

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号

特許第7217271号

(P7217271)

(45)発行日 令和5年2月2日(2023.2.2)

(24)登録日 令和5年1月25日(2023.1.25)

(51)国際特許分類

F I

H 0 4 W 12/041 (2021.01)

H 0 4 W 12/041

H 0 4 W 76/10 (2018.01)

H 0 4 W 76/10

H 0 4 L 9/08 (2006.01)

H 0 4 L 9/08

C

請求項の数 16 (全33頁)

(21)出願番号 特願2020-518458(P2020-518458)

(86)(22)出願日 平成30年9月29日(2018.9.29)

(65)公表番号 特表2020-536426(P2020-536426
A)

(43)公表日 令和2年12月10日(2020.12.10)

(86)国際出願番号 PCT/US2018/053661

(87)国際公開番号 WO2019/070542

(87)国際公開日 平成31年4月11日(2019.4.11)

審査請求日 令和3年9月6日(2021.9.6)

(31)優先権主張番号 62/567,086

(32)優先日 平成29年10月2日(2017.10.2)

(33)優先権主張国・地域又は機関
米国(US)

(31)優先権主張番号 16/146,709

(32)優先日 平成30年9月28日(2018.9.28)

最終頁に続く

(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 9 2 1
2 1 サン ディエゴ モアハウス ドライ
ブ 5 7 7 5

(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 ス・ボム・イ

アメリカ合衆国・カリフォルニア・9 2
1 2 1 - 1 7 1 4・サン・ディエゴ・モ
アハウス・ドライヴ・5 7 7 5

(72)発明者 エイドリアン・エドワード・エスコット

アメリカ合衆国・カリフォルニア・9 2

最終頁に続く

(54)【発明の名称】 ネットワークポリシーの鍵生成への組み込み

(57)【特許請求の範囲】

【請求項 1】

ユーザ機器(UE)によるワイヤレス通信のための方法であって、
ネットワークとのセキュアな接続を確立するために第1のメッセージを受信するステッ
プであって、前記第1のメッセージはネットワークポリシー情報を含む、ステップと、
前記ネットワークポリシー情報に部分的に基づいて第1の鍵を生成するステップと、
前記第1の鍵を使用して前記ネットワークポリシー情報を検証するステップとを含む、
方法。

【請求項 2】

前記第1のメッセージが、前記ネットワークポリシー情報が有効である時間量をさらに
含む、請求項1に記載の方法。

10

【請求項 3】

前記第1の鍵が、前記ネットワーク内の前記UEとセキュリティアンカー機能(SEAF)との
間で共有されるアンカー鍵、または前記ネットワークポリシー情報が有効である前記時間
量のうちの少なくとも1つにさらに基づいて生成される、請求項2に記載の方法。

【請求項 4】

前記第1のメッセージを受信する前に、前記SEAFとの認証手順または登録手順のうちの
少なくとも1つを実行するステップをさらに含み、前記アンカー鍵が、前記認証手順また
は前記登録手順のうちの少なくとも1つに基づいて確立される、請求項3に記載の方法。

【請求項 5】

20

前記ネットワークポリシー情報が、前記ネットワークとの通信セッションを確立するとき、前記UEがセッション管理トークンを前記ネットワーク内のセッション管理機能(SMF)から受信することになるかどうかの指示を含む、請求項1に記載の方法。

【請求項6】

前記第1のメッセージが、前記ネットワーク内のアクセスおよびモビリティ管理機能(AMF)から受信される、請求項1に記載の方法。

【請求項7】

ネットワークとのセキュアな接続を確立するために第1のメッセージを受信するための手段であって、前記第1のメッセージはネットワークポリシー情報を含む、手段と、
前記ネットワークポリシー情報に部分的に基づいて第1の鍵を生成するための手段と、
前記第1の鍵を使用して前記ネットワークポリシー情報を検証するための手段と
を備える、ユーザ機器(UE)。

10

【請求項8】

セキュリティアンカー機能(SEAF)によるワイヤレス通信のための方法であって、
ネットワークポリシー情報に少なくとも部分的に基づいてネットワークノードに対する鍵を生成するステップであって、前記鍵は、ユーザ機器(UE)と前記ネットワークノードとの間のセキュアな接続を確立するために使用され、前記ネットワークポリシー情報がネットワークのセキュリティ特徴を含む、ステップと、
前記鍵を前記ネットワークノードに送るステップとを含む、方法。

【請求項9】

前記鍵を生成する前に、前記UEとの認証手順または登録手順のうちの少なくとも1つに関与するステップをさらに含み、前記関与するステップが、前記UEと前記SEAFとの間で共有されるべきアンカー鍵を確立するステップを含む、請求項8に記載の方法。

20

【請求項10】

前記鍵が、前記アンカー鍵または前記ネットワークポリシー情報が有効である時間量のうちの少なくとも1つにさらに基づいて生成される、請求項9に記載の方法。

【請求項11】

前記ネットワークポリシー情報または前記ネットワークポリシー情報が有効である前記時間量のうちの少なくとも1つを前記ネットワークノードに送るステップをさらに含み、請求項10に記載の方法。

30

【請求項12】

前記ネットワークポリシー情報が、ネットワーク内のセッション管理機能(SMF)が前記UEと前記ネットワークとの間の通信セッションに対するセッション管理トークンを生成して、前記セッション管理トークンを前記UEに送信することになっているかどうかの指示を含む、請求項8に記載の方法。

【請求項13】

前記UEのポリシー情報を含むメッセージを受信するステップをさらに含み、UEポリシー情報は、UE能力情報またはUEセキュリティ情報のうちの少なくとも1つを含む、請求項8に記載の方法。

【請求項14】

ネットワークポリシー情報に少なくとも部分的に基づいてネットワークノードに対する鍵を生成するための手段であって、前記鍵は、ユーザ機器(UE)と前記ネットワークノードとの間のセキュアな接続を確立するために使用され、前記ネットワークポリシー情報がネットワークのセキュリティ特徴を含む、手段と、

40

前記鍵を前記ネットワークノードに送るための手段と
を備える、セキュリティアンカー機能(SEAF)。

【請求項15】

ユーザ機器(UE)のプロセッサによる実行時に、請求項1～6のいずれか一項に記載の方法を前記プロセッサに実行させる命令を備えたコンピュータプログラム。

【請求項16】

50

セキュリティアンカー機能(SEAF)のプロセッサによる実行時に、請求項8～13のいずれか一項に記載の方法を前記プロセッサに実行させる命令を備えたコンピュータプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

米国特許法第119条に基づく優先権の主張

本出願は、2017年10月2日に出願した米国仮特許出願第62/567,086号の利益を主張する2018年9月28日に出願した米国出願第16/146,709号の優先権を主張するものであり、その内容全体が参照により本明細書に組み込まれる。

【0002】

本開示のいくつかの態様は、一般にワイヤレス通信に関し、より詳細には、ネットワーク内でセキュアな通信を確立するための方法および装置に関する。

【背景技術】

【0003】

ワイヤレス通信システムは、電話、ビデオ、データ、メッセージング、およびブロードキャストなどの様々な電気通信サービスを提供するために広く展開されている。一般のワイヤレス通信システムは、利用可能なシステムリソース(たとえば、帯域幅、送信電力)を共有することによって複数のユーザとの通信をサポートすることが可能な多元接続技術を採用してもよい。そのような多元接続技術の例は、ロングタームエボリューション(LTE)システム、符号分割多元接続(CDMA)システム、時分割多元接続(TDMA)システム、周波数分割多元接続(FDMA)システム、直交周波数分割多元接続(OFDMA)システム、シングルキャリア周波数分割多元接続(SC-FDMA)システム、および時分割同期符号分割多元接続(TD-SCDMA)システムを含む。

【0004】

いくつかの例では、ワイヤレス多元接続通信システムは、ユーザ機器(UE)としても知られている複数の通信デバイスのための通信を各々が同時にサポートする、いくつかの基地局を含んでもよい。LTEまたはLTE-Aネットワークでは、1つまたは複数の基地局のセットがeノードB(eNB)を定義してもよい。他の例では(たとえば、次世代または5Gネットワークでは)、ワイヤレス多元接続通信システムは、いくつかの集約ユニット(CU)(たとえば、中央ノード(CN)、アクセスノードコントローラ(ANC)など)と通信するいくつかの分散ユニット(DU)(たとえば、エッジユニット(EU)、エッジノード(EN)、無線ヘッド(RH)、スマート無線ヘッド(SRH)、送信受信ポイント(TRP)など)を含んでもよく、集約ユニットと通信する1つまたは複数の分散ユニットのセットがアクセスノード(たとえば、ニューラジオ基地局(NR BS:new radio base station)、ニューラジオノードB(NR NB:new radio node-B)、ネットワークノード、5G NB、gNBなど)を定義してもよい。基地局またはDUは、(たとえば、基地局から、またはUEへの送信のための)ダウンリンクチャネルおよび(たとえば、UEから基地局または分散ユニットへの送信のための)アップリンクチャネル上でUEのセットと通信してもよい。

【0005】

これらの多元接続技術は、異なるワイヤレスデバイスが都市、国家、地域、さらには地球規模で通信することを可能にする共通プロトコルを提供するために、様々な電気通信規格において採用されている。新興の電気通信規格の一例は、ニューラジオ(NR)、たとえば5G無線アクセスである。NRは、第3世代パートナーシッププロジェクト(3GPP)によって公表されたLTEモバイル規格に対する拡張のセットである。それは、スペクトル効率を改善し、コストを削減し、サービスを改善し、新しいスペクトルを利用し、またダウンリンク(DL)およびアップリンク(UL)上でOFDMAをサイクリックプレフィックス(CP)とともに使用する他のオープン規格とよりうまく統合することによって、モバイルブロードバンドインターネットアクセスをよりうまくサポートし、ならびにビームフォーミング、多入力多出力(MIMO)アンテナ技術、およびキャリアアグリゲーションをサポートするように設計されている。

10

20

30

40

50

【 0 0 0 6 】

しかしながら、モバイルブロードバンドアクセスに対する需要が増大し続けるにつれて、NR技術におけるさらなる改善が必要である。好ましくは、これらの改善は、他の多元接続技術、およびこれらの技術を用いる電気通信規格に適用可能であるべきである。

【 発明の概要 】

【 課題を解決するための手段 】

【 0 0 0 7 】

本開示のシステム、方法、およびデバイスはそれぞれ、いくつかの態様を有し、それらのうちの単一の態様だけが、その望ましい属性を担うわけではない。以下の特許請求の範囲によって表される本開示の範囲を限定することなく、いくつかの特徴についてここで簡潔に説明する。この説明を考慮した後、また特に「発明を実施するための形態」と題するセクションを読んだ後、本開示の特徴が、ワイヤレスネットワークにおける改善された通信を含む利点をどのようにもたらすかが理解されよう。

10

【 0 0 0 8 】

本開示のいくつかの態様は、ユーザ機器(UE)によるワイヤレス通信のための方法を提供する。方法は、一般に、ネットワークとのセキュアな接続を確立するために第1のメッセージを受信するステップを含み、第1のメッセージはネットワークポリシー情報を含む。方法は、ネットワークポリシー情報に部分的に基づいて第1の鍵を生成するステップも含む。方法は、第1の鍵を使用してネットワーク情報を検証するステップをさらに含む。

