステップをさらに含んでよい、2008。
【０１８１】
反対方向において(たとえば、アップリンク方向において)、ゲートウェイは、アクセスノードから第2のメッセージを受信してよく、第2のメッセージは、クライアントデバイスおよびゲートウェイによってのみ共有される第1の共有鍵を用いて暗号化および/または認証される、2010。
【０１８２】
第2のメッセージは、第3のメッセージを取得するために、第1の共有鍵を使用して解読および/または認証されてよい、2012。
【０１８３】
第3のメッセージは、パケットデータネットワークに送信されてよい、2014。
【０１８４】
図21は、本明細書で説明する態様による、次世代セルラーネットワーク内でユーザプレーンメッセージ(たとえば、ユーザプレーンデータトラフィック)のセキュリティおよび/または保全性を保護するための、セッション鍵管理エンティティ(SKME)と本明細書で呼ばれるネットワークエンティティにおいて動作可能な例示的な方法2100を示す。
【０１８５】
ゲートウェイ(P-GW)からのクライアントデバイスに対するユーザプレーン(UP)鍵要求が、セッション鍵管理エンティティ(SKME)において受信されてよい、2102。UP鍵要求は、クライアントデバイス識別子を含んでよい。
【０１８６】
一時的モバイル加入者識別情報(TMSI)がMMEによって割り振られ、秘密保持のためにMME 114においてクライアントデバイスを識別するために使用されてよい。加えて、TMSIは、グローバル一意一時的クライアントデバイス識別情報(GUTI)の一部である。
【０１８７】
たとえば、3GPP TS 23.003から、GUTIのフォーマットおよびサイズは、
<GUTI>=<GUMMEI><M-TMSI>、
ここで、<GUMMEI>=<MCC><MNC><MME Identifier>
および、<MME Identifier>=<MME Group ID><MME Code>
MCCおよびMNCは、初期の3GPPシステムにおけるサイズと同じフィールドサイズを有するものとする。
M-TMSIは、32ビット長とする。
MMEグループIDは、16ビット長とする。
MMEコードは、8ビット長とする。
【０１８８】
GUTIはサービングネットワークにおいて使用され、したがって、サービングネットワーク内のP-GWがパケットデータネットワーク接続のために使用される場合、GUTIは、クライアントデバイスを識別するために使用され得る。一般に、国際モバイル加入者識別番号(IMSI)およびベアラID(トンネル終点識別子(TEID)を含む)が、P-GWにおいてクライアントデ

バイスを識別するために使用されてよい。

【０１８９】

SKMEは、K_{SKME}に基づいてクライアントデバイスに対するUP鍵(たとえば、K_{P-GW})を導出してよく、K_{P-GW}=F(K_{SKME}、GW ID)である、2104。

【０１９０】

SKMEは、導出されたUP鍵(たとえば、K_{P-GW})をP-GWに送信してよい、2106。

【０１９１】

図22は、本明細書で説明する態様による、セルラーネットワーク内でユーザプレーンメッセージ(たとえば、ユーザプレーンデータトラフィック)を保護する鍵を導出するための、SKMEにおいて動作可能な例示的な方法2200を示す。

【０１９２】

方法は、第1の共有鍵(たとえば、K_{SKME}鍵)を第1のエンティティ(たとえば、HSS)から取得するステップによって開始してよく、第1の共有鍵は、第1のエンティティおよびデバイスによって共有されてよい、2202。SKMEは、第1の共有鍵に基づいて第2の共有鍵(たとえば、K_{P-GW}鍵)を導出してよく、第2の共有鍵は、パケットデータネットワークへのゲートウェイおよびデバイスによって共有されてよい、2204。SKMEは、第1の共有鍵に基づいて第3の共有鍵(たとえば、K_{eNB}鍵)をさらに導出してよく、第3の共有鍵は、モビリティ管理エンティティ(MME)およびデバイスによって共有されてよい、2206。次に、SKMEは、第2の共有鍵をゲートウェイに送信してよい、2208。最後に、SKMEは、第3の共有鍵をMMEに送信してよい、2210。

【０１９３】

例示的なデバイスおよびデバイスにおいて使用可能な方法

図23は、本明細書で説明する方法を実行するように構成されたデバイス2300の例示的なハードウェア実装形態のブロック図を示す。たとえば、デバイス2300は、チップ構成要素、クライアントデバイス、ユーザ機器、端末、または何らかの他のタイプのデバイスを組み込むことができる。

【０１９４】

デバイス2300は、ワイヤレス通信回路2302およびメモリ/記憶デバイス2306に結合された処理回路、処理関数、または処理モジュール2304を含んでよい。ワイヤレス通信回路2302は、デバイス2300をサービングネットワークにワイヤレスに結合する働きをしてよい。処理回路/関数/モジュール2304は、デバイスおよびP-GWによって共有される共有鍵を使用してユーザプレーンデータトラフィックの暗号化/解読/認証を実行するように構成された、暗号化/解読/認証用回路、関数またはモジュール2308を含んでよい。処理回路/関数/モジュール2304は、デバイス2300とP-GWとの間で通過中のユーザプレーンデータトラフィックを保護するために使用されるいくつかの鍵の取得、生成および/またはローカルな導出を行うように構成された鍵取得/生成/導出用回路/関数/モジュール2310をさらに含んでよい。ユーザプレーンデータトラフィックの保護を容易にするために、メモリ/記憶デバイス2306は、秘密のルート鍵、K鍵2312を記憶してよく(またはそのような鍵は、デバイス2300のUSIM(図示せず)に記憶されてもよく)、暗号化/解読および認証のための他の鍵(図示せず)に加えて、IK、CK鍵2314、K_{SKME}鍵2316、K_{ASME}鍵2318、K_{P-GW}鍵2320、およびK_{eNB}鍵2322が、デバイス2300のメモリ/記憶デバイス2306にローカルに記憶されてよい。

【０１９５】

概して、処理回路/関数/モジュール2304は、デバイス2300のためのデータを処理するように適合された1つまたは複数のプロセッサ(たとえば、第1のプロセッサなど)であり得る。たとえば、処理回路/関数/モジュール2304は、本明細書で説明するプロセスまたは方法のいずれか1つを実行するための手段としての働きをする特定用途向け集積回路(ASIC)などの専用プロセッサであってよい。処理回路/関数/モジュール2304は、認証情報を検証すること、認証情報を生成すること、アクセスリストを維持すること、コマンドがアクセスリスト内にあることを決定すること、セキュアなチャネルを確立すること、実行を許可すること、デバイスを識別すること、またはセキュアなチャネルを確立することを行うため

の手段の一例としての働きをする。処理回路/関数/モジュール2304はまた、受信および/または送信するための手段の一例としての働きをしてもよい。

【０１９６】

処理回路/関数/モジュール2304の例は、マイクロプロセッサ、マイクロコントローラ、デジタル信号プロセッサ(DSP)、フィールドプログラマブルゲートアレイ(FPGA)、プログラマブル論理デバイス(PLD)、ステートマシン、ゲート論理、個別のハードウェア回路、および本開示の全体にわたって説明される様々な機能性を実施するように構成された他の適切なハードウェアを含む。処理回路/関数/モジュール2304はまた、1つまたは複数の通信バスを管理すること、およびメモリ/記憶デバイス2306内に組み込まれ得るコンピュータ可読記憶媒体に記憶された命令を実行することを行う役目を果たしてよい。命令(それはソフトウェアの形態であってよい)は、処理回路/関数/モジュール2304によって実行されたとき、処理回路/関数/モジュール2304に、本明細書で説明する様々な機能、ステップおよび/または方法を実行させることができる。メモリ/記憶デバイス2306内に組み込まれ得るコンピュータ可読記憶媒体は、ソフトウェア命令を実行するときに処理回路/関数/モジュール2304によって操作されるデータを記憶するために使用されてよい。

【０１９７】

メモリ/記憶デバイス2306は、限定はしないが、フラッシュメモリ、磁気的または光学的なハードディスクドライブなどのような、非揮発性メモリであってよい。いくつかの態様では、メモリは、永続的に情報を記憶するために継続的に電力供給され得る、DRAM(たとえば、DDR SDRAM)、SRAMなどの揮発性メモリであってよい。メモリ/記憶デバイス2306は、鍵を記憶するための手段の一例としての働きをする。

【０１９８】

ソフトウェアまたは命令は、ソフトウェア、ファームウェア、ミドルウェア、マイクロコード、ハードウェア記述言語と呼ばれるか、または他の名称で呼ばれるかにかかわらず、ソフトウェア、命令、命令セット、コード、コードセグメント、プログラムコード、プログラム、サブプログラム、ソフトウェアモジュール、アプリケーション、ソフトウェアアプリケーション、ソフトウェアパッケージ、ルーチン、サブルーチン、オブジェクト、実行可能ファイル、実行スレッド、プロシージャ、関数などを意味するように広く解釈されなければならない。ソフトウェアは、メモリ/記憶デバイス2306内に組み込まれたコンピュータ可読記憶媒体上にあってよい。コンピュータ可読記憶媒体は、非一時的コンピュータ可読記憶媒体であってよい。非一時的なコンピュータ可読記憶媒体は、例として、磁気記憶デバイス(たとえば、ハードディスク、フロッピーディスク、磁気ストリップ)、光ディスク(たとえば、コンパクトディスク(CD)、またはデジタル多用途ディスク(DVD))、スマートカード、フラッシュメモリデバイス(たとえば、カード、スティック、または鍵ドライブ)、ランダムアクセスメモリ(RAM)、リードオンリメモリ(ROM)、プログラマブルROM(PROM)、消去可能なPROM(EPROM)、電気的消去可能PROM(EEPROM)、レジスタ、リムーバブルディスク、およびコンピュータによってアクセスおよび読み出し可能なソフトウェアおよび/または命令を記憶するための任意の他の適切な媒体を含む。コンピュータ可読記憶媒体は、処理回路/関数/モジュール2304の中もしくは外にあってよく、または処理回路/関数/モジュール2304を含む複数のエンティティにわたって分散されてもよい。コンピュータ可読記憶媒体は、コンピュータプログラム製品の中に組み込まれてもよい。加えて、デバイス2300は、例として、搬送波、伝送線路、ならびに、コンピュータによってアクセスおよび読み出し可能なソフトウェアおよび/または命令を送信するための任意の他の適切な媒体も含むことができるコンピュータ可読媒体と対話することができる。