【 0 0 0 9 】

20

本開示のいくつかの態様は、セキュリティアンカー機能(SEAF:security anchor function)など、ネットワークノードによるワイヤレス通信のための方法を提供する。方法は、一般に、ネットワークポリシー情報に少なくとも部分的に基づいてネットワークノードに対する鍵を生成するステップを含む。鍵は、UEとネットワークノードとの間にセキュアな接続を確立するために使用される。方法は、鍵をネットワークノードに送るステップも含み得る。

【 0 0 1 0 】

本開示のいくつかの態様は、ユーザ機器(UE)によるワイヤレス通信のための方法を提供する。方法は、一般に、ネットワークとの認証手順に基づいて、ネットワーク内でUEとセキュリティアンカー機能(SEAF)との間で共有されるアンカー鍵を確立するステップを含む。方法は、ネットワークとのセキュアな接続を確立するために第1のメッセージを受信するステップも含み、第1のメッセージは、ネットワークとの通信セッションに対するネットワークポリシートークン、ネットワークポリシー情報、第1の鍵が有効である第1の時間量、およびネットワークポリシートークンが有効である第2の時間量を含む。方法は、ネットワークとのセキュアな接続を確立する前に、共有アンカー鍵から導出された鍵、ネットワークポリシー情報、第1の時間量、および第2の時間量に基づいて、ネットワークポリシートークンが有効であるかどうかを決定するステップをさらに含む。

30

【 0 0 1 1 】

本開示のいくつかの態様は、セキュリティアンカー機能(SEAF)など、ネットワークノードによるワイヤレス通信のための方法を提供する。方法は、一般に、UEとの認証手順に基づいて、ネットワーク内でSEAFとUEとの間で共有されるアンカー鍵を確立するステップを含む。方法は、アンカー鍵、ネットワークポリシー情報、およびネットワークポリシートークンが有効である第1の時間量に部分的に基づいてネットワークポリシートークンを生成するステップも含む。方法は、別のネットワークノードに対する鍵を生成するステップと、鍵、ネットワークポリシー情報、およびネットワークポリシートークンを他のネットワークノードに送るステップとをさらに含む。

40

【 0 0 1 2 】

上記で説明した動作を実行することができる方法、装置、システム、コンピュータプログラム製品、および処理システムを含む多数の他の態様が提供される。

【 0 0 1 3 】

50

上記の目的および関係する目的を達成するために、1つまたは複数の態様は、以下で十分に説明され、特に特許請求の範囲で指摘される特徴を含む。以下の説明および添付の図面は、1つまたは複数の態様のいくつかの例示的な特徴を詳細に記載する。しかしながら、これらの特徴は、様々な態様の原理が利用されてもよい様々な方法のほんのいくつかを示すものであり、この説明は、すべてのそのような態様およびそれらの均等物を含むものである。

【0014】

本開示の上記の特徴が詳細に理解されてもよいように、上記で簡単に要約したより具体的な説明が、態様を参照することによって行われることがあり、態様のうちのいくつかは添付の図面に示される。しかしながら、本説明は他の等しく効果的な態様に通じ得るので、添付の図面が、本開示のいくつかの典型的な態様のみを示し、したがって本開示の範囲を限定するものと見なされるべきではないことに留意されたい。

【図面の簡単な説明】

【0015】

【図1】本開示のいくつかの態様による、例示的な電気通信システムを概念的に示すブロック図である。

【図2】本開示のいくつかの態様による、分散型RANの例示的な論理アーキテクチャを示すブロック図である。

【図3】本開示のいくつかの態様による、分散型RANの例示的な物理アーキテクチャを示す図である。

【図4】本開示のいくつかの態様による、例示的なBSおよびユーザ機器(UE)の設計を概念的に示すブロック図である。

【図5】本開示のいくつかの態様による、通信プロトコルスタックを実装するための例を示す図である。

【図6】本開示のいくつかの態様による、DL中心のサブフレームの一例を示す図である。

【図7】本開示のいくつかの態様による、UL中心のサブフレームの一例を示す図である。

【図8】本開示のいくつかの態様による、1つまたは複数の非コロケートネットワークノードを有する例示的な5Gアーキテクチャを示す図である。

【図9】本開示のいくつかの態様による、1つまたは複数の非コロケートネットワークノードを有する例示的な5Gアーキテクチャを示す図である。

【図10】本開示のいくつかの態様による、ネットワーク内のワイヤレス通信のための例示的な動作を示すフロー図である。

【図11】本開示のいくつかの態様による、ネットワーク内のワイヤレス通信のための例示的な動作を示すフロー図である。

【図12】本開示のいくつかの態様による、例示的な登録手順を示すコールフロー図である。

【図13】本開示のいくつかの態様による、ネットワーク内のワイヤレス通信のための例示的な動作を示すフロー図である。

【図14】本開示のいくつかの態様による、ネットワーク内のワイヤレス通信のための例示的な動作を示すフロー図である。

【図15】本開示のいくつかの態様による、例示的な登録手順を示すコールフロー図である。

【発明を実施するための形態】

【0016】

理解を容易にするために、可能な場合、図に共通する同一の要素を示すために、同一の参照番号が使用されている。特定の記載なしに、一実施形態において開示する要素が他の実施形態において有利に利用されてもよいことが企図される。

【0017】

本開示の態様は、ニューラジオ(NR)(ニューラジオアクセス技術または5G技術)ワイヤレスネットワークなどのワイヤレスネットワークのための装置、方法、処理システム、およ

10

20

30

40

50

びコンピュータ可読媒体を提供する。

【0018】

NRは、拡張モバイルブロードバンド(eMBB:Enhanced mobile broadband)ターゲットの広い帯域幅(たとえば、80MHzを越える)、ミリ波(mmW:millimeter wave)ターゲットの高いキャリア周波数(たとえば、60GHz)、マッシュMTC(mMTC)ターゲットの後方互換性のないMTC技法、および/またはミッションクリティカルターゲットの超高信頼低レイテンシ通信(URLLC:ultra reliable low latency communication)などの、様々なワイヤレス通信サービスをサポートし得る。これらのサービスは、レイテンシ要件および信頼性要件を含んでもよい。これらのサービスはまた、それぞれのサービス品質(QoS)要件を満たすための異なる送信時間間隔(TTI)を有することがある。加えて、これらのサービスは、同じサブフレームにおいて共存してもよい。

10

【0019】

NRは、ネットワークスライシングの概念を導入する。たとえば、ネットワークは、種々のサービス、たとえば、インターネットオブエブリシング(IoE)、URLLC、eMBB、車両間(V2V)通信などをサポートし得るマルチスライス(multiple slices)を有し得る。スライスは、いくつかのネットワーク能力およびネットワーク特性を提供するために必要なネットワーク機能および対応するリソースのセットを含む完全な論理ネットワークとして定義され得る。

【0020】

いくつかの態様では、5G NRシステムは、様々な異なる配置シナリオをサポート可能であり得る。特に、5G技術および/またはサービス要件が継続的に発達するにつれて、5Gネットワーク内で1つまたは複数のネットワークノードによって実行されるサービス、能力、および/または機能は変化することがある。ネットワークアーキテクチャにおける変化がUEに知られていないことがあるので、特定のネットワーク構成、能力、セキュリティ構成などについて、UEに知らせることは有益である。しかしながら、ネットワークに対する現在の技法を使用して、ネットワーク(セキュリティ)構成、能力、およびポリシーについてセキュアな方法でUEに知らせることは不可能である。

20

【0021】

たとえば、5Gシステムでは、一般的に、UEとサービングネットワークとの間に単一の制御プレーンインターフェース(N1)が存在する。このN1インターフェースは、一般に、UEとアクセスおよびモビリティ管理機能(AMF:access and mobility management function)との間の非アクセス層(NAS:non-access stratum)接続を確立するために使用される。しかしながら、いくつかの配置シナリオでは、AMFは、ネットワーク内でセキュリティ機能の役目を果たさない(セキュリティ機能にアクセスできない)場合がある。したがって、AMFは、UEとのシグナリング接続を有する唯一のエンティティであり得るので、(不正なまたは悪意のある)AMFは、ネットワーク構成情報をインターセプトして、UEに提供されるネットワーク構成情報を修正し、UEとネットワークとの間の接続/通信に不正アクセスすることができる場合があり得る。それに応じて、本開示の態様は、ネットワーク(セキュリティ)構成、能力、ネットワークポリシーなどについてUEにセキュアに知らせるための技法を提供する。

30

【0022】

本開示の様々な態様は、添付の図面を参照しながら以下でより十分に説明される。しかしながら、本開示は、多くの異なる形態で具現化されてもよく、本開示全体にわたって提示される任意の特定の構造または機能に限定されるものと解釈されるべきでない。むしろ、これらの態様は、本開示が周到で完全になり、本開示の範囲を当業者に十分に伝えるために提供される。本明細書の教示に基づいて、本開示の範囲は、本開示の任意の他の態様とは独立して実施されるにしても、本開示の任意の他の態様と組み合わせて実施されるにしても、本明細書において開示される本開示のあらゆる態様を包含することを意図していることは、当業者は理解されたい。たとえば、本明細書に記載される任意の数の態様を使用して、装置が実装されてもよく、または方法が実践されてもよい。加えて、本開示の範

40

50

図は、本明細書に記載された本開示の様々な態様に加えて、またはそれらの態様以外に、他の構造、機能、または構造および機能を使用して実践されるそのような装置または方法を包含するものとする。本明細書で開示する本開示のいずれの態様も、請求項の1つまたは複数の要素によって具現化されてもよいことを理解されたい。

【0023】

「例示的」という語は、本明細書では「例、事例、または例示として機能すること」を意味するために使用される。本明細書で「例示的」であるものとして説明されるいずれの態様も、必ずしも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。

【0024】

特定の態様について本明細書で説明するが、これらの態様の多くの変形および置換が、本開示の範囲内に入る。好ましい態様のいくつかの利益および利点について述べるが、本開示の範囲は、特定の利益、用途、または目的に限定されるものではない。そうではなく、本開示の態様は、様々なワイヤレス技法、システム構成、ネットワーク、および送信プロトコルに広く適用可能であることが意図され、それらのうちのいくつかは例として図および好ましい態様の以下の説明において示される。詳細な説明および図面は、限定ではなく、本開示の単なる例示であり、本開示の範囲は、添付の特許請求の範囲およびその均等物によって定義される。