【０１９９】

図24は、本明細書で説明する態様による、セルラーネットワーク内でユーザプレーンメッセージ(たとえば、ユーザプレーンデータトラフィック)を保護するための、デバイス(たとえば、チップ構成要素、クライアントデバイス)において動作可能な例示的な方法2400を示す。

【０２００】

方法は、第1の共有鍵を、デバイスにおいて取得するステップを含んでよい、2402。第1の共有鍵に基づく第2の共有鍵もまた、デバイスにおいて取得されてよい、2404。第2の共有鍵は、デバイスとパケットデータネットワークゲートウェイ(P-GW)との間で通過中のデータトラフィックをセキュアにするためのものである。第2の共有鍵は、デバイスおよびP-GWによって共有されてよい。方法は、第1のセキュアにされたデータトラフィックを作成するために、第2の共有鍵に基づいてデータトラフィックをセキュアにするステップを含んでよい、2406。データがセキュアにされた後、方法は、第1のセキュアにされたデータトラフィックをアクセスノードを介してP-GWに送信するステップを含んでよい、2408。P-GWおよびアクセスノードは、別個のネットワークエンティティであってよい。

【０２０１】

本明細書で説明する態様では、第1の共有鍵は、P-GWに知られていないことがある。第1の共有鍵および第2の共有鍵はデバイスにおいてローカルに導出されてよく、デバイスに送信されることはない。言い換えれば、第1の共有鍵および第2の共有鍵は、デバイスにオーバージエアで送信されることはない。第2の共有鍵が、ユーザプレーン通信の少なくともいくつかの層をセキュアにする一方で、異なる鍵が、制御プレーン通信をセキュアにすることができる。

【０２０２】

随意に、方法は、デバイスとモビリティ管理エンティティ(MME)との間で送信される制御メッセージング(たとえば、制御プレーン制御メッセージング)をセキュアにするために、第1の共有鍵に基づいて第3の共有鍵をデバイスにおいて取得するステップを含んでよい、2410。第3の共有鍵は、デバイスおよびMMEによって共有されてよい。P-GW、MMEおよびアクセスノードは、別個のネットワークエンティティであってよい。

【０２０３】

随意に、方法は、デバイスとアクセスノードとの間のデータトラフィック、およびデバイスとMMEとの間の制御メッセージングをセキュアにするために、第3の共有鍵に基づいて第4の共有鍵を、デバイスにおいて取得するステップを含んでよい、2412。第4の共有鍵は、デバイスおよびアクセスノードによって共有されてよい。方法は、第2のセキュアにされたデータトラフィックを作成するために、第4の共有鍵に基づいて第1のセキュアにされたデータトラフィックをセキュアにするステップを、随意にさらに含んでよい、2414。いくつかの態様では、第1のセキュアにされたデータトラフィックは、第2のセキュアにされたデータトラフィックの中にカプセル化される。方法は、第1のセキュアにされたデータトラフィックの代わりに第2のセキュアにされたデータトラフィックを、アクセスノードを介してP-GWに送信するステップをさらに含んでよい、2416。P-GW、MMEおよびアクセスノードは、別個のネットワークエンティティであってよい。

【０２０４】

本明細書で説明する追加の態様によれば、第2の共有鍵は、ユーザプレーンのインターネットプロトコル(IP)層内の第2のセキュアにされたデータトラフィックを保護する一方で、第4の共有鍵は、ユーザプレーンのパケットデータ収束プロトコル(PDCP)層内の第2のセキュアにされたデータトラフィックを保護する。言い換えれば、第4の共有鍵は、ユーザプレーンのいくつかの層上のトラフィックのいくつかの送信を保護する一方で、第2の共有鍵は、ユーザプレーンの他の層上のトラフィックの他の送信を保護するために使用される。

【０２０５】

本明細書で説明する態様によれば、第1の共有鍵は、デバイスとネットワークエンティティとの間で共有されてよい。ネットワークエンティティは、第1の共有鍵をホーム加入者サーバ(HSS)から取得してもよい。デバイスは、P-GWとは独立に、第2の共有鍵を取得してもよい。第2の共有鍵を取得するステップは、第2の共有鍵を、第1の共有鍵およびパケットデータネットワークゲートウェイ識別子(GW ID)の関数としてデバイスにおいて導出するステップを含んでよい。

【０２０６】

本明細書で説明する態様によれば、データトラフィックは、制御メッセージングとは異なる。データトラフィックはユーザプレーン上で送信されてよく、制御メッセージングは制御プレーン上で送信されてよい。ユーザプレーンおよび制御プレーンは、別個の送信経路である。

【０２０７】

本明細書で説明するいくつかの態様によれば、データトラフィックをセキュアにするステップは、第2の共有鍵に基づいてデータトラフィックを暗号化するステップを含む。本明細書で説明する他の態様によれば、データトラフィックをセキュアにするステップは、第2の共有鍵に基づく認証署名を含めるステップを含んでよい。

【０２０８】

データトラフィックを受信することに関して、いくつかの態様によれば、デバイスは、第3のセキュアにされたデータトラフィックをアクセスノードを介してP-GWから受信してよい。第3のセキュアにされたデータトラフィックは、第2の共有鍵に基づいてセキュアにされてよい。次いで、デバイスは、セキュアでないデータトラフィックを作成するために、第2の共有鍵に基づいて第3のセキュアにされたデータトラフィックの解読および/または認証を続行してよい。

【０２０９】

例示的なパケットデータネットワークゲートウェイ(P-GW)およびそこにおいて動作可能な方法

図25は、本明細書で説明する方法を実行するように構成されたパケットデータネットワークゲートウェイ(P-GW)2500の例示的なハードウェア実装形態のブロック図を示す。

【０２１０】

P-GW2500は、ネットワーク通信回路2502およびメモリ/記憶デバイス2506に結合された処理回路、処理関数、または処理モジュール2504を含んでよい。ネットワーク通信回路2502は、P-GW2500をセルラーシステムのパケットデータネットワークおよび/またはコアネットワークに通信可能に結合する働きをしてよい。処理回路/関数/モジュール2504は、P-GW2500およびデバイスによって共有される共有鍵を使用してユーザプレーンデータトラフィックの暗号化/解読/認証を実行するように構成された、暗号化/解読/認証用回路、関数またはモジュール2508を含んでよい。処理回路/関数/モジュール2504は、P-GW2500とデバイスとの間で通過中のユーザプレーンデータトラフィックを保護するために使用されるいくつかの鍵の取得および/またはローカルな導出を行うように構成された鍵取得/生成用回路/関数/モジュール2510をさらに含んでよい。本明細書で説明する例示的な態様では、鍵取得/生成用回路/関数/モジュール2510は、一般に、SKMEから共有鍵(たとえば、K_{P-GW})を取得してよく、ここで共有鍵はSKMEにおいて導出され、SKMEによって鍵取得/生成用回路/関数/モジュール2510に提供される。ユーザプレーンデータトラフィックの保護を容易にするために、メモリ/記憶デバイス2506は、取得されたK_{P-GW}鍵2512をP-GW2500のメモリ/記憶デバイス2506にローカルに記憶してよい。

【０２１１】

図26は、本明細書で説明する態様による、セルラーネットワーク内でユーザプレーンメッセージ(たとえば、ユーザプレーンデータトラフィック)を保護するための、P-GWにおいて動作可能な例示的な方法2600を示す。

【０２１２】

方法2600は、パケットデータネットワークからデータトラフィックを、P-GWにおいて受信するステップを含んでよい、2602。方法は、P-GWとデバイスとの間で通過中のデータトラフィックをセキュアにするために、秘密の共有鍵をネットワークエンティティからP-GWにおいて取得するステップをさらに含んでよく、秘密の共有鍵はP-GWおよびデバイスによって共有される、2604。方法は、第1のセキュアにされたデータトラフィックを作成するために、秘密の共有鍵に基づいてデータトラフィックをセキュアにするステップを含んでよい、2606。方法は、第1のセキュアにされたデータトラフィックをアクセスノードを介してデバイスに送信するステップをさらに含んでよく、P-GW、アクセスノードおよびネッ

トワークエンティティは、別個のネットワークエンティティである、2608。
【０２１３】
本明細書で説明する態様によれば、秘密の共有鍵は、アクセスノードに知られていないことがある。秘密の共有鍵は、ネットワークエンティティから、制御プレーンインターフェース上でP-GWに提供されてよい。ネットワークエンティティは、SKMEであってよい。
【０２１４】
本明細書で説明する態様によれば、秘密の共有鍵が、ユーザプレーン通信の少なくともいくつかの層をセキュアにする一方で、異なる共有鍵が、制御プレーン通信をセキュアにしてよい。たとえば、秘密の共有鍵は、ユーザプレーンのインターネットプロトコル(IP)層内のデータトラフィックを保護してよい。P-GWは、デバイスとは独立に、秘密の共有鍵を取得してもよい。秘密の共有鍵は、P-GW識別子(GW ID)の関数であってよい。
【０２１５】
いくつかの態様によれば、秘密の共有鍵を取得するステップは、ホーム加入者サーバ(HSS)とモビリティ管理エンティティ(MME)との間に位置するネットワークエンティティから秘密の共有鍵を取得するステップをさらに含んでよい。再び、ネットワークエンティティは、SKMEであってよい。
【０２１６】
いくつかの態様によれば、秘密の共有鍵は、P-GWと同じドメイン内のネットワークエンティティから取得されてよい。
【０２１７】
随意に、方法はまた、秘密の共有鍵によってセキュアにされた、セキュアにされたアップリンクデータトラフィックを、アクセスノードを介してデバイスからP-GWにおいて受信するステップを含んでよい、2610。方法は、アップリンクデータトラフィックを取得するために、秘密の共有鍵を用いてセキュアにされたアップリンクデータトラフィックを解読および/または認証するステップを随意にさらに含んでよい、2612。方法は、アップリンクデータトラフィックをパケットデータネットワークに送信するステップを随意にさらに含んでよい、2614。
【０２１８】
例示的なネットワークエンティティ(たとえば、SKME)およびそこにおいて動作可能な方法
図27は、本明細書で説明する方法を実行するように構成されたセッション鍵管理エンティティ(SKME)と本明細書で呼ばれるネットワークエンティティ2700の例示的なハードウェア実装形態のブロック図を示す。
【０２１９】
ネットワークエンティティ2700は、ネットワーク通信回路2702およびメモリ/記憶デバイス2706に結合された処理回路、処理関数、または処理モジュール2704を含んでよい。ネットワーク通信回路2702は、ネットワークエンティティ2700を他のネットワークエンティティまたはセルラーシステムのノードに通信可能に結合する働きをしてよい。処理回路/関数/モジュール2704は、P-GWとデバイスとの間で通過中のユーザプレーンデータトラフィックを保護するために使用されるいくつかの鍵の取得および/またはローカルな導出を行うように構成された鍵取得/生成用回路/関数/モジュール2710を含んでよい。本明細書で説明する例示的な態様では、鍵取得/生成用回路/関数/モジュール2710は、一般に、共有鍵(たとえば、K_{P-GW})を導出してよく、ここで共有鍵はSKMEにおいて導出され、P-GWに提供される。いくつかの態様では、SKMEは、K_{P-GW}を記憶する必要はない。他の態様では、SKMEは、K_{P-GW}を随意に記憶してもよい。したがって、メモリ/記憶デバイス2706は、ネットワークエンティティ2700のK_{P-GW}鍵2712を随意にローカルに記憶してよい。
【０２２０】
図28は、本明細書で説明する態様による、セルラーネットワーク内でユーザプレーンメッセージ(たとえば、ユーザプレーンデータトラフィック)の保護に関連する、SKMEにおいて動作可能な例示的な方法2800を示す。
【０２２１】

方法2800は、第1の共有鍵を、ネットワークエンティティにおいて取得するステップによって開始してよい、2802。ネットワークエンティティは、第1の共有鍵に基づいて第2の共有鍵を取得してよい、2804。第2の共有鍵は、デバイスとパケットデータネットワークゲートウェイ(P-GW)との間で通過中のデータトラフィックをセキュアにするためのものであってよく、第2の共有鍵は、デバイスおよびP-GWによって共有される。方法は、第2の共有鍵をP-GWに送信するステップによって継続されてよい、2806。

【０２２２】

方法は、第1の共有鍵に基づいて第3の共有鍵をネットワークエンティティにおいて取得するステップによって継続されてよい、2808。第3の共有鍵は、デバイスとモビリティ管理エンティティ(MME)との間で送信される制御メッセージングをセキュアにするためのものであってよく、第3の共有鍵は、デバイスおよびMMEによって共有される。方法は、第3の共有鍵をMMEに送信するステップをさらに含んでよい、2810。ネットワークエンティティ、P-GWおよびMMEは、別個のネットワークエンティティであってよい。

【０２２３】

いくつかの態様によれば、第2の共有鍵を取得するステップは、第2の共有鍵を、第1の共有鍵およびパケットデータネットワークゲートウェイ識別子(GW ID)の関数として導出するステップをさらに含んでよい。

【０２２４】

いくつかの態様によれば、データトラフィックは、制御メッセージングとは異なる。たとえば、データトラフィックはユーザプレーン上で送信されてよく、制御メッセージングは制御プレーン上で送信されてよく、ユーザプレーンおよび制御プレーンは別個の送信経路である。

【０２２５】

いくつかの態様によれば、ネットワークエンティティは、ホーム加入者サーバ(HSS)とMMEとの間に位置し、ネットワークエンティティは、HSSおよびMMEとは異なる。

【０２２６】

図面に示す構成要素、ステップ、特徴および/または機能のうちの1つもしくは複数は、単一の構成要素、ステップ、特徴、もしくは機能に再構成および/または結合されてよく、あるいは、いくつかの構成要素、ステップもしくは機能に組み込まれてもよい。また、本明細書で開示する新規の特徴から逸脱することなく追加の要素、構成要素、ステップ、および/または機能が追加され得る。図に示す装置、デバイス、および/または構成要素は、本明細書で説明する方法、特徴、またはステップのうちの1つまたは複数を実行するように構成され得る。本明細書で説明する新規のアルゴリズムはまた、効率的にソフトウェアで実装されてもよく、かつ/またはハードウェアに埋め込まれてもよい。

【０２２７】

開示した方法におけるステップの具体的な順序または階層は、例示的方法および/またはプロセスの例示であることを理解されたい。設計の選好に基づいて、方法におけるステップの具体的な順序または階層は再構成され得ることを理解されたい。添付の方法クレームは、様々なステップの要素を例示的順序で提示したものであり、その中で特に記載されていない限り、提示された特定の順序または階層に限定されることを意図するものではない。本開示から逸脱することなく、追加の要素、構成要素、ステップ、および/または機能が追加されることもあり、または利用されないことがある。

【０２２８】

本開示の特徴について、いくつかの実装形態および図面に関して説明した場合があるが、本開示のすべての実装形態は、本明細書で説明した有利な特徴のうちの1つまたは複数を含み得る。言い換えれば、1つまたは複数の実装形態について、いくつかの有利な特徴を有するものとして説明した場合があるが、そのような特徴のうちの1つまたは複数は、本明細書で説明した様々な実装形態のいずれかに従って使用されてもよい。同様に、例示的実装形態について、デバイスの実装形態、システムの実装形態、または方法の実装形態として本明細書で説明した場合があるが、そのような例示的実装形態が様々なデバイス、

システム、および方法において実装され得ることを理解されたい。

【０２２９】

加えて、少なくともいくつかの実装形態について、フローチャート、流れ図、構造図、またはブロック図として示される方法として説明したことに留意されたい。フローチャートは、動作を順次的方法として説明することがあるが、動作の多くは、並行してまたは同時に実行されてもよい。加えて、動作の順序は並べ替えられてもよい。方法は、その動作が完了したとき、終了する。いくつかの態様では、プロセスは、方法、関数、手順、サブルーチン、サブプログラムなどに対応し得る。プロセスが関数に対応するとき、その終了は、呼出し側関数またはメイン関数への関数の戻りに対応する。本明細書に記載の様々なプロセスのうちの1つまたは複数は、機械可読、コンピュータ可読、および/またはプロセッサ可読記憶媒体内に記憶され得るプログラミング(たとえば、命令および/またはデータ)によって部分的または完全に実装され、1つまたは複数のプロセッサ、マシン、および/またはデバイスによって実行され得る。

【０２３０】

さらに、本明細書で開示した実装形態に関して説明した様々な例示的論理ブロック、モジュール、回路、およびアルゴリズムステップは、ハードウェア、ソフトウェア、ファームウェア、ミドルウェア、マイクロコード、またはそれらの任意の組合せとして実装されてもよいことが当業者にはさらに諒解されよう。この互換性を明確に示すために、様々な例示的構成要素、ブロック、モジュール、回路、およびステップについて、全般的にそれらの機能に関して上記で説明した。そのような機能がハードウェアとして実装されるかソフトウェアとして実装されるかは、特定の適用例および全体的なシステムに課された設計制約に依存する。

【０２３１】

本開示内で、「例示的」という語は、「一例、事例、または例示としての役割を果たすこと」を意味するために使用される。「例示的」として本明細書で説明する任意の実装形態または態様は、必ずしも本開示の他の態様よりも好ましいまたは有利であると解釈されるべきではない。同様に、「態様」という用語は、本開示のすべての態様が、説明された特徴、利点、または動作モードを含むことを必要としない。「結合された」という用語は、本明細書では、2つの物体間の直接的または間接的な結合を指すために使用される。たとえば、物体Aが物体Bに物理的に接触し、物体Bが物体Cに接触する場合、物体Aと物体Cとは、互いに物理的に直接接触していない場合でも、それでも互いに結合されていると見なすことができる。たとえば、第1のダイがパッケージ内の第2のダイに物理的に直接接触していなくても、第1のダイは、第2のダイに結合されている可能性がある。「回路(circuit)」および「回路(circuitry)」という用語は広義に使用され、電子回路のタイプに関する制限なく、接続され、構成されると、本開示で説明した機能の性能を可能にする電気デバイスおよび導体のハードウェア実装と、プロセッサによって実行されると、本開示で説明した機能の性能を可能にする情報および命令のソフトウェア実装の両方を含むものとする。

【０２３２】

本明細書で使用する「決定する」という用語は、多種多様なアクションを包含する。たとえば、「決定する」ことは、計算すること(calculating、computing)、処理すること、導出すること、調査すること、探索すること(たとえば、テーブル、データベース、または別のデータ構造内を探索すること)、確認することなどを含むことができる。加えて、「決定する」ことは、受信すること(たとえば、情報を受信すること)、アクセスすること(たとえば、メモリ内のデータにアクセスすること)などを含み得る。加えて、「決定すること」は、解決すること、選択すること、選ぶこと、確立することなどを含むことができる。

【０２３３】

上記の説明は、本明細書に記載された様々な態様を任意の当業者が実践することを可能にするために提供される。これらの態様に対する様々な修正形態は、当業者に容易に明ら

かになり、本明細書において定義された一般原理は、他の態様に適用される場合がある。したがって、特許請求の範囲は本明細書に示された態様に限定されるものではなく、特許請求の範囲の文言と整合するすべての範囲を与えられるものであり、単数形の要素への言及は、「唯一の」と明記されていない限り、「唯一の」ではなく、「1つまたは複数の」を意味するものである。別段に明記されていない限り、「いくつか(some)」という用語は、1つまたは複数を指す。項目のリスト「のうちの少なくとも1つ」を言及する句は、単一のメンバーを含むそれらの項目の任意の組合せを指す。一例として、「a、b、またはcのうちの少なくとも1つ」は、a;b;c;aおよびb;aおよびc;bおよびc;ならびにa、b、およびcを包含するものとする。当業者に周知であり、または後に当業者に知られることになる、本開示全体にわたって説明された様々な態様の要素に対するすべての構造的および機能的均等物が、参照によって本明細書に明白に組み込まれ、特許請求の範囲によって包含されるものとする。その上、本明細書において開示されるものは、そのような開示が特許請求の範囲において明示的に列挙されているかどうかにかかわらず、公に供されることは意図されていない。いかなるクレーム要素も、「のための手段」という句を使用して要素が明確に列挙されていない限り、または方法クレームの場合、「のためのステップ」という句を使用して要素が列挙されていない限り、米国特許法第112条第6項の規定に基づいて解釈されるべきではない。