【0025】

本明細書で説明する技法は、CDMA、TDMA、FDMA、OFDMA、SC-FDMA、および他のネットワークなどの様々なワイヤレス通信ネットワークに使用されてもよい。「ネットワーク」および「システム」という用語は、しばしば互換的に使用される。CDMAネットワークは、ユニバーサル地上波無線アクセス(UTRA)、cdma2000などの無線技術を実装し得る。UTRAは、広帯域CDMA(WCDMA(登録商標))、時分割同期CDMA(TD-SCDMA)、およびCDMAの他の変形を含む。cdma2000は、IS-2000規格、IS-95規格、およびIS-856規格を対象とする。TDMAネットワークは、モバイル通信用グローバルシステム(GSM(登録商標))などの無線技術を実装してもよい。OFDMAネットワークは、発展型UTRA(E-UTRA)、ウルトラモバイルブロードバンド(UMB)、IEEE 802.11(Wi-Fi)、IEEE 802.16(WiMAX)、IEEE 802.20、Flash-OFDMA(登録商標)などの無線技術を実装してもよい。UTRAおよびE-UTRAは、ユニバーサルモバイルテレコミュニケーションシステム(UMTS)の一部である。3GPPロングタームエボリューション(LTE)およびLTEアドバンスド(LTE-A)は、周波数分割複信(FDD)と時分割複信(TDD)の両方において、ダウンリンク上でOFDMAを、またアップリンク上でSC-FDMAを採用する、E-UTRAを使用するUMTSの新たなリリースである。UTRA、E-UTRA、UMTS、LTE、LTE-AおよびGSM(登録商標)は、「第3世代パートナーシッププロジェクト」(3GPP)と称する団体による文書に記載されている。cdma2000およびUMBは、「第3世代パートナーシッププロジェクト2」(3GPP2)と称する団体の文書に記載されている。本明細書で説明する技法は、上述のワイヤレスネットワークおよび無線技術、ならびに5G次世代/NRネットワークなど、他のワイヤレスネットワークおよび無線技術のために使用され得る。

【0026】

例示的なワイヤレス通信システム

図1は、ニューラジオ(NR)または5Gネットワークなどの例示的なワイヤレスネットワーク100を示し、本開示の態様は、たとえば、UEネットワーク(セキュリティ)ポリシー情報(たとえば、ネットワーク構成、セキュリティ情報、能力など)をセキュアに提供するために実行され得る。場合によっては、ネットワーク100は、各スライスが、的確に構成されたネットワーク機能、ネットワーク適用例、および特定の使用事例またはビジネスモデルの要件を満足するためにともにバンドリングされる下位のクラウドインフラストラクチャの組成として定義されるマルチスライスネットワークであり得る。

【0027】

図1に示すように、ワイヤレスネットワーク100は、いくつかのBS110と他のネットワークエンティティとを含んでもよい。BSは、UEと通信する局であってもよい。各BS110

10

20

30

40

50

は、特定の地理的エリアに通信カバレッジを提供してもよい。3GPPでは、「セル」という用語は、この用語が使用される状況に応じて、このカバレッジエリアにサービスしているノードBおよび/またはノードBサブシステムのカバレッジエリアを指すことがある。NRシステムでは、「セル」およびeNB、ノードB、5G NB、AP、NR BS、またはTRPなどの用語は交換可能であってもよい。いくつかの例では、セルは、必ずしも静止しているとは限らないことがあり、セルの地理的エリアは、モバイル基地局のロケーションに従って移動してもよい。いくつかの例では、基地局は、任意の適切なトランスポートネットワークを使用して、直接物理接続、仮想ネットワークなどの様々なタイプのバックホールインターフェースを通じて、ワイヤレスネットワーク100内で互いに、および/または1つもしくは複数の他の基地局もしくはネットワークノード(図示せず)に相互接続されてもよい。

10

【0028】

一般に、任意の数のワイヤレスネットワークが、所与の地理的エリアにおいて展開されてもよい。各ワイヤレスネットワークは、特定の無線アクセス技術(RAT)をサポートしてもよく、1つまたは複数の周波数で動作してもよい。RATは、無線技術、エアインターフェースなどと呼ばれることもある。周波数は、キャリア、周波数チャネルなどと呼ばれることもある。各周波数は、異なるRATのワイヤレスネットワーク間の干渉を回避するために、所与の地理的エリアにおいて単一のRATをサポートしてもよい。場合によっては、マルチスライスネットワークアーキテクチャを採用する、NRまたは5G RATネットワークが展開されてよい。

【0029】

20

BSは、マクロセル、ピコセル、フェムトセル、および/または他のタイプのセルのための通信カバレッジを提供してもよい。マクロセルは、比較的大きな地理的エリア(たとえば、半径数千メートル)をカバーすることができ、サービスに加入しているUEによる無制限アクセスを可能にしてもよい。ピコセルは、比較的小さい地理的エリアをカバーすることができ、サービスに加入しているUEによる無制限アクセスを可能にしてもよい。フェムトセルは、比較的小さい地理的エリア(たとえば、自宅)をカバーすることができ、フェムトセルとの関連を有するUE(たとえば、限定加入者グループ(CSG)内のUE、自宅内のユーザのためのUEなど)による制限付きアクセスを可能にしてもよい。マクロセルのためのBSは、マクロBSと呼ばれることがある。ピコセルのためのBSは、ピコBSと呼ばれることがある。フェムトセルのためのBSは、フェムトBSまたはホームBSと呼ばれることがある。図1に示す例では、BS110a、110bおよび110cは、それぞれマクロセル102a、102bおよび102cのためのマクロBSであってもよい。BS110xは、ピコセル102xのためのピコBSであってもよい。BS110yおよび110zは、それぞれフェムトセル102yおよび102zのためのフェムトBSであってもよい。BSは1つまたは複数(たとえば、3つ)のセルをサポートしてもよい。

30

【0030】

ワイヤレスネットワーク100は、中継局も含んでもよい。中継局は、アップストリーム局(たとえばBSまたはUE)からデータおよび/または他の情報の送信を受信し、ダウンストリーム局(たとえば、UEまたBS)にデータおよび/または他の情報の送信を送る局である。また、中継局は、他のUEのための送信を中継するUEであってもよい。図1に示す例では、中継局110rは、BS110aとUE120rとの間の通信を容易にするために、BS110aおよびUE120rと通信することができる。中継局はまた、リレーBS、リレーなどと呼ばれることもある。

40

【0031】

ワイヤレスネットワーク100は、異なるタイプのBS、たとえばマクロBS、ピコBS、フェムトBS、リレーなどを含む異種ネットワークとすることができる。これらの異なるタイプのBSは、異なる送信電力レベル、異なるカバレッジエリア、およびワイヤレスネットワーク100中の干渉に対する異なる影響を有してもよい。たとえば、マクロBSは高い送信電力レベル(たとえば、20ワット)を有することがあり、一方で、ピコBS、フェムトBS、およびリレーはより低い送信電力レベル(たとえば、1ワット)を有することがある。

50

【0032】

ワイヤレスネットワーク100は、同期動作または非同期動作をサポートしてもよい。同期動作の場合、BSは、同様のフレームタイミングを有することができ、異なるBSからの送信は、時間的にほぼ整合してもよい。非同期動作の場合、BSは、異なるフレームタイミングを有する場合があります、異なるBSからの送信は、時間的に整合していない場合がある。本明細書で説明する技法は、同期動作と非同期動作の両方に使用されてもよい。

【0033】

ネットワークコントローラ130は、BSのセットに結合し、これらのBSのための調整および制御を行ってもよい。ネットワークコントローラ130は、バックホールを介してBS110と通信してもよい。BS110はまた、たとえば直接または間接的にワイヤレスバックホールもしくは有線バックホールを介して互いに通信してもよい。

10

【0034】

UE120(たとえば、120x、120yなど)は、ワイヤレスネットワーク100の全体にわたって分散されてもよく、各UEは静止であってもよく、またはモバイルであってもよい。UEは、移動局、端末、アクセス端末、加入者ユニット、局、顧客構内設備(CPE:Customer Premises Equipment)、セルラーフォン、スマートフォン、携帯情報端末(PDA)、ワイヤレスモデム、ワイヤレス通信デバイス、ハンドヘルドデバイス、ラップトップコンピュータ、コードレスフォン、ワイヤレスローカルループ(WLL)局、タブレット、カメラ、ゲームデバイス、ネットブック、スマートブック、ウルトラブック、医療デバイスもしくは医療機器、生体センサ/デバイス、スマートウォッチ、スマート衣料、スマートグラス、スマートリストバンド、スマートジュエリー(たとえば、スマートリング、スマートブレスレットなど)などのウェアラブルデバイス、娯楽デバイス(たとえば、音楽デバイス、ビデオデバイス、衛星無線など)、車両コンポーネントもしくは車両センサ、スマートメータ/センサ、工業生産機器、全地球測位システムデバイス、またはワイヤレス媒体もしくはワイヤード媒体を介して通信するように構成される任意の他の適切なデバイスと呼ばれる場合もある。一部のUEは、発展型デバイスもしくはマシンタイプ通信(MTC)デバイスまたは発展型MTC(eMTC)デバイスと見なされる場合がある。MTC UEおよびeMTC UEは、BS、別のデバイス(たとえば、リモートデバイス)、または何らかの他のエンティティと通信することができる、たとえばロボット、ドローン、リモートデバイス、センサ、メータ、モニタ、ロケーションタグなどを含む。ワイヤレスノードは、たとえばワイヤード通信リンクまたはワイヤレス通信リンクを介して、ネットワーク(たとえば、インターネットもしくはセルラーネットワークなどのワイドエリアネットワーク)のための、またはネットワークへの接続性を提供してもよい。一部のUEは、モノのインターネット(IoT)デバイスと見なされてもよい。

20

30

【0035】

図1において、両矢印を有する実線は、UEとサービングBSとの間の所望の送信を示し、サービングBSは、ダウンリンクおよび/またはアップリンク上でUEにサービスするように指定されたBSである。両矢印を有する破線は、UEとBSとの間の干渉する送信を示す。

【0036】

特定のワイヤレスネットワーク(たとえば、LTE)は、ダウンリンク上で直交周波数分割多重化(OFDM)を利用し、かつアップリンク上でシングルキャリア周波数分割多重化(SC-FDM)を利用する。OFDMおよびSC-FDMは、システム帯域幅を、一般にトーン、ビンなどとも呼ばれる複数の(K個の)直交サブキャリアに区分する。各サブキャリアは、データで変調されてもよい。一般に、変調シンボルは、OFDMでは周波数領域において送られ、SC-FDMでは時間領域において送られる。隣接するサブキャリア間の間隔は固定される場合があり、サブキャリアの総数(K)は、システム帯域幅に依存する場合がある。たとえば、サブキャリアの間隔は15kHzであってもよく、最小のリソース割振り(「リソースブロック」と呼ばれる)は12個のサブキャリア(または180kHz)であってもよい。その結果、公称FFTサイズは、1.25、2.5、5、10または20メガヘルツ(MHz)のシステム帯域幅に対して、それぞれ128、256、512、1024または2048に等しくなってもよい。システム帯域幅はま

40

50

た、サブバンドに区分されてもよい。たとえば、サブバンドは、1.08MHz(すなわち、6個のリソースブロック)をカバーすることができ、1.25、2.5、5、10または20MHzのシステム帯域幅に対して、それぞれ1、2、4、8または16個のサブバンドが存在してもよい。

【0037】

本明細書で説明する例の態様はLTE技術に関連付けられてもよいが、本開示の態様は、NR/5Gなどの他のワイヤレス通信システムに適用可能であってもよい。

【0038】

NRは、アップリンクおよびダウンリンク上でCPを用いてOFDMを利用し、TDDを使用する半二重動作に対するサポートを含んでもよい。100MHzの単一のコンポーネントキャリア帯域幅がサポートされてもよい。NRリソースブロックは、0.1msの持続時間にわたって、サブキャリア帯域幅が75kHzの12個のサブキャリアにまたがってもよい。各無線フレームは、10msの長さを有する50個のサブフレームで構成されてもよい。結果として、各サブフレームは0.2msの長さを有することができる。各サブフレームは、データ送信用のリンク方向(すなわち、DLまたはUL)を示してもよく、サブフレームごとのリンク方向は、動的に切り替えられてもよい。各サブフレームは、DL/ULデータならびにDL/UL制御データを含んでもよい。NRに関するULサブフレームおよびDLサブフレームは、図6および図7に関して以下でより詳細に説明されるようなものであってもよい。ビームフォーミングがサポートされてもよく、ビーム方向が動的に構成されてもよい。プリコーディングを用いたMIMO送信もサポートされてもよい。DLにおけるMIMO構成は、最大で8個のストリームおよびUEごとに最大で2個のストリームを用いたマルチレイヤDL送信で最大で8個の送信アンテナをサポートしてもよい。UEごとに最大で2個のストリームを用いたマルチレイヤ送信がサポートされてもよい。最大で8個のサービングセルを用いて複数のセルのアグリゲーションがサポートされてもよい。代替として、NRは、OFDMベース以外の異なるエアインターフェースをサポートしてもよい。NRネットワークは、CUおよび/またはDUなどのエンティティを含んでもよい。

【0039】

いくつかの例では、エアインターフェースへのアクセスがスケジュールされてもよく、スケジューリングエンティティ(たとえば、基地局)は、そのサービスエリアまたはセル内のいくつかのまたはすべてのデバイスおよび機器の間で通信のためのリソースを割り振る。本開示内では、以下でさらに説明するように、スケジューリングエンティティは、1つまたは複数の従属エンティティ用のリソースをスケジュールすること、割り当てること、再構成すること、および解放することを担当してもよい。すなわち、スケジュールされた通信に対して、従属エンティティは、スケジューリングエンティティによって割り振られたリソースを利用する。基地局は、スケジューリングエンティティとして機能してもよい。唯一のエンティティではない。すなわち、いくつかの例では、UEが、1つまたは複数の従属エンティティ(たとえば、1つまたは複数の他のUE)のためのリソースをスケジュールする、スケジューリングエンティティとして機能してもよい。この例では、UEは、スケジューリングエンティティとして機能しており、他のUEは、ワイヤレス通信のためにUEによってスケジュールされたリソースを利用する。UEは、ピアツーピア(P2P)ネットワーク中および/またはメッシュネットワーク中でスケジューリングエンティティとして機能してもよい。メッシュネットワーク例では、UEは、スケジューリングエンティティと通信することに加えて、場合によっては互いに直接通信してもよい。

【0040】

したがって、時間-周波数リソースへのスケジュールされたアクセスを伴い、セルラー構成、P2P構成、およびメッシュ構成を有するワイヤレス通信ネットワークでは、スケジューリングエンティティおよび1つまたは複数の従属エンティティは、スケジュールされたリソースを利用して通信してもよい。

【0041】

上述のように、RANは、CUおよびDUを含んでもよい。NR BS(たとえば、gNB、5Gノ

10

20

30

40

50

ードB、ノードB、送信受信ポイント(TRP)、アクセスポイント(AP))は、1つまたは複数のBSに対応してもよい。NRセルは、アクセスセル(ACell)またはデータオンリーセル(DCell)として構成されてもよい。たとえば、RAN(たとえば、集約ユニットまたは分散ユニット)は、セルを構成することができる。DCellは、キャリアアグリゲーションまたは二重接続性に使用されるが、初期アクセス、セル選択/再選択、またはハンドオーバーに使用されないセルであってもよい。場合によっては、DCellは同期信号を送信しないことがあり、場合によっては、DCellはSSを送信することがある。NR BSは、セルタイプを示すダウンリンク信号をUEに送信してもよい。セルタイプ指示に基づいて、UEはNR BSと通信してもよい。たとえば、UEは、示されたセルタイプに基づいて、セル選択用、アクセス用、ハンドオーバー用、および/または測定用と見なすべきNR BSを決定してもよい。

10

【0042】

図2は、図1に示したワイヤレス通信システム内で実装されてもよい分散型無線アクセスネットワーク(RAN)200の例示的な論理アーキテクチャを示す。5Gアクセスノード206は、アクセスノードコントローラ(ANC)202を含んでもよい。ANCは、分散型RAN200の集約ユニット(CU)であってもよい。次世代コアネットワーク(NG-CN:next generation core network)204へのバックホールインターフェースは、ANCにおいて終端してもよい。近隣次世代アクセスノード(NG-AN)へのバックホールインターフェースは、ANCにおいて終端してもよい。ANCは、1つまたは複数のTRP208(BS、NR BS、ノードB、5G NB、AP、または何らかの他の用語で呼ばれることもある)を含んでもよい。上記で説明したように、TRPは「セル」と交換可能に使用されてもよい。

20

【0043】

TRP208は、DUであってもよい。TRPは、1つのANC(ANC202)に接続されてもよく、または2つ以上のANC(図示せず)に接続されてもよい。たとえば、RAN共有、サービスとしての無線(RaaS:radio as a service)、およびサービス固有ANC配置に対して、TRPは2つ以上のANCに接続されてもよい。TRPは、1つまたは複数のアンテナポートを含んでもよい。TRPは、UEへのトラフィックを個別に(たとえば、動的選択)または一緒に(たとえば、共同送信)サービスするように構成されてもよい。

【0044】

ローカルアーキテクチャ200は、フロントホール定義を示すために使用されてもよい。異なる展開タイプにわたるフロントホール(fronthauling)解決策をサポートするアーキテクチャが定義されてもよい。たとえば、アーキテクチャは、送信ネットワーク能力(たとえば、帯域幅、レイテンシ、および/またはジッタ)に基づいてもよい。

30

【0045】

アーキテクチャは、特徴および/または構成要素をLTEと共有してもよい。態様によれば、次世代AN(NG-AN)210は、NRとの二重接続性をサポートしてもよい。NG-ANは、LTEおよびNRに対して共通フロントホールを共有してもよい。

【0046】

アーキテクチャは、TRP208間の協働を可能にしてもよい。たとえば、協働は、TRP内に事前設定されてもよく、かつ/またはANC202を経由してTRPにわたって事前設定されてもよい。態様によれば、TRP間インターフェースが必要とされない/存在しない場合がある。

40

【0047】

態様によれば、アーキテクチャ200内に、分割された論理機能の動的構成が存在する場合がある。図5を参照しながらより詳細に説明するように、無線リソース制御(RRC)レイヤ、パケットデータコンバージェンスプロトコル(PDCP)レイヤ、無線リンク制御(RLC)レイヤ、媒体アクセス制御(MAC)レイヤ、および物理(PHY)レイヤは、DUまたはCU(たとえば、それぞれTRPまたはANC)に適応可能に配置されてもよい。いくつかの態様によれば、BSは、集約ユニット(CU)(たとえば、ANC202)および/または1つもしくは複数の分散ユニット(たとえば、1つもしくは複数のTRP208)を含んでもよい。

【0048】

50

図3は、本開示のいくつかの態様による、分散型RAN300の例示的な物理アーキテクチャを示す。集中型コアネットワークユニット(C-CU)302が、コアネットワーク機能をホストしてもよい。C-CUは、中央に配置されてもよい。C-CU機能は、ピーク容量に対処しようとして、(たとえば、アドバンスドワイヤレスサービス(AWS)に)オフロードされてもよい。

【0049】

集中型RANユニット(C-RU)304が、1つまたは複数のANC機能をホストしてもよい。場合によっては、C-RUは、コアネットワーク機能を局所的にホストしてもよい。C-RUは分散配置を有してもよい。C-RUは、ネットワークエッジのより近くにあってもよい。

【0050】

DU306が、1つまたは複数のTRP(エッジノード(EN)、エッジユニット(EU)、無線ヘッド(RH)、スマート無線ヘッド(SRH)など)をホストしてもよい。DUは、無線周波数(RF)機能を備えたネットワークのエッジに位置してもよい。

【0051】

図4は、本開示の態様を実施するために使用されてもよい、図1に示すBS110およびUE120の例示的な構成要素を示す。上記で説明したように、BSはTRPを含んでもよい。BS110およびUE120の1つまたは複数の構成要素は、本開示の態様を実践するために使用されてもよい。たとえば、UE120のアンテナ452、Tx/Rx222、プロセッサ466、458、464、および/もしくはコントローラ/プロセッサ480、ならびに/またはBS110のアンテナ434、プロセッサ430、420、438、および/もしくはコントローラ/プロセッサ440は、本明細書で説明し、図10～図15を参照しながら示す動作を実行するために使用されてもよい。

【0052】

態様によれば、制限された接続シナリオの場合、基地局110は図1のマクロBS110cであってもよく、UE120はUE120yであってもよい。基地局110はまた、何らかの他のタイプの基地局であってもよい。基地局110は、アンテナ434a～434tを備えることができ、UE120は、アンテナ452a～452rを備えることができる。

【0053】

基地局110において、送信プロセッサ420は、データソース412からデータを受信し、コントローラ/プロセッサ440から制御情報を受信してもよい。制御情報は、物理ブロードキャストチャネル(PBCH)、物理制御フォーマットインジケータチャネル(PCFICH)、物理ハイブリッドARQインジケータチャネル(PHICH)、物理ダウンリンク制御チャネル(PDCCH)などに関するものであってもよい。データは、物理ダウンリンク共有チャネル(PDSCH)などに関するものであってもよい。プロセッサ420は、データおよび制御情報を処理(たとえば、符号化およびシンボルマッピング)して、それぞれデータシンボルおよび制御シンボルを取得することができる。プロセッサ420はまた、たとえばPSS、SSS、およびセル固有基準信号に関する基準シンボルを生成することもできる。送信(TX)多入力多出力(MIMO)プロセッサ430は、適用可能な場合には、データシンボル、制御シンボル、および/または基準シンボルに対して空間処理(たとえば、プリコーディング)を実行することができ、出力シンボルストリームを変調器(MOD)432a～432tに提供することができる。各変調器432は、(たとえば、OFDMなどのための)それぞれの出力シンボルストリームを処理して、出力サンプルストリームを取得することができる。各変調器432は、出力サンプルストリームをさらに処理(たとえば、アナログに変換、増幅、フィルタリング、およびアップコンバート)して、ダウンリンク信号を取得することができる。変調器432a～432tからのダウンリンク信号を、それぞれアンテナ434a～434tを介して送信してもよい。

【0054】

UE120において、アンテナ452a～452rは、基地局110からダウンリンク信号を受信することができ、受信信号をそれぞれ復調器(DEMOD)454a～454rに提供することができる。各復調器454は、それぞれの受信信号を調整(たとえば、フィルタリング、増幅、ダウンコンバート、およびデジタル化)して、入力サンプルを取得することができる。各復調器

10

20

30

40

50

454は、(たとえば、OFDMなどのための)入力サンプルをさらに処理して、受信シンボルを取得することができる。MIMO検出器456は、すべての復調器454a~454rから受信シンボルを取得し、適用可能な場合、受信シンボルに対してMIMO検出を実行し、検出されたシンボルを提供することができる。受信プロセッサ458は、検出されたシンボルを処理(たとえば、復調、デインターリーブ、および復号)し、UE120のための復号されたデータをデータシンク460に提供し、復号された制御情報をコントローラ/プロセッサ480に提供することができる。