【０２３４】

このため、本明細書で説明され添付の図面に示される例に関連する様々な特徴は、本開示の範囲から逸脱することなく、異なる例および実装形態で実装され得る。したがって、いくつかの特定の構成および配置が説明され添付の図面に示されたが、説明された実装形態への様々な他の追加および修正、ならびにそうした実装形態からの削除が当業者に明らかであるので、そのような実装形態は例示にすぎず、本開示の範囲を限定するものではない。したがって、本開示の範囲は、以下の特許請求の範囲の文言、および法的均等物によってのみ決定される。

【符号の説明】

【０２３５】

100 第4世代(4G)セルラーネットワーク
102 発展型ユニバーサル地上波無線アクセスネットワーク(E-UTRAN)
104 発展型パケットコア(EPC)
106 クライアントデバイス
108 ユニバーサル加入者識別モジュール(USIM)
110 破線
112 アクセスノード
114 モビリティ管理エンティティ(MME)
116 実線
118 サービングゲートウェイ(S-GW)
120 パケットデータネットワーク(PDN)ゲートウェイ(P-GW)
122 パケットデータネットワーク(PDN)
124 ホーム加入者サーバ(HSS)
126 認証センター(AuC)
200 プロトコルスタック
202 クライアントデバイス
204 アクセスノード
206 P-GW
208 アプリケーションサーバ(APPサーバ)
210 インターネットプロトコル層(IP層)
212 パケットデータ収斂プロトコル(PDCP)層
214 無線リンク制御(RLC)層
216 媒体アクセス制御(MAC)層

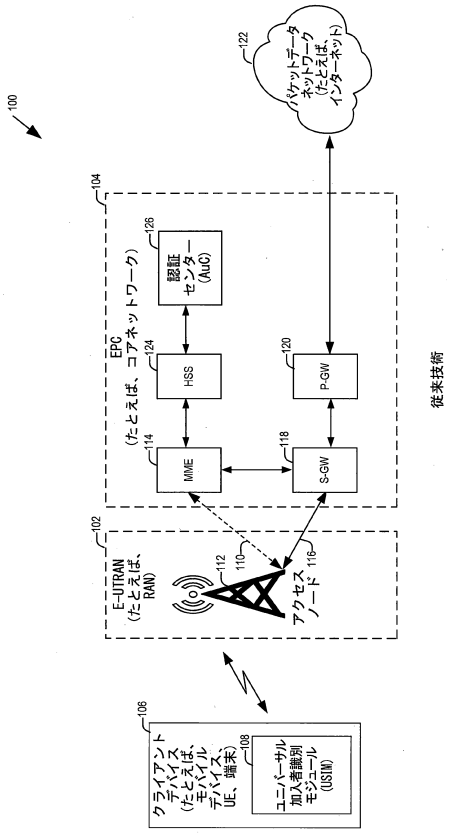
218 物理(PHY)層
220 PDCP層
222 RLC層
224 MAC層
226 PHY層
228 ユーザプレーンに対する汎用パケット無線サービス(GPRS)トンネリングプロトコル(GTP-U)層
230 ユーザデータグラムプロトコル(UDP)層
232 インターネットプロトコル層(IP層)
234 MAC層
236 イーサーネット層
238 GTP-U層
240 ユーザデータグラムプロトコル(UDP)層
242 IP層
244 MAC層
246 イーサーネット層
248 IP層
250 IP層
252 共有鍵、K_{eNB}鍵
254 インターネットプロトコルセキュリティ(IPSEC)
300 鍵階層
302 K鍵
304 保全性鍵(IK)、暗号鍵(CK)
306 アクセスセキュリティ管理エンティティ(ASME)鍵(KASME鍵)
308 非アクセス層暗号化鍵(K_{NASenc}鍵)
310 非アクセス層保全性鍵(K_{NASint}鍵)
312 K_{eNB}鍵
314 ユーザプレーン保全性鍵、K_{UPint}鍵
316 ユーザプレーン暗号化鍵、K_{UPenc}鍵
318 制御プレーン(無線リソース制御)保全性鍵、K_{RRCint}鍵
320 制御プレーン(無線リソース制御)暗号化鍵、K_{RRCenc}鍵
400 LTE(リリース8)セルラーネットワーク
402 コアネットワーク
404 アクセスノード
406 クライアントデバイス
408 HSS
410 MME
412 S-GW
414 P-GW
416 RRC
418 PDCP/RLCエンティティ
420 IPエンティティ
422 パイプライン
424 パイプライン
426 IPSECトンネル
500 次世代(たとえば、5G)セルラーネットワーク
502 E-UTRAN
504 EPC
506 クライアントデバイス
508 USIM

510 破線
512 アクセスノード
514 モビリティ管理エンティティ(MME)
516 実線
518 サービングゲートウェイ(S-GW)
520 パケットデータネットワーク(PDN)ゲートウェイ(P-GW)
522 パケットデータネットワーク
524 HSS
526 認証センター(AuC)
528 セッション鍵管理エンティティ(SKME)
530 訪問先セッション鍵管理エンティティ(V-SKME)
532 訪問先P-GW(V-P-GW)
534 第1の制御プレーンシグナリング経路
536 第2の制御プレーンシグナリング経路
600 プロトコルスタック
602 クライアントデバイス
604 アクセスノード
606 パケットデータネットワークゲートウェイ(P-GW)
608 アプリケーションサーバ(APPサーバ)
610 インターネットプロトコル層(IP層)
612 パケットデータ収斂プロトコル(PDCP)層
614 無線リンク制御(RLC)層
616 媒体アクセス制御(MAC)層
618 物理(PHY)層
620 PDCP層
622 RLC層
624 MAC層
626 PHY層
628 ユーザプレーンに対するGPRSトンネリングプロトコル(GTP-U)層
630 ユーザデータグラムプロトコル(UDP)層
632 インターネットプロトコル(IP)層
634 MAC層
636 イーサーネット層
638 (GTP-U)層
640 ユーザデータグラムプロトコル(UDP)層
642 インターネットプロトコル(IP)層
644 MAC層
646 イーサーネット層
648 IP層
650 IP層
652 K_{eNB}鍵
656 ユーザプレーンセキュリティ(UP-SEC)層
658 UP-SEC層
660 K_{P-GW}鍵
700 鍵階層
702 K鍵
704 IK、CK鍵
706 K_{SKME}鍵
708 K_{ASME}鍵
710 非アクセス層暗号化鍵、K_{NASenc}鍵

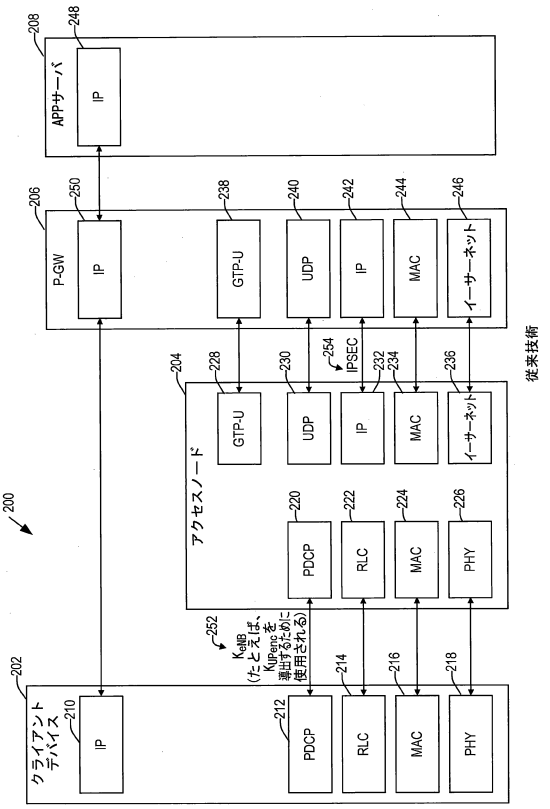
712 非アクセス層保全性鍵、K_{NASint}鍵
714 K_{eNB}鍵
716 ユーザプレーン保全性鍵、K_{UPint}鍵
718 ユーザプレーン暗号化鍵、K_{UPenc}鍵
720 制御プレーン保全性鍵、K_{RRCint}鍵
722 制御プレーン暗号化鍵、K_{RRCenc}鍵
724 K_{P-GW}鍵
726 $K_{P-GWint}$鍵
728 $K_{P-GWenc}$鍵
800 次世代(たとえば、5G)セルラーネットワーク
802 コアネットワーク
804 アクセスノード
806 クライアントデバイス
808 HSS
809 SKME
810 MME
811 セッション鍵管理エンティティ鍵、K_{SKME}鍵
812 S-GW
813 ローカルトラストアンカーまたはローカル鍵アンカー
814 P-GW
816 RRC
818 PDCP/RLCエンティティ
820 IPエンティティ
822 パイプライン
824 パイプライン
826 パイプライン
828 制御プレーン信号経路
900 コールフロー
902 デバイス
904 アクセスノード
906 MME
908 P-GW
910 セッション鍵管理エンティティ(SKME)
912 PDN接続要求
914 セッション生成要求
916 ポリシー制御および課金ルール関数(PCRF)
918 ユーザプレーン(UP)鍵要求
920 UP鍵応答
922 セッション生成応答
924 ベアラセットアップ要求/PDN接続受諾
926 RRC接続再構成要求
928 RRC接続再構成完了
930 ベアラセットアップ応答
932 直接転送
934 PDN接続完了
936 共有されたK_{P-GW}鍵に基づいて暗号化および/または認証された第1のメッセージをP-GWを介してユーザプレーン内のネットワークに送信する
938 共有されたK_{P-GW}鍵に基づいて暗号化および/または認証された第2のメッセージをP-GWを介してネットワークから受信する
1000 次世代セルラーネットワーク