【0055】

アップリンクでは、UE120において、送信プロセッサ464が、データソース462からの(たとえば、物理アップリンク共有チャネル(PUSCH)についての)データ、およびコントローラ/プロセッサ480からの(たとえば、物理アップリンク制御チャネル(PUCCH)についての)制御情報を受信し、処理してもよい。送信プロセッサ464はまた、基準信号のための基準シンボルを生成してもよい。送信プロセッサ464からのシンボルは、適用可能な場合には、TX MIMOプロセッサ466によってプリコーディングされ、(たとえばSC-FDMなどのために)復調器454a~454rによってさらに処理され、基地局110に送信されてもよい。BS110において、UE120からのアップリンク信号は、アンテナ434によって受信され、変調器432によって処理され、適用可能な場合には、MIMO検出器436によって検出され、受信プロセッサ438によってさらに処理されて、UE120によって送られた復号データおよび制御情報を取得してもよい。受信プロセッサ438は、データシンク439に復号されたデータを提供し、コントローラ/プロセッサ440に復号された制御情報を提供してもよい。

【0056】

コントローラ/プロセッサ440および480は、それぞれ基地局110およびUE120における動作を指示してもよい。基地局110におけるプロセッサ440ならびに/または他のプロセッサおよびモジュールは、たとえば、本明細書で説明する技法に対するプロセスを実行または指示してもよい。UE120におけるプロセッサ480ならびに/または他のプロセッサおよびモジュールはまた、たとえば、図10、図12~図13および/または図15に示す機能的ブロックの実施および/または本明細書で説明する技法に対する他のプロセスを実行または指示し得る。メモリ442および482は、それぞれBS110およびUE120のためのデータおよびプログラムコードを記憶してもよい。スケジューラ444は、ダウンリンクおよび/またはアップリンク上でのデータ送信のためにUEをスケジューリングしてもよい。

【0057】

図5は、本開示の態様による、通信プロトコルスタックを実装するための例を示す図500を示す。示された通信プロトコルスタックは、5Gシステム(たとえば、アップリンクベースのモビリティをサポートするシステム)内で動作するデバイスによって実装され得る。図500は、無線リソース制御(RRC)レイヤ510、パケットデータコンバージェンスプロトコル(PDCP)レイヤ515、無線リンク制御(RLC)レイヤ520、媒体アクセス制御(MAC)レイヤ525、および物理(PHY)レイヤ530を含む通信プロトコルスタックを示す。様々な例では、プロトコルスタックのレイヤは、ソフトウェアの個別のモジュール、プロセッサもしくはASICの部分、通信リンクによって接続された非コロケートデバイスの部分、またはそれらの様々な組合せとして実装されてもよい。コロケート実装形態および非コロケート実装形態は、たとえばネットワークアクセスデバイス(たとえば、AN、CU、および/もしくはDU)またはUEのためのプロトコルスタックの中で使用されてもよい。

【0058】

第1のオプション505-aは、プロトコルスタックの実装が集中ネットワークアクセスデバイス(たとえば、図2のANC202)と分散ネットワークアクセスデバイス(たとえば、図2のDU208)との間で分割される、プロトコルスタックの分割実装形態を示す。第1のオプション505-aでは、RRCレイヤ510およびPDCPレイヤ515は、集約ユニットによって実装されてもよく、RLCレイヤ520、MACレイヤ525、およびPHYレイヤ530は、DUによって実装されてもよい。様々な例では、CUおよびDUは、コロケートされてもよく、またはコロケートされなくてもよい。第1のオプション505-aは、マクロセル配置、マイクロセ

10

20

30

40

50

ル配置、またはピコセル配置において有用であってもよい。

【0059】

第2のオプション505-bは、プロトコルスタックが単一のネットワークアクセスデバイス(たとえば、アクセスノード(AN)、ニューラジオ基地局(NB BS)、ニューラジオノードB(NR NB)、ネットワークノード(NN)など)の中で実装される、プロトコルスタックの統合実装形態を示す。第2のオプションでは、RRCレイヤ510、PDCPレイヤ515、RLCレイヤ520、MACレイヤ525、およびPHYレイヤ530は各々、ANによって実装されてもよい。

第2のオプション505-bは、フェムトセル配置において有用であってもよい。

【0060】

ネットワークアクセスデバイスがプロトコルスタックの一部を実装するのか全部を実装するのかにかかわらず、UEは、全プロトコルスタック(たとえば、RRCレイヤ510、PDCPレイヤ515、RLCレイヤ520、MACレイヤ525、およびPHYレイヤ530)を実装してもよい。

【0061】

図6は、ワイヤレスネットワーク100内で通信するために使用され得るDL中心のサブフレームの一例を示す図600である。DL中心のサブフレームは、制御部分602を含んでもよい。制御部分602は、DL中心のサブフレームの最初の部分または開始部分に存在してもよい。制御部分602は、DL中心のサブフレームの様々な部分に対応する様々なスケジューリング情報および/または制御情報を含んでもよい。いくつかの構成では、制御部分602は、図6に示すように、物理DL制御チャネル(PDCCH)であってもよい。DL中心のサブフレームは、DLデータ部分604も含んでもよい。DLデータ部分604は時々、DL中心のサブフレームのペイロードと呼ばれてもよい。DLデータ部分604は、スケジューリングエンティティ(たとえば、UEまたはBS)から従属エンティティ(たとえば、UE)にDLデータを通信するために利用される通信リソースを含んでもよい。いくつかの構成では、DLデータ部分604は、物理DL共有チャネル(PDSCH)であってもよい。

【0062】

DL中心のサブフレームは、共通UL部分606も含んでもよい。共通UL部分606は時々、ULバースト、共通ULバースト、および/または様々な他の適切な用語で呼ばれてもよい。共通UL部分606は、DL中心のサブフレームの様々な他の部分に対応するフィードバック情報を含んでもよい。たとえば、共通UL部分606は、制御部分602に対応するフィードバック情報を含んでもよい。フィードバック情報の非限定的な例は、ACK信号、NACK信号、HARQインジケータ、および/または様々な他の適切なタイプの情報を含んでもよい。共通UL部分606は、ランダムアクセスチャネル(RACH)手順、スケジューリング要求(SR)に関する情報、および様々な他の適切なタイプの情報などの追加のまたは代替の情報を含んでもよい。図6に示すように、DLデータ部分604の終わりは、共通UL部分606の始まりから時間的に分離されてもよい。この時間の分離は時々、ギャップ、ガード期間、ガードインターバル、および/または様々な他の適切な用語で呼ばれてもよい。この分離は、DL通信(たとえば、従属エンティティ(たとえば、UE)による受信動作)からUL通信(たとえば、従属エンティティ(たとえば、UE)による送信)への切替えのための時間を与える。上記はDL中心のサブフレームの一例にすぎず、同様の特徴を有する代替構造が、必ずしも本明細書で説明する態様から逸脱することなく存在し得ることを、当業者は理解されよう。

【0063】

図7は、ワイヤレスネットワーク100内で通信するために使用され得るUL中心のサブフレームの一例を示す図700である。UL中心のサブフレームは、制御部分702を含んでもよい。制御部分702は、UL中心のサブフレームの最初の部分または開始部分に存在してもよい。図7における制御部分702は、図6を参照しながら上記で説明した制御部分と同様であってもよい。UL中心のサブフレームは、ULデータ部分704も含んでもよい。ULデータ部分704は時々、UL中心のサブフレームのペイロードと呼ばれてもよい。UL部分は、従属エンティティ(たとえば、UE)からスケジューリングエンティティ(たとえば、UEまたはBS)にULデータを通信するために利用される通信リソースを指すことがある。いくつかの構

10

20

30

40

50

成では、制御部分702は、物理DL制御チャネル(PDCCH)であってよい。

【0064】

図7に示すように、制御部分702の終わりは、ULデータ部分704の始まりから時間的に分離されてもよい。この時間の分離は時々、ギャップ、ガード期間、ガードインターバル、および/または様々な他の適切な用語で呼ばれてもよい。この分離は、DL通信(たとえば、スケジューリングエンティティによる受信動作)からUL通信(たとえば、スケジューリングエンティティによる送信)への切替えのための時間を与える。UL中心のサブフレームは、共通UL部分706も含んでもよい。図7における共通UL部分706は、図6を参照しながら上記で説明した共通UL部分606と同様であってもよい。共通UL部分706は、追加または代替として、チャネル品質インジケータ(CQI)、サウンディング基準信号(SRS)に関する情報、および様々な他の適切なタイプの情報を含んでもよい。上記はUL中心のサブフレームの一例にすぎず、同様の特徴を有する代替構造が、必ずしも本明細書で説明する態様から逸脱することなく存在し得ることを、当業者は理解されよう。

【0065】

いくつかの状況では、2つ以上の従属エンティティ(たとえば、UE)はサイドリンク信号を使用して互いに通信することができる。そのようなサイドリンク通信の現実世界の適用例は、公共安全、近接サービス、UEからネットワークへの中継、車両間(V2V)通信、インターネットオブエブリシング(IoE:Internet of Everything)通信、IoT通信、ミッションクリティカルメッシュ、および/または様々な他の適切な適用例を含んでもよい。一般に、サイドリンク信号は、スケジューリングおよび/または制御のためにスケジューリングエンティティが利用されてもよいにもかかわらず、スケジューリングエンティティ(たとえば、UEまたはBS)を通じてその通信を中継せずに、ある従属エンティティ(たとえば、UE1)から別の従属エンティティ(たとえば、UE2)に通信される信号を指す場合がある。いくつかの例では、サイドリンク信号は、(通常は無認可スペクトルを使用するワイヤレスローカルエリアネットワークとは異なり)認可スペクトルを使用して通信されてもよい。

【0066】

UEは、リソースの専用セットを使用してパイロットを送信することに関連する構成(たとえば、無線リソース制御(RRC)専用状態など)、またはリソースの共通セットを使用してパイロットを送信することに関連する構成(たとえば、RRC共通状態など)を含む、様々な無線リソース構成において動作してもよい。RRC専用状態において動作するとき、UEは、パイロット信号をネットワークに送信するために、リソースの専用セットを選択してもよい。RRC共通状態において動作するとき、UEは、パイロット信号をネットワークに送信するために、リソースの共通セットを選択してもよい。いずれの場合も、UEによって送信されるパイロット信号は、ANもしくはDU、またはそれらの部分などの1つまたは複数のネットワークアクセスデバイスによって受信されてもよい。各受信ネットワークアクセスデバイスは、リソースの共通セット上で送信されるパイロット信号を受信および測定するとともに、ネットワークアクセスデバイスがUEのためのネットワークアクセスデバイスの監視セットのメンバーであるUEに割り振られたリソースの専用セット上で送信されるパイロット信号も受信および測定するように構成されてもよい。受信ネットワークアクセスデバイスのうちの1つもしくは複数、または受信ネットワークアクセスデバイスがパイロット信号の測定値を送信する先のCUは、UE用のサービングセルを識別するために、またはUEのうちの1つもしくは複数のためのサービングセルの変更を開始するために、測定値を使用してもよい。

【0067】

ネットワークポリシーの鍵生成への例示的な組み込み

上述のように、拡張モバイルブロードバンド(eMBB:enhanced mobile broadband)ターゲットの広い帯域幅(たとえば、80MHzを越える)、ミリ波(mmW:millimeter wave)ターゲットの高いキャリア周波数(たとえば、60GHz)、マッシブMTC(mMTC:massive MTC)ターゲットの後方互換性のないMTC技法、およびミッションクリティカルターゲットの超高信頼低レイテンシ通信(URLLC:ultra reliable low latency communication)を含

10

20

30

40

50

む特徴を含む、新しいエアインターフェースが、5Gのために導入されている。

【0068】

5Gのためのサービスおよび技術が継続的に発達するに連れて、5Gは、様々な異なる配置シナリオをサポート可能になり得る。たとえば、現在の5Gアーキテクチャでは、ネットワーク内で種々の機能を実行する役目を果たす1つまたは複数のネットワークノード(たとえば、セキュリティアンカー機能(SEAF)、アクセスおよびモビリティ管理機能(AMF)、セッション管理機能(SMF)など)が、コロケートされ得るかまたは物理的に分離され得る。

【0069】

SEAFは、AMFをネットワークエッジ(たとえば、RAN)の近くに移動および/または配置する必要がある場合でも、セキュリティアンカーを物理的にセキュアなロケーション内に保持するために、5Gにおいて導入された。したがって、いくつかの配置では、SEAFはAMFとコロケートされてもよく、他の配置では、SEAFはAMFから分離されてもよい(たとえば、SEAFおよびAMFはそれぞれ、独立型機能を有し得る)。同様に、SMFは、AMFおよびSEAFから分離され得る。場合によっては、SMFは、AMFから物理的に分離されてもよく、(たとえば、ネットワーク共有シナリオの場合には)AMFとは異なるセキュリティ領域内にあってもよい。場合によっては、SMFはスライス固有であってもよい。

【0070】

図8は、本開示のいくつかの態様による、1つまたは複数のネットワークノードが物理的に分離され得る5Gアーキテクチャ800の参照例を示す。特に、アーキテクチャ800は、(たとえば、他の配置シナリオにおけるコロケートされたSEAF/AMFとは対照的に)SEAFがAMFから物理的に分離される配置シナリオの参照例を示す。

【0071】

示すように、5Gアーキテクチャ800は、マルチスライスを含み得る。各スライスは、種々のサービス、たとえば、インターネットオブエブリシング(IoE)、URLLC、eMBB、車両通信(すなわち、車両間(V2V)、車両インフラストラクチャ間(V2I)、車両歩行者間(V2P)、車両ネットワーク間(V2N)などのV2X)などをサポートし得る。

【0072】

スライスは、5G-ANと5G-CNの両方を含み得るいくつかのネットワーク能力およびネットワーク特性を提供するために必要なネットワーク機能および対応するリソースのセットを含む完全な論理ネットワークとして定義され得る。より具体的には、スライスは、的確に構成されたネットワーク機能、ネットワーク適用例、および特定の使用事例またはビジネスモデルの要件を満足するためにともにバンドリングされる下位のクラウドインフラストラクチャの組成であり得る。場合によっては、異なるスライスが、別々のリソースを割り当てられてもよく、レイテンシおよび/または電力など、異なる要件を有してもよい。

【0073】

この例では、AMFは、複数のスライスを同時にサービスするように構成され得る。たとえば、AMFは、UEとネットワークスライスとの間にモビリティ管理NASセキュリティアンカーを提供し得る。SMFは、一般に、サービス(スライス)固有のPDUセッション確立をサポートするためにサービス認可/認証を実行するように構成される。SMFは、ユーザプレーン機能(UPF)とRANとの間で維持されるトンネルを含む、修正およびリリースなどの機能も実行し得る。ユーザプレーンセキュリティは、UDFにおいて終了することができる。場合によっては、SMFは、サービス固有のQoSをサポート可能であり得る。

【0074】

図9は、本開示のいくつかの態様による、1つまたは複数のネットワークノード(たとえば、SEAF、AMF、SMFなど)が物理的に分離され得る5Gアーキテクチャ900の別の参照例を示す。場合によっては、5Gセキュリティアーキテクチャは、PDUセッション認可のためにサードパーティ認証サーバ機能(AUSF)(たとえば、サードパーティAAA)による二次認証をネイティブにサポートするように設計され得る。サービス認証は、サービス固有のPDUセッションの確立を可能にする。図8と同様に、ユーザプレーンセキュリティはUPFにおいて終了することができ、サービス固有のQoSがサポートされ得る。SMFは、サードパー

10

20

30

40

50

ティAAAに直接インターフェース可能であり得るか、またはSEAFを介してサードパーティAAAと相互作用可能であり得る。

【 0 0 7 5 】

上述のように、5Gネットワークは継続的に発達し得るので、特定のネットワーク構成、能力、セキュリティ情報などに関する情報(本明細書でネットワークポリシー情報と総称される)をUEに提供することが望ましい。しかしながら、現在のアーキテクチャでは、UEとサービングネットワークとの間の唯一の制御プレーンインターフェースがN1であり、N1はUEとAMFとの間のNAS接続のために使用されるので、現在の技法を使用して、セキュアな方法でネットワークポリシー情報をUEに提供することは不可能である。

【 0 0 7 6 】

たとえば、アーキテクチャ800を参照すると、AMFは、(たとえば、NASシグナリングに基づいて)UEとのシグナリング接続を有する唯一のエンティティであり得るので、AMFは、別のネットワークノード(たとえば、SEAF、SMFなど)から受信された任意のネットワークセキュリティポリシー情報に関して、UEに偽って知らせることが可能であり得る。したがって、AMFおよびSEAFが分離されている情報をネットワークポリシー情報が含む場合、UEは、(たとえば、SEAFとのシグナリング接続も有するのとは対照的に)AMFとのシグナリング接続のみを有し得るので、現在の技法は、AMFとSEAFとが分離されていることをUEにセキュアに知らせることができない場合がある。

【 0 0 7 7 】

そのような場合、独立型(不正な)AMFは、それがSEAFとコロケートされていると主張することが可能であり得、そのようなシナリオは、UEによって検出され得ない。そのような独立型(不正な)AMFは、UEとネットワークとの間の接続/セッションに不正アクセスするために、ネットワークセキュリティ能力、セッション管理NAS保護、スライス固有のセキュリティ能力/要件などを修正可能であり得る。

【 0 0 7 8 】

さらに、正確な(セキュアな)ネットワークポリシー情報がないと、UEは、(たとえば、PDUセッション確立に対して)ビディングダウンアタックを被ることがある。ビディングダウンシナリオの一例では、AMFは、SMFとは異なるセキュリティ領域内にあり得る。たとえば、ある場合には、AMFが、(たとえば、あまりセキュアでないロケーションにあり得る)サービングネットワーク内でUE(またはRAN)の近くに配置される一方で、SMFが、ネットワークの奥の方に配置される場合がある。ある場合には、AMFがサービングネットワーク(たとえば、VPLMN)内にある場合がある一方で、SMFがホームネットワーク内にある。

【 0 0 7 9 】

しかしながら、AMFはSMFとは異なるセキュリティ領域内にある場合がある一方で、SMFは、依然として、(たとえば、AMFによってアクセスされ得ないスライス固有の加入情報に基づいて)スライス固有のPDUセッション生成を認可する役目を果たす場合がある。たとえば、SMFは、一般的に、AMFから論理的に分離したネットワーク機能であり、PDUセッション認可および管理に対する役目を果たす。上述のように、SMFはスライス固有であり、したがって、スライス固有のPDUセッションパラメータをUEと交換し得る。

【 0 0 8 0 】

しかしながら、UEによって要求されSMFによって構成された、認可されたQoSルール、SSCモード、S-NSSAI、割り振られたIPv4アドレスなどのPDUセッションパラメータは、UEとSMFとの間の(たとえば、AMFを含む)中間ノードによって修正されるべきではない。そうではなく、そのようなパラメータは、SMFが、SEAFから取得される特定の鍵を使用し、同じSMF鍵を導出することによってUEにおいて検証可能であることによって保護されるべきである。したがって、AMFがSEAFから分離される状況では、(悪意のあるまたは不正アクセスされた)AMFは、たとえばセキュリティ、QoS、または他のパケット処理を格下げするために、UEによって要求されるか、またはSMFによって認可されるセッション情報を修正し得る。

10

20

30

40

50

【 0 0 8 1 】

それに応じて、本明細書で提示する態様は、たとえばビディングダウンアタックを最小化するために、ネットワークポリシー情報をUEにセキュアに知らせるための技法を提供する。特に、態様は、ネットワークポリシー情報を、UEとAMFとの間のNAS接続をセキュアにするために使用される鍵(たとえば、 K_{AMF})導出内に組み込むための技法を提供する。以下で説明するように、ネットワークポリシー情報を鍵導出内に組み込むことによって、UEは、AMFから何らかの受信されたネットワークポリシー情報が変更/修正/不正アクセスされたかどうかを検出可能であり得る。

【 0 0 8 2 】

本明細書で説明する技法は、PDUセッション確立のビディングダウンアタックに対して保護するために使用することができるが、本明細書で提示する態様は、SEAFとUEとの間のノードによるUEポリシービディングダウンに対して保護するためにも使用され得ることに留意されたい。すなわち、以下で説明するように、本明細書で提示する態様は、たとえば、UEポリシー情報を鍵(たとえば、 K_{AMF})導出内に組み込むことによって、UEポリシー情報(たとえば、ネットワーク能力、セキュリティ能力、またはそれらの任意の組合せを含む、UEセキュリティ特徴および/またはUE能力)を保護するためにも使用され得る。UEポリシー情報は、登録/添付要求メッセージ内でネットワークに提供され得る。

【 0 0 8 3 】

いくつかの態様によれば、 K_{AMF} 導出は、ネットワーク内で交換されるパラメータを保護するために使用され得る。特に、UEがネットワークに登録するとき、SEAFは、ネットワークポリシー情報および/またはUEポリシー情報を鍵(たとえば、 K_{AMF})導出内に組み込むことによって、ネットワーク(セキュリティ)ポリシー情報(たとえば、ネットワーク構成、能力、セキュリティ特徴など)および/または(たとえば、UEによって受信された)UEポリシー情報をUEに知らせ得る。

【 0 0 8 4 】

たとえば、SEAFはネットワークポリシー情報、UEポリシー情報、鮮度パラメータ(freshness parameter)、またはそれらの任意の組合せに基づいてAMF鍵(たとえば、 K_{AMF})を導出し、AMFおよびUEがNASセキュリティ状況を確認することができ、SEAFもUEから受信されたUEポリシー情報をUEに知らせ得るように、鍵をAMFに送り得る。AMFおよびUEは、暗号化および完全性保護鍵を K_{AMF} から導出し、(たとえば、N1インターフェース上の)NASメッセージを保護し得る。

【 0 0 8 5 】

ネットワークポリシー情報を K_{AMF} 導出内に組み込むことによって、ネットワークポリシー情報における変化はUEにおいて異なる K_{AMF} 導出をもたらすので、AMFは、SEAFから受信されたネットワークポリシー情報を修正することによってネットワーク特徴をビディングダウンすることなどの無認可の行動を実行することが防止され得る。同様に、UEポリシー情報を K_{AMF} 導出内に組み込むことによって、UE能力における変化も異なる K_{AMF} 導出をもたらすことになるので、UEとSEAFとの間のネットワークノードは、UE能力を修正することによってUE能力をビディングダウンすることを防止され得る。