1002 クライアントデバイス
1004 次世代セルラーネットワーク
1006 クライアントデバイス
1008 HSS
1010 ホームネットワーク内のP-GW、H-P-GW
1011 K_{SKME}鍵
1012 ホームSKME(H-SKME)
1013 K_{SKME}'鍵
1014 ホームネットワーク
1015 訪問先ネットワーク
1016 訪問先SKME(V-SKME)
1017 訪問先ネットワーク
1018 MME
1019 K_{ASME}鍵
1020 S-GW
1022 アクセスノード
1024 訪問先ネットワーク内のP-GW、V-P-GW
1026 V-SKME
1027 K_{SKME}鍵
1028 MME
1030 S-GW
1032 アクセスノード
1034 制御プレーンインターフェース
1036 制御プレーンインターフェース
2300 デバイス
2302 ワイヤレス通信回路
2304 処理モジュール
2306 メモリ/記憶デバイス
2308 暗号化/解読/認証用回路、関数またはモジュール
2310 鍵取得/生成/導出用回路/関数/モジュール
2312 秘密のルート鍵、K鍵
2314 IK、CK鍵
2316 K_{SKME}鍵
2318 K_{ASME}鍵
2320 K_{P-GW}鍵
2322 K_{eNB}鍵
2500 パケットデータネットワークゲートウェイ(P-GW)
2502 ネットワーク通信回路
2504 処理モジュール
2506 メモリ/記憶デバイス
2508 暗号化/解読/認証用回路、関数またはモジュール
2510 鍵取得/生成用回路/関数/モジュール
2512 K_{P-GW}鍵
2700 ネットワークエンティティ、セッション鍵管理エンティティ(SKME)
2702 ネットワーク通信回路
2704 処理モジュール
2706 メモリ/記憶デバイス
2710 鍵取得/生成用回路/関数/モジュール
2712 K_{P-GW}鍵

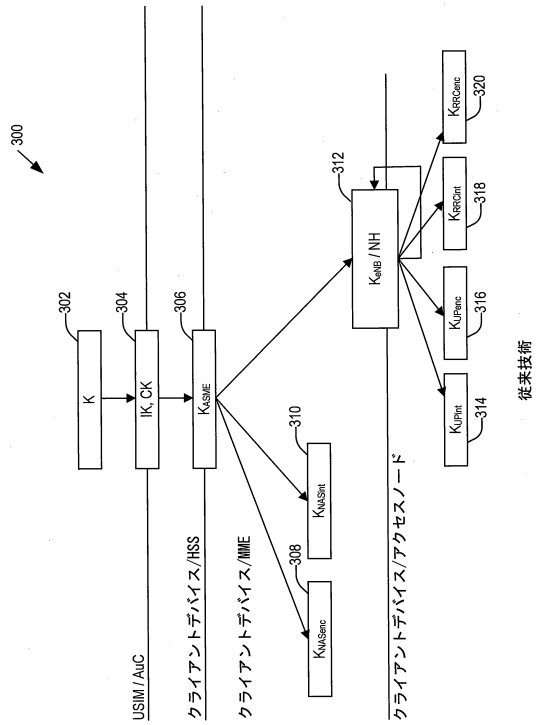
【図１】


100
パケットデータネットワーク（たとえば、インターネット）
122
104
EPC（たとえば、コアネットワーク）
認証センター（AuC）
126
HSS
124
P-GW
120
MME
114
S-GW
118
102
E-UTRAN（たとえば、RAN）
112
110
アクセスノード
116
106
クライアントデバイス（たとえば、モバイルデバイス、UE、端末）
ユニバーサル加入者識別モジュール（USIM）
108
従来技術

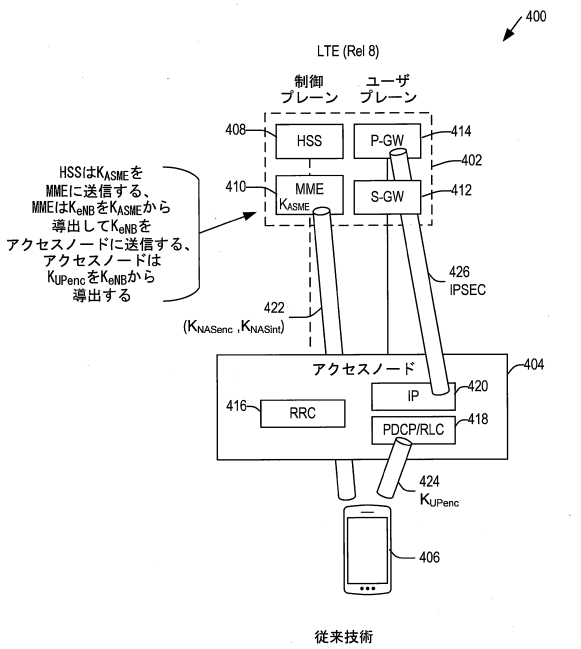
【図２】


208
APPサーバ
248
IP
206
P-GW
250
GTP-U
238
UDP
240
IP
242
MAC
244
イーサーネット
246
254
IPSEC
204
アクセスノード
228
230
232
234
236
220
222
224
226
PDCP
RLC
MAC
PHY
200
252
KeNB（たとえば、KUPencを導出するために使用される）
202
クライアントデバイス
210
212
214
216
218
従来技術

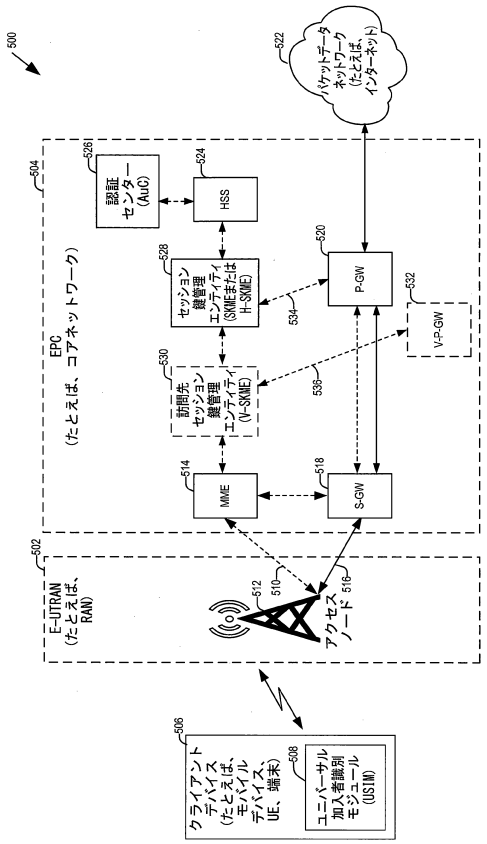
【図３】


300
K
302
IK, CK
304
KASME
306
KeNB / NH
312
KRRCenc
320
KRRCint
318
KUPenc
316
KUPint
314
KNASint
310
KNASenc
308
USIM / AuC
クライアントデバイス/HSS
クライアントデバイス/MME
クライアントデバイス/アクセスノード
従来技術

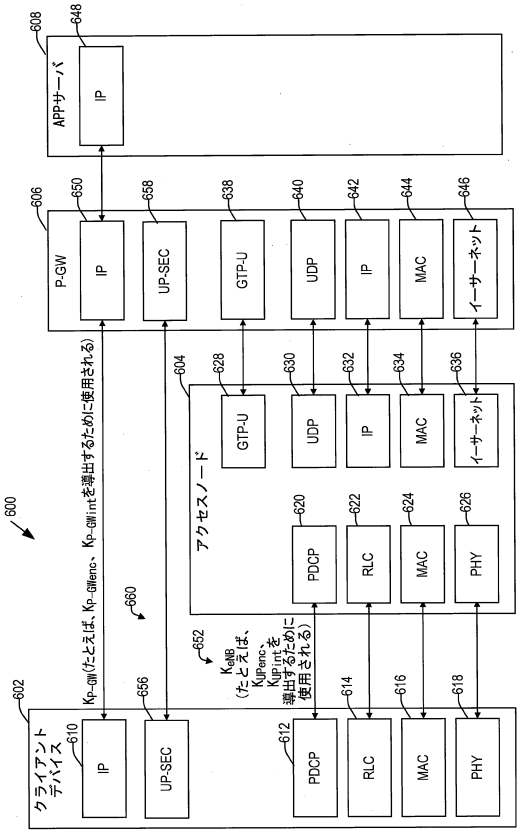
【図４】


400
LTE (Rel 8)
制御プレーン
ユーザプレーン
408
HSS
P-GW
414
402
410
MME
KASME
S-GW
412
HSSはKASMEをMMEに送信する、MMEはKeNBをKASMEから導出してKeNBをアクセスノードに送信する、アクセスノードはKUPencをKeNBから導出する
426
IPSEC
422
(KNASenc , KNASint)
アクセスノード
404
IP
420
416
RRC
PDCP/RLC
418
424
KUPenc
406
従来技術

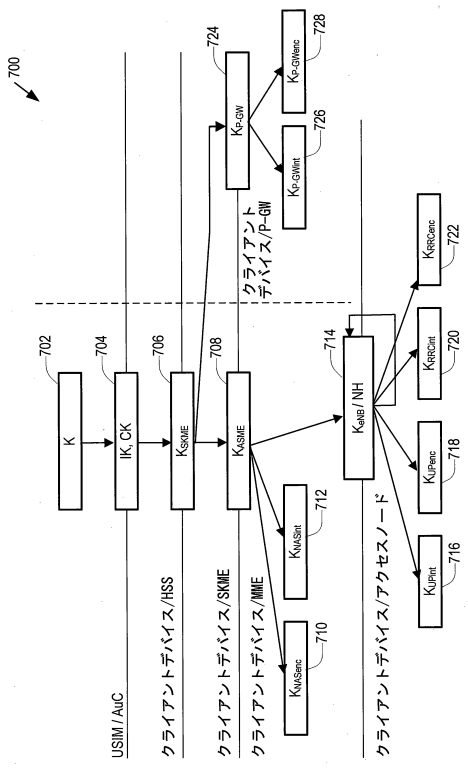
【図５】


500
パケットデータネットワーク（たとえば、インターネット）
522
EPC（たとえば、コアネットワーク）
504
認証センター（AuC）
526
HSS
524
セッション鍵管理エンティティ（SKMEまたはH-SKME）
528
P-GW
520
V-P-GW
532
訪問先セッション鍵管理エンティティ（V-SKME）
530
MME
514
S-GW
518
534
536
E-UTRAN（たとえば、RAN）
502
アクセスノード
510
512
516
クライアントデバイス（たとえば、モバイルデバイス、UE、端末）
506
ユニバーサル加入者識別モジュール（USIM）
508