【 0 0 8 6 】

図10は、ワイヤレス通信のための例示的な動作1000を示す。いくつかの態様によれば、動作1000は、たとえば、ネットワークとのセキュアな(たとえば、NAS)接続を確立するためにユーザ機器によって実行され得る。

【 0 0 8 7 】

動作1000は、UEが、ネットワークとのセキュアな接続を確立するために第1のメッセージ(たとえば、セキュリティモードコマンド(SMC:security mode command)メッセージ)を(たとえば、AMFから)受信する、1002において開始し得る。第1のメッセージは、ネットワークポリシー情報(たとえば、ネットワーク構成、能力、セキュリティ特徴など)を含む。1004において、UEは、ネットワークポリシー情報に部分的に基づいて第1の鍵(たとえば、 K_{AMF})を生成する。

10

20

30

40

50

【0088】

いくつかの態様では、ネットワークポリシー情報は、ネットワークとの通信セッションを確立するときに、UEがセッション管理トークンをネットワーク内のSMFから受信することになるかどうかの指示を含む。いくつかの態様では、ネットワークポリシー情報は、AMFがネットワーク内でSEAFとコロケートされるかどうかの指示を含む。いくつかの態様では、ネットワークポリシー情報は、AMFのセキュリティレベルを含む。いくつかの態様では、ネットワークポリシー情報は、SEAFのセキュリティ領域、AMFのセキュリティ領域、またはそれらの任意の組合せを含む。いくつかの態様では、ネットワークポリシー情報は、UEからネットワークに送られたUEポリシー情報にตอบสนองして形成されている場合がある。いくつかの態様では、第1の鍵は、ネットワークに送られたUEポリシー情報に基づいて決定され得る。

10

【0089】

1006において、UEは、第1の鍵を使用して、ネットワークポリシー情報が有効であることを検証する。たとえば、場合によっては、UEは、第1の鍵に部分的に基づいて、(ネットワークポリシー情報を含む)第1のメッセージが有効であるかどうかを決定し得る。

【0090】

以下でより詳細に説明するように、場合によっては、第1のメッセージは、第2の鍵(たとえば、SEAFからAMFに提供された K_{AMF})に基づいて導出された保護鍵を用いて完全性保護されるSMCメッセージであり得る。UEは、第1の鍵に基づいて第1のメッセージの完全性検証を実行することによって、第1のメッセージ(および/またはそのメッセージに含まれるネットワークポリシー情報)が有効であるかどうかを決定し得る。一態様では、UEは、第1のメッセージの完全性検証が正しい場合に、第1のメッセージは有効であると決定し得る。

20

【0091】

UEは、第1の鍵が第2の鍵と同じであるとUEが決定する場合に、第1のメッセージの完全性検証は正しいと決定し得る。UEは、第1の鍵が第2の鍵と同じであるとの決定に基づいて、ネットワークポリシー情報は有効であると決定し得る。同様に、UEは、第1のメッセージの完全性検証が正しくない場合に、第1のメッセージは無効であると決定し得る。UEは、第1の鍵が第2の鍵とは異なる場合に、第1のメッセージの完全性検証は正しくないと決定し得る。UEは、第1の鍵が第2の鍵とは異なるとの決定に基づいて、ネットワークポリシー情報は無効であると決定し得る。

30

【0092】

図11は、ワイヤレス通信のための例示的な動作1100を示す。いくつかの態様によれば、動作1100は、たとえば、ネットワークポリシー情報をUEにセキュアに提供するために、ネットワークノード(たとえば、SEAF)によって実行され得る。

【0093】

動作1100は、ネットワークノードが、ネットワークポリシー情報に少なくとも部分的に基づいて別のネットワークノード(たとえば、AMF)に対する鍵(たとえば、 K_{AMF})を生成する、1102において開始し得る。上述のように、ネットワークポリシー情報は、他のネットワークノード(たとえば、AMF)がネットワークノードとコロケートされるかどうかの指示を含み得る。場合によっては、ネットワークポリシー情報は、ネットワークノードのセキュリティレベル、またはネットワーク内のSMFが、UEとネットワークとの間の通信セッションのためのSMトークンを生成し、そのSMトークンをUEに送ることになっているかどうかの指示のうちの少なくとも1つを含み得る。鍵は、UEとネットワークノードとの間にセキュアな接続を確立するために使用される。

40

【0094】

いくつかの態様では、ネットワークノードは、UEポリシー(または能力)情報を含む登録メッセージ/添付要求メッセージを受信し得る。ネットワークノードは、受信されたUEポリシー情報を他のネットワークノードに対する鍵(たとえば、 K_{AMF})導出内に組み込み得る。たとえば、図11の1102において、ネットワークノードは、ネットワークポリシー情報

50

、鮮度パラメータ、UEポリシー情報、またはそれらの任意の組合せに部分的に基づいて、他のネットワークノード(たとえば、AMF)に対する鍵(たとえば、 K_{AMF})を生成し得る。

【0095】

1104において、ネットワークノードは、鍵を他のネットワークノードに送る。いくつかの態様では、ネットワークノードは、ネットワークポリシー情報またはネットワークポリシー情報が有効である時間量のうちの少なくとも1つをネットワークノードにさらに送り得る。

【0096】

図12は、本開示のいくつかの態様による、ネットワーク(セキュリティ)ポリシー情報および/またはUEポリシー情報を(たとえば、ポリシー情報および/またはUEポリシー情報を鍵導出内に組み込むことによって)SEAFがUEにセキュアに知らせることを可能にする例示的登録手順を示すコールフロー図である。

【0097】

いくつかの態様では、示すように、UEは、最初に、登録要求/添付要求をネットワーク(たとえば、AMF、SEAFなど)に送り得る。登録要求/添付要求は、UEポリシー(能力)を含む。次いで、ステップ1において、UEは、ネットワークとの認証/登録手順を実行する。UEおよびSEAFは、新しい認証に基づいてまたは前の認証に基づいて共有アンカー鍵(K_{SEAF})を確立し得る。登録の間に、AMFは、SEAFからの鍵(K_{AMF})を要求し得る。

【0098】

ステップ2において、SEAFは、AMFのために、UEをネットワークに登録するための K_{AMF} を生成する(たとえば、導出する)。 K_{AMF} 導出は、ネットワークポリシー情報(たとえば、ネットワーク構成、能力、セキュリティ特徴など)および/またはUEポリシー情報を組み込む。一態様では、ネットワークポリシー情報は、AMFタイプ、たとえばコロケートされたAMF/SEAF、独立型AMFなどを含み得る。

【0099】

たとえば、ネットワークポリシー情報は、1つまたは複数のSEAF/AMF分離ビットを含み得る。 K_{AMF} を要求するAMFがSEAFから分離された独立型AMFである場合、SEAFは、SEAF/AMF分離ビットを第1の値(たとえば、1)に設定し得る。 K_{AMF} を要求するAMFがコロケートされたAMF/SEAFである場合、SEAFは、SEAF/AMF分離ビットを異なる第2の値(たとえば、0)に設定し得る。一態様では、 K_{AMF} 導出は、再生アタックを防止するために使用される1つまたは複数の鮮度パラメータも組み込み得る。そのような鮮度パラメータの例は、(UEとSEAFの両方において維持される)カウンタ、UEとSEAFとの間で交換されるランダムな値、またはそれらの任意の組合せを含み得る。一態様では、SEAFは、 K_{AMF} を生成(導出)するために下式(1)を使用し得る。

$K_{AMF} = KDF(K_{SEAF}, \text{鮮度パラメータ}, \text{ネットワークポリシー情報}, \text{UEポリシー})$ (1)

ここで、KDFは鍵導出関数(たとえば、HMAC-SHA-1、HMAC-SHA-256、HMAC-SHA-512、PRF-X(その出力サイズがXである疑似ランダム関数))であり、 K_{SEAF} はサービングネットワーク内のアンカー保護鍵であり(かつSEAFにおいて保持され)、鮮度パラメータはカウンタ、再生アタックを防止するために使用されるランダムな値であり、ネットワークポリシー情報はネットワーク構成、能力、セキュリティ特徴など含み、UEポリシーはUE能力情報および/またはUEセキュリティ情報のうちの少なくとも1つを含む。

【0100】

ステップ3において、SEAFは、 K_{AMF} 、鮮度パラメータ、およびネットワークポリシー情報をAMFに提供する。いくつかの態様では、SEAFはまた、ステップ3においてUEポリシーをAMFに提供(たとえば、再送)し得る。ステップ4において、AMFは、NASセキュリティモードコマンド(SMC)をUEに送る。いくつかの態様では、AMFはまた、ステップ4においてUEポリシーをUEに提供(たとえば、再送)し得る。NAS SMCは、SEAFから取得された鮮度パラメータおよびネットワークポリシー情報を含み、NAS SMCは、 K_{AMF} に基づいて完全性保護され得る。たとえば、SEAFから K_{AMF} を受信すると、AMFは、 K_{AMF} に基づいてNAS完全性保護鍵(たとえば、 K_{NASINT})を導出し、 K_{NASINT} を使用してNAS SM

10

20

30

40

50

Cメッセージを完全性保護し得る。

【0101】

ステップ5において、UEは、 K_{SEAF} およびNAS SMCメッセージ内の情報(たとえば、鮮度パラメータ、ネットワークポリシー情報など)を使用して K_{AMF} を生成(たとえば、導出)し、NAS SMCメッセージを検証する。すなわち、ネットワークポリシー情報内の何らかの変化は、UEにおいて異なる K_{AMF} 導出を引き起こすことになるので、UEは、ネットワークポリシー情報に対して(たとえば、AMFによる)何らかの変化が存在しているかどうかを検出することができる。UEによって生成された K_{AMF} と K_{AMF} を使用するNAS SMCの完全性保護とを比較することによって、使用するNAS SMCの完全性保護をUEが検査するとき、UEは、そのような変化を検出することができる。したがって、SMCの完全性検証は正しいとの決定は、UEによって生成された K_{AMF} と(SEAFから)AMFに提供された K_{AMF} とは同じであることを暗示し、そのことは、次いで、(AMFから)UEに提供されたネットワークポリシー情報は有効であることを暗示する。

10

【0102】

SMCの検証は正しいと仮定すると、(ステップ6において)UEは、NASセキュリティモード完了メッセージをAMFに送る。いくつかの態様では、UEは、(ネットワークに提供された)UEポリシー情報が、中間ネットワークノードのいずれかによって修正されたかどうかを検出することができる。すなわち、いくつかの態様では、UEは、(たとえば、UEによって生成された K_{AMF} と(SEAFから)AMFに提供された K_{AMF} とが同じかどうかに基づいて)UEポリシー情報が修正されたかどうかを決定するために、(たとえば、ネットワークポリシー情報に加えてまたはその代替として)UEポリシー情報に基づいて K_{AMF} を生成し得る。

20

【0103】

図12のコールフローは、ネットワークポリシー情報をUEにセキュアに知らせるためにネットワークポリシー情報を鍵導出内に組み込むことを説明しているが、本明細書で提示する技法は、UEセキュリティ特徴を保護するためにも使用することができることに留意されたい。すなわち、ネットワークポリシー情報に加えてまたはその代替として、鍵(K_{AMF})導出は、(UEセキュリティ特徴を含む)UE能力を組み込んでよく、ここでUE能力は、登録/添付要求メッセージ内でネットワークに提供される。