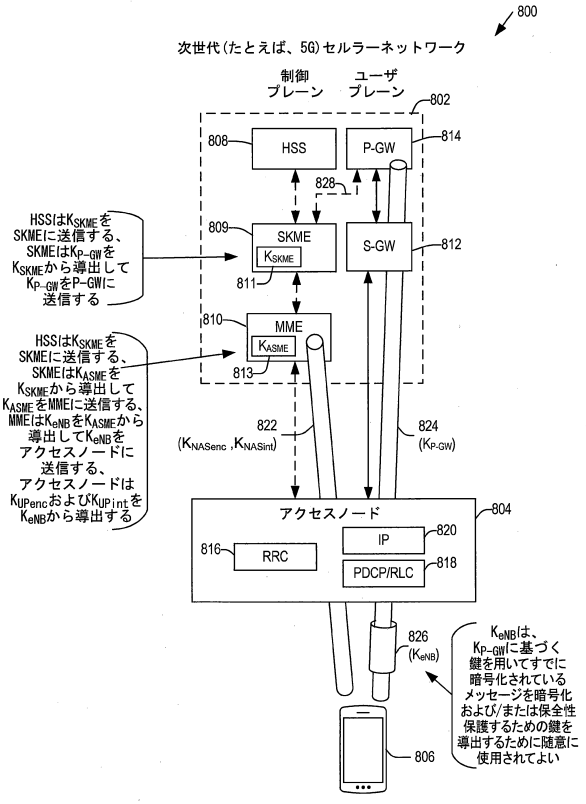
【図６】


600
APP-サーバ
608
IP
648
P-GW
606
IP
650
UP-SEC
658
GTP-U
638
UDP
640
IP
642
MAC
644
イーサーネット
646
アクセスノード
604
GTP-U
628
UDP
630
IP
632
MAC
634
イーサーネット
636
PDCP
620
RLC
622
MAC
624
PHY
626
KP-GW（たとえば、KP-GWenc、KP-GWintを導出するために使用される）
660
KeNB（たとえば、KUPenc、KUPintを導出するために使用される）
652
クライアントデバイス
602
IP
610
UP-SEC
656
PDCP
612
RLC
614
MAC
616
PHY
618

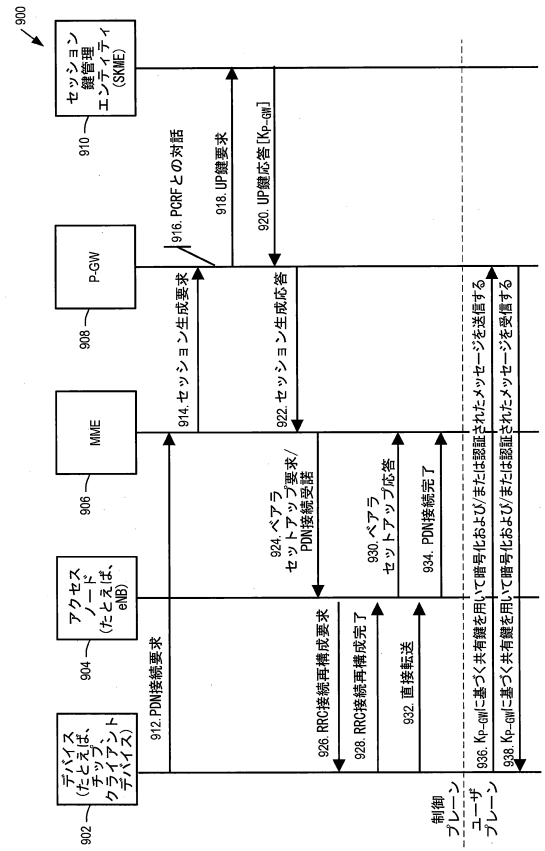
【図７】


700
K
702
IK, CK
704
KSKME
706
KASME
708
KP-GW
724
KP-GWenc
728
KP-GWint
726
クライアントデバイス/P-GW
KeNB / NH
714
KRRCenc
722
KRRCint
720
KUPenc
718
KUPint
716
KNASint
712
KNASenc
710
USIM / AuC
クライアントデバイス/HSS
クライアントデバイス/SKME
クライアントデバイス/MME
クライアントデバイス/アクセスノード

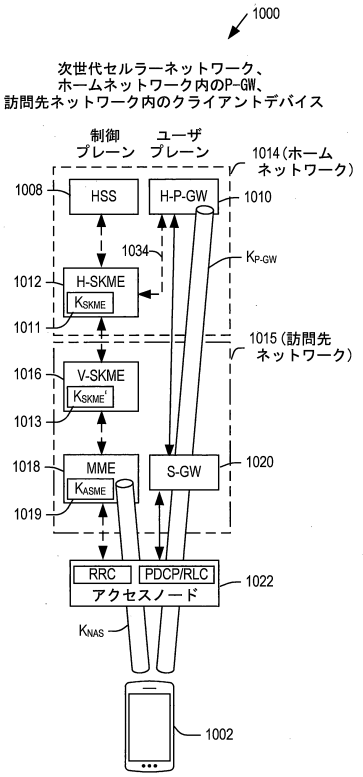
【図８】


800
次世代（たとえば、5G）セルラーネットワーク
制御プレーン
ユーザプレーン
802
HSS
808
P-GW
814
828
SKME
809
KSKME
S-GW
812
811
MME
810
KASME
813
HSSはKSKMEをSKMEに送信する、SKMEはKP-GWをKSKMEから導出してKP-GWをP-GWに送信する
HSSはKSKMEをSKMEに送信する、SKMEはKASMEをKSKMEから導出してKASMEをMMEに送信する、MMEはKeNBをKASMEから導出してKeNBをアクセスノードに送信する、アクセスノードはKUPencおよびKUPintをKeNBから導出する
822
(KNASenc, KNASint)
824
(KP-GW)
アクセスノード
804
IP
820
RRC
816
PDCP/RLC
818
826
(KeNB)
806
KeNBは、KP-GWに基づく鍵を用いてすでに暗号化されているメッセージを暗号化および/または保全性保護するための鍵を導出するために随意に使用されてよい

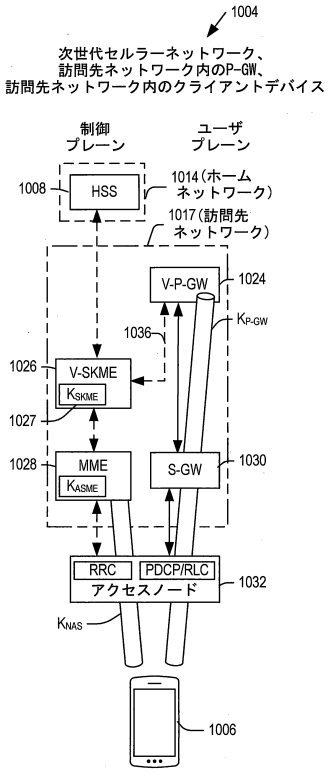
【図９】



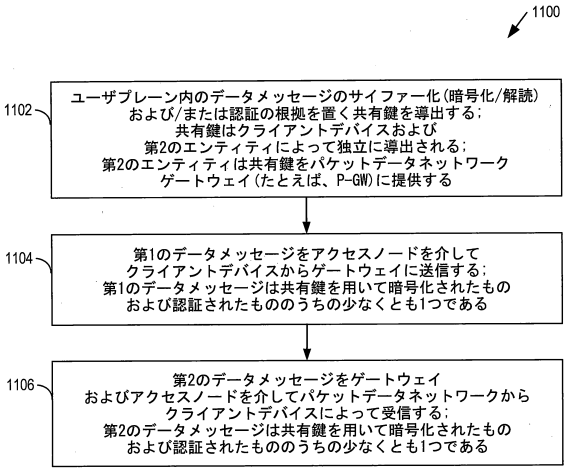
【図１０Ａ】



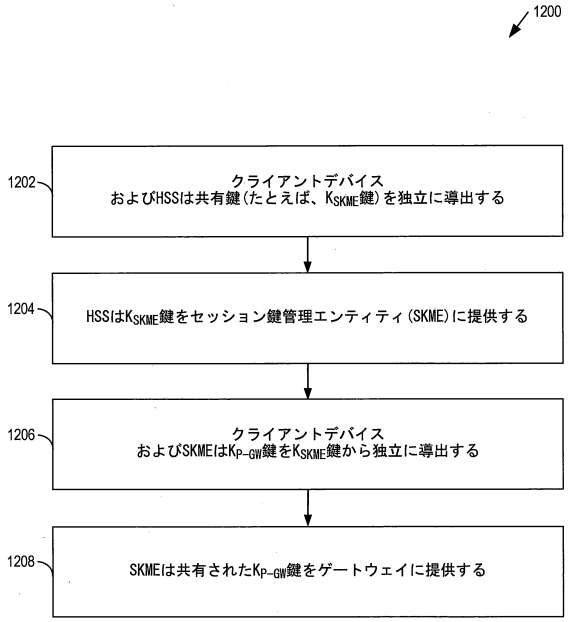
【図１０Ｂ】



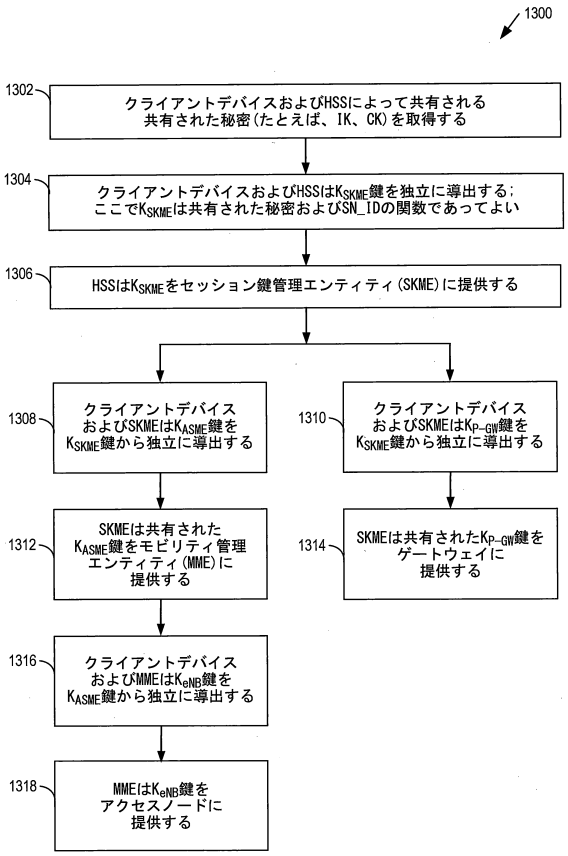
【図１１】



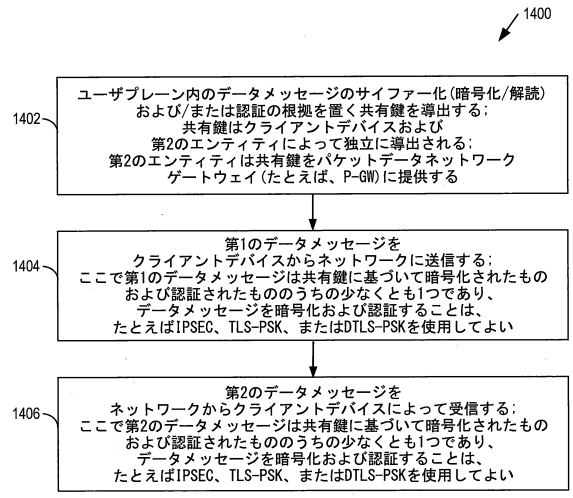
【図１２】



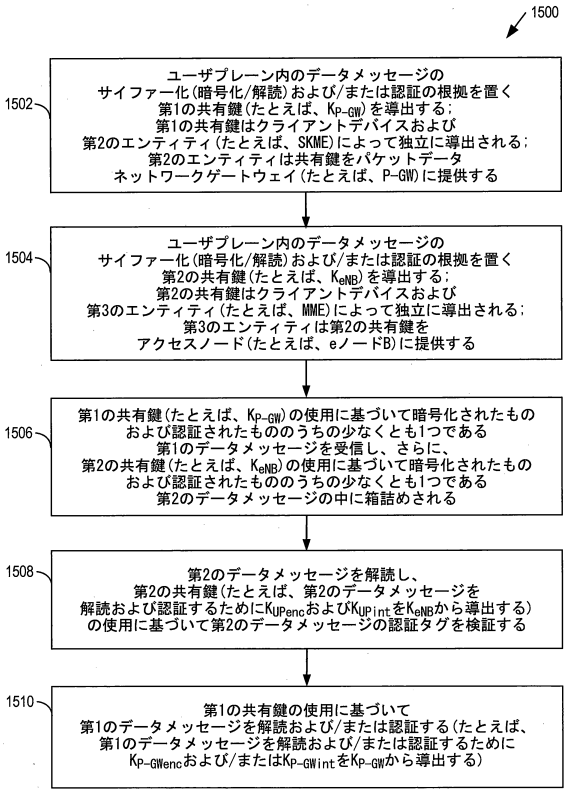
【図１３】



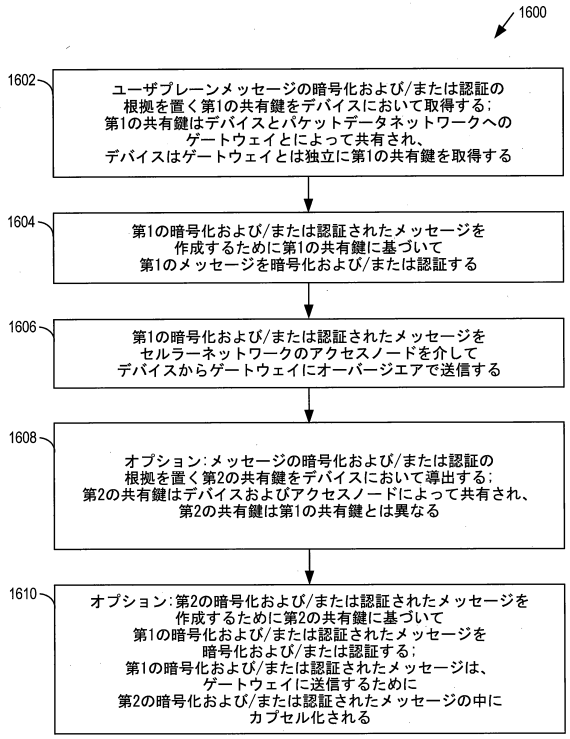
【図１４】



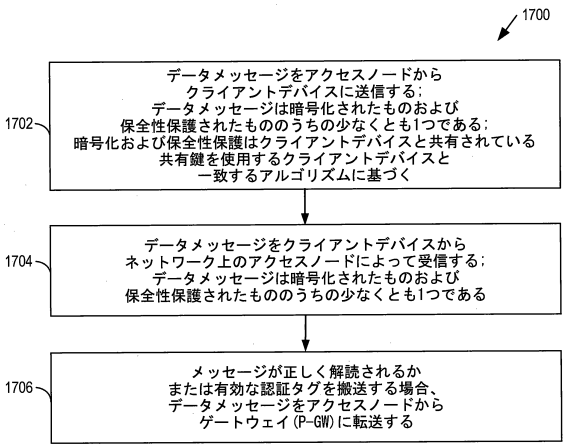
【図１５】



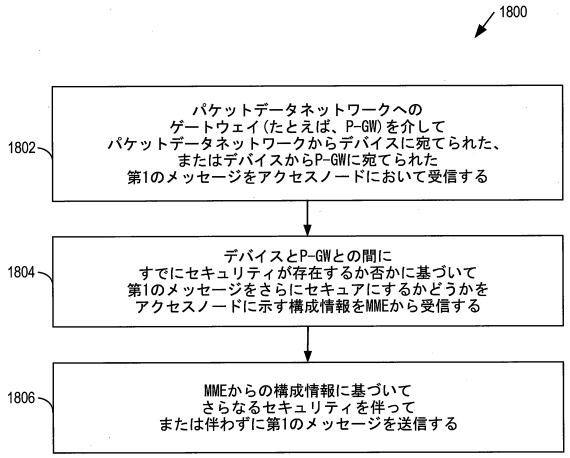
【図１６】



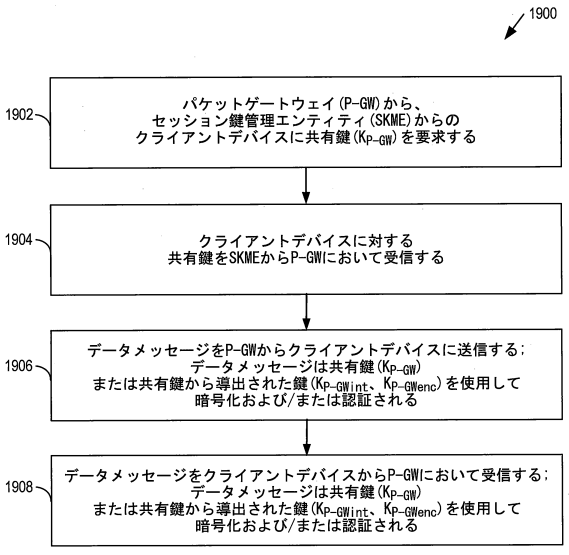
【図１７】



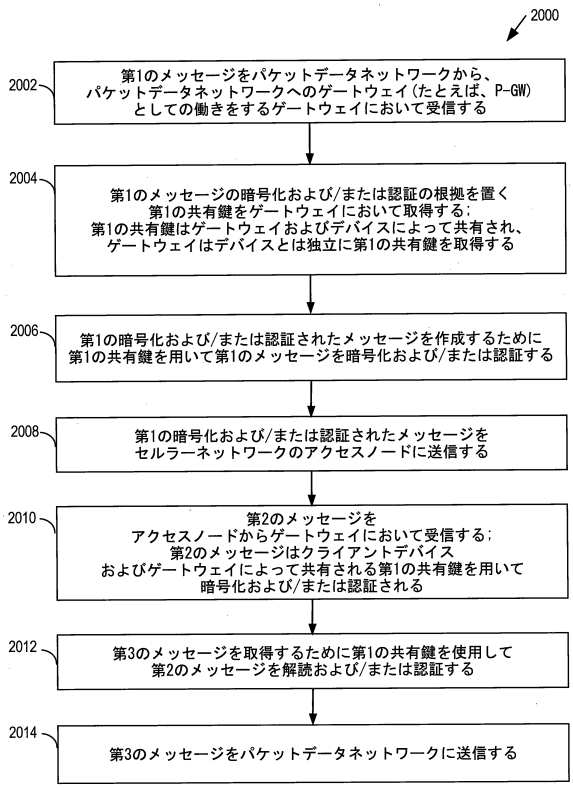
【図１８】



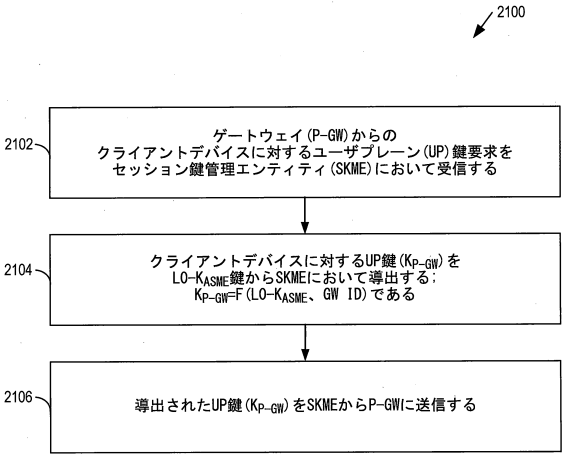
【図１９】



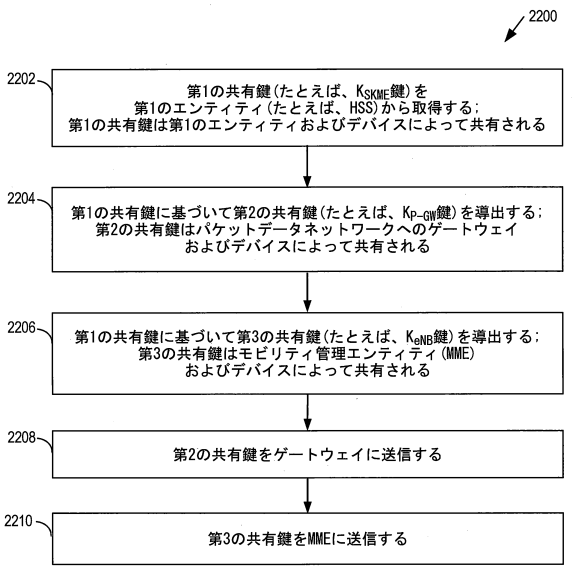
【図２０】



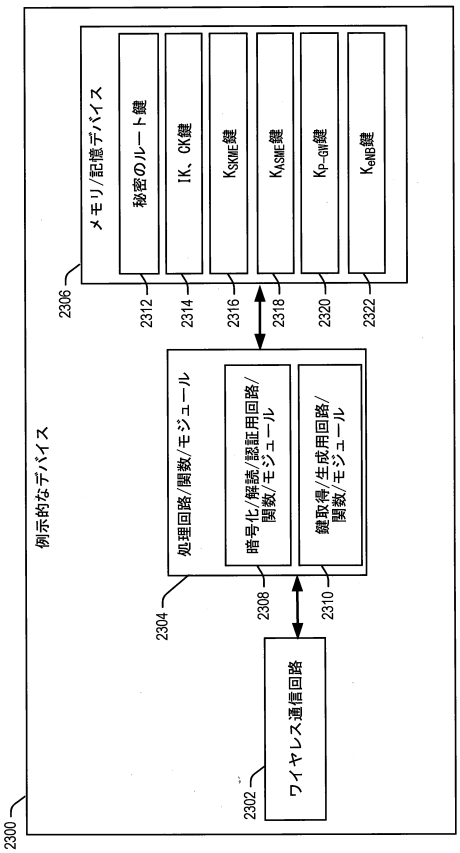
【図２１】



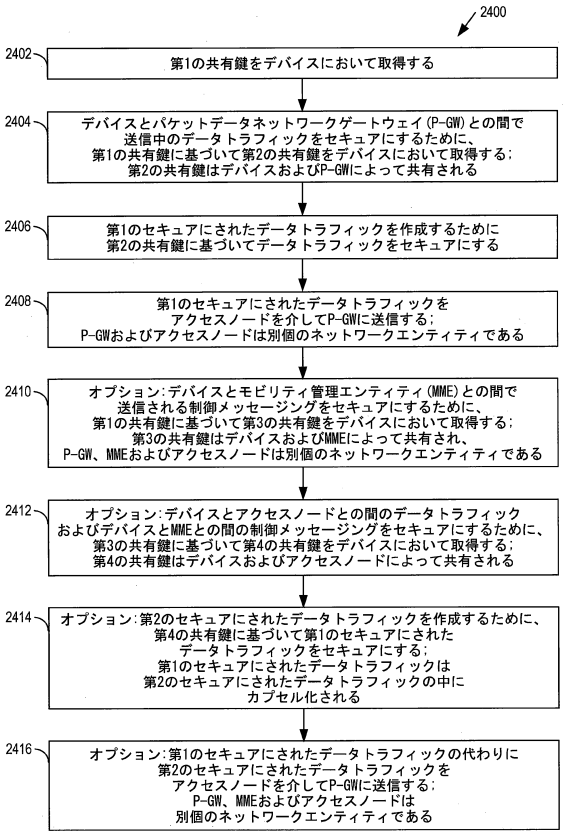
【図２２】



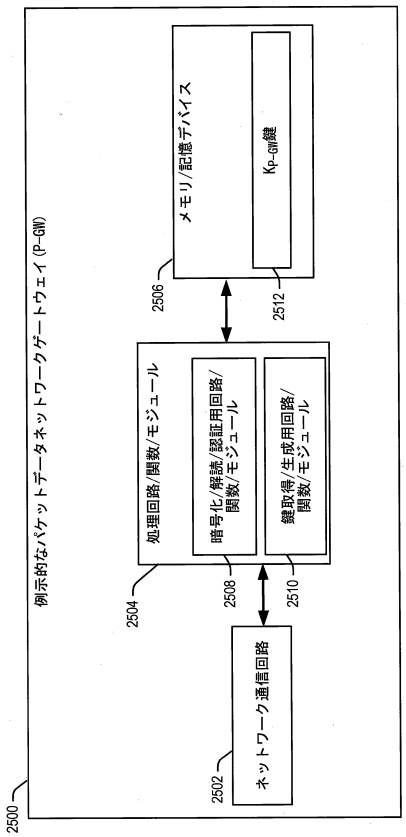
【図２３】



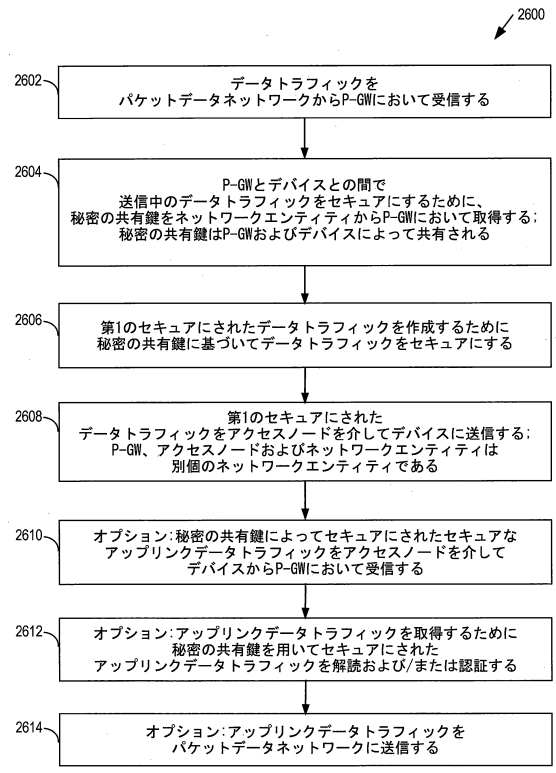
【図２４】



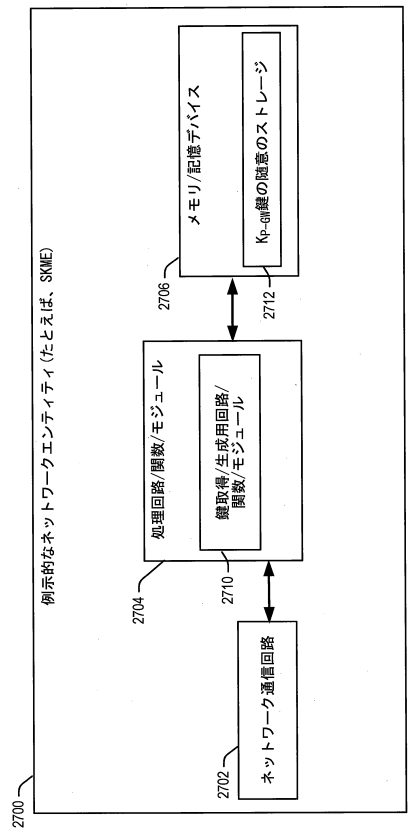
【図２５】



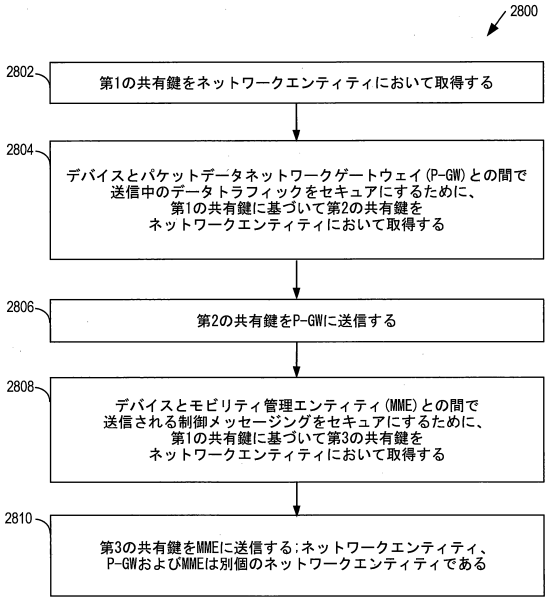
【図２６】



【図２７】



【図２８】


2800
2802
第1の共有鍵をネットワークエンティティにおいて取得する
2804
デバイスとパケットデータネットワークゲートウェイ(P-GW)との間で
送信中のデータトラフィックをセキュアにするために、
第1の共有鍵に基づいて第2の共有鍵を
ネットワークエンティティにおいて取得する
2806
第2の共有鍵をP-GWに送信する
2808
デバイスとモビリティ管理エンティティ(MME)との間で
送信される制御メッセージングをセキュアにするために、
第1の共有鍵に基づいて第3の共有鍵を
ネットワークエンティティにおいて取得する
2810
第3の共有鍵をMMEに送信する;ネットワークエンティティ、
P-GWおよびMMEは別個のネットワークエンティティである

フロントページの続き

(31)優先権主張番号　14/923,223
(32)優先日　平成27年10月26日(2015.10.26)
(33)優先権主張国・地域又は機関
米国(US)

(72)発明者　ギャヴィン・バーナード・ホーン
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５
(72)発明者　アナンド・パラニグンダー
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５

合議体
審判長　廣川　浩
審判官　中木　努
審判官　望月　章俊

(56)参考文献　特表２０１３－５４６２３３（ＪＰ，Ａ）
国際公開第２０１４／０４１８０６（WO，Ａ1）
３GPP　TS　33．４０２　V12．４．０（２０１４－０９），p３９－４２，２０１４年9月２６日アップロード，URL：ｈｔｔｐｓ：／／www．３ｇｐｐ．ｏｒｇ／ｆｔｐ／Ｓｐｅｃｓ／ａｒｃｈｉｖｅ／３３_ｓｅｒｉｅｓ／３３．４０２／３３４０２－ｃ４０．ｚｉｐ

(58)調査した分野(Int.Cl.，ＤＢ名)
H04W4/00-99/00