【0104】

図10～図12で説明する技法は、鍵導出における鍵使用を制限することによって、AMFがUEに任意の中継するネットワーク能力パラメータをAMFが修正することを防止するために使用され得る。しかしながら、これらの技法はネットワーク能力のビディングダウンを防止するために有用であり得る一方で、そのような技法は、PDUセッションパラメータビディングダウン(たとえば、SM NASトークン)を防止するためには十分でない場合がある。

30

【0105】

それに応じて、本明細書で提示する態様は、(たとえば、PDUセッション確立および/またはネットワーク能力パラメータに対する)ビディングダウンアタックを防止するために使用され得る技法を提供する。

【0106】

より具体的には、UEがネットワークに登録するとき、SEAFは、 K_{AMF} とともにネットワークポリシー情報(たとえば、ネットワーク構成、(セキュリティ)能力など)および完全性保護されたネットワークポリシー情報(たとえば、ネットワークポリシートークン)をAMFに提供する。ネットワークポリシー情報は、 K_{SEAF} を使用して完全性保護される。ネットワークポリシートークンは、NASセキュリティモードコマンド上にピギーバックされて、UEに提供される。ネットワークポリシートークンは、SEAFとUEとの間に存在する任意のネットワーク機能がネットワーク能力を修正することを防止する。

40

【0107】

図13は、ワイヤレス通信のための例示的な動作1300を示す。いくつかの態様によれば、動作1300は、たとえば、ネットワークとのセキュアな(たとえば、NAS)接続を確立するためにユーザ機器によって実行され得る。

50

【 0 1 0 8 】

動作1300は、UEが、ネットワークとの認証手順に基づいて、ネットワーク内でUEとSEAFとの間で共有されるアンカー鍵(たとえば、 K_{SEAF})を確立することで、1302において開始し得る。1304において、UEは、ネットワークとのセキュアな接続を確立するために第1のメッセージ(たとえば、SMCメッセージ)を受信する。第1のメッセージは、ネットワークとの通信セッションのためのネットワークポリシートークン、ネットワークポリシー情報、ネットワークポリシー情報が有効である第1の時間量、およびセキュアな接続のために使用される第1の鍵が有効である第2の時間量を含む。ネットワークポリシートークンは、ネットワークポリシー情報と関連付けられた完全性保護情報を含む。

【 0 1 0 9 】

1306において、UEは、ネットワークとのセキュアな接続を確立する前に、共有アンカー鍵から導出された鍵、ネットワークポリシー情報、第1の時間量、および第2の時間量に基づいて、ネットワークポリシートークンが有効であるかどうかを決定する。いくつかの態様では、ネットワークポリシートークンが有効であるかどうかを決定することは、共有アンカー鍵から導出された鍵に基づいて完全性保護情報を検証することを含む。いくつかの態様では、UEは、UEポリシー情報(たとえば、UE能力情報、UEセキュリティ情報など)をネットワークに送り得る。UEは、ネットワークに送られたUEポリシー情報に基づいて鍵を生成し得る。場合によっては、ネットワークポリシー情報は、UEポリシー情報に基づく場合がある。

【 0 1 1 0 】

図14は、ワイヤレス通信のための例示的な動作1400を示す。いくつかの態様によれば、動作1400は、たとえば、ネットワークポリシー情報をUEにセキュアに提供するために、ネットワークノード(たとえば、SEAF)によって実行され得る。

【 0 1 1 1 】

動作1400は、ネットワークノードが、UEとの認証手順に基づいて、ネットワーク内でネットワークノードとUEとの間で共有されるアンカー鍵(たとえば、 K_{SEAF})を確立することで、1402において開始し得る。1404において、ネットワークノードは、アンカー鍵、ネットワークポリシー情報、およびネットワークポリシートークンが有効である第1の時間量に部分的に基づいてネットワークポリシートークン(たとえば、 K_{token})を生成する。ネットワークポリシートークンは、ネットワークポリシー情報と関連付けられた完全性保護情報を含む。1406において、ネットワークノードは、別のネットワークノード(たとえば、AMF)に対する鍵(たとえば、 K_{AMF})を生成する。1408において、ネットワークノードは、鍵、ネットワークポリシー情報およびネットワークポリシートークンを他のネットワークノードに送る。

【 0 1 1 2 】

いくつかの態様では、上記で説明したように、ネットワークノードは、たとえば、中間ノードがUEから受信されたUEポリシー情報を修正することを防止するために、UEポリシー情報を鍵(たとえば、 K_{AMF})導出内に組み込んでもよい。上述のように、ネットワークノードは、UEポリシー情報を登録/添付要求メッセージを介して受信し得る。

【 0 1 1 3 】

図15は、本開示のいくつかの態様による、SEAFがPDUセッション確立に対するビディングダウンアタックを防止することを可能にする、例示的な登録手順を示すコールフロー図である。

【 0 1 1 4 】

示すように、ステップ1において、UEは、ネットワークとの登録手順を実行する。UEおよびSEAFは、新しい認証に基づいてまたは前の認証に基づいて共有アンカー鍵(K_{SEAF})を確立し得る。登録の間に、AMFは、SEAFからの鍵(K_{AMF})を要求し得る。図示されていないが、場合によっては、UEは、UEポリシー情報(たとえば、UE能力情報、UEセキュリティ情報など)をネットワークに、登録/添付要求メッセージを介して提供し得る。

【 0 1 1 5 】

ステップ2において、SEAFは、AMFのために、UEをネットワークに登録するための K_{AMF} を生成する。SEAFは、 K_{SEAF} および1つまたは複数の第1の鮮度パラメータを使用して K_{AMF} を生成し得る。加えて、SEAFは、 K_{SEAF} 、(たとえば、再生アタックを防止するための)1つまたは複数の第2の鮮度パラメータ、およびネットワークポリシー情報を使用してネットワークポリシートークンを生成する。上述のように、ネットワークポリシートークンは、ネットワークポリシー情報のメッセージ認証コード(または完全性保護情報)である。図12と同様に、ネットワークポリシー情報は、1つまたは複数のSEAF/AMF分離ビットを含み得る。いくつかの態様では、SEAFは、UEポリシー情報にさらに基づいて K_{AMF} を生成し得る。

【0116】

10

ステップ3において、SEAFは、 K_{AMF} 、第1および第2の鮮度パラメータ、ネットワークポリシートークン、およびネットワークポリシー情報をAMFに提供する。ステップ4において、AMFは、NASセキュリティモードコマンドをUEに送る。NASセキュリティモードコマンドは、SEAFから取得されたネットワークポリシー情報、第1および第2の鮮度パラメータ、およびネットワークポリシートークンを含む。

【0117】

ステップ5において、UEは、 K_{SEAF} を使用してネットワークポリシートークンに対する検証手順を実行する。検証に成功した場合、UEは、 K_{SEAF} を使用して K_{AMF} を導出し、導出された K_{AMF} を使用してNASセキュリティモードコマンドに対する検証手順を実行する。NASセキュリティモードコマンドが検証されると仮定すると、(ステップ6において)UEは、NASセキュリティモード完了メッセージをAMFに送る。このようにして、(トークンはUEとSEAFとの間の鍵に基づいて生成され、検証されるので)、SEAFは、ネットワーク能力をセキュアな方法でUEに直接示すことができる。

20

【0118】

いくつかの態様では、(図15に対する)SEAFは、再生アタックを防止するためにネットワークポリシーを生成するために、(図12のSEAFと比較して)UEの追加の状態(たとえば、鮮度パラメータ)を維持しなければならない場合があることに留意されたい。これは、デシンクを起こしやすい接続であり得る、UEとSEAFとの間の接続状態を維持することと同様であり得る。さらに、図13～図15で説明した技法と同様の技法は、(UEセキュリティ情報および/またはUE能力情報を含む)UEポリシー情報に対するビディングダウンアタックを防止するためにも使用され得ることに留意されたい。

30

【0119】

本明細書で開示する方法は、説明した方法を実現するための1つまたは複数のステップまたはアクションを含む。方法ステップおよび/またはアクションは、特許請求の範囲の範囲から逸脱することなく互いに入れ替えられてもよい。言い換えれば、ステップまたはアクションの特定の順序が指定されない限り、特定のステップおよび/またはアクションの順序および/または使用は、特許請求の範囲の範囲から逸脱することなく修正されてもよい。

【0120】

本明細書で使用する場合、項目の列挙「のうちの少なくとも1つ」を指す句は、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-b、a-c、b-c、およびa-b-c、ならびに複数の同じ要素を有する任意の組合せ(たとえば、a-a、a-a-a、a-a-b、a-a-c、a-b-b、a-c-c、b-b、b-b-b、b-b-c、c-c、およびc-c-c、または任意の他の順序のa、b、およびc)を包含するものとする。

40

【0121】

本明細書で使用する「決定すること」という用語は、幅広い様々なアクションを包含する。たとえば、「決定すること」は、算出すること、計算すること、処理すること、導出すること、調査すること、ルックアップすること(たとえば、テーブル、データベースまたは別のデータ構造においてルックアップすること)、確認することなどを含んでもよい。また、「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

50

こと(たとえば、メモリ内のデータにアクセスすること)などを含んでもよい。また、「決定すること」は、解決すること、選択すること、選出すること、確立することなどを含んでもよい。

【0122】

場合によっては、デバイスは、フレームを実際に送信するのではなく、送信のためのフレームを出力するインターフェースを有し得る。たとえば、プロセッサは、送信のためにバスインターフェースを介してRFフロントエンドにフレームを出力し得る。同様に、デバイスは、フレームを実際に受信するのではなく、別のデバイスから受信したフレームを取得するためのインターフェースを有し得る。たとえば、プロセッサは、送信のためにRFフロントエンドからバスインターフェースを介してフレームを取得(または受信)し得る。

10

【0123】

上記で説明した方法の様々な動作は、対応する機能を実行することが可能な任意の適切な手段によって実行されてもよい。手段は、限定はしないが、回路、特定用途向け集積回路(ASIC)、またはプロセッサを含む、様々なハードウェアおよび/またはソフトウェア構成要素および/またはモジュールを含んでもよい。一般に、図に示す動作がある場合、それらの動作は、同様の番号を付された対応する同等のミーンズプラスファンクション構成要素を有してもよい。

【0124】

たとえば、送信するための手段、受信するための手段、決定するための手段、実行するための手段、関与するための手段、示すための手段、確立するための手段、検証するための手段、送るための手段、通信するための手段、記憶するための手段、入力するための手段、保護するための手段、防止するための手段、終了するための手段、生成するための手段、転送するための手段、および/または提供するための手段は、BS110における送信プロセッサ420、コントローラ/プロセッサ440、受信プロセッサ438、またはアンテナ434、ならびに/あるいはUE120における送信プロセッサ464、コントローラ/プロセッサ480、受信プロセッサ458、またはアンテナ452など、BS110またはUE120における1つまたは複数のプロセッサまたはアンテナを備え得る。

20

【0125】

本開示に関連して説明する様々な例示的な論理ブロック、モジュール、および回路は、汎用プロセッサ、デジタル信号プロセッサ(DSP)、特定用途向け集積回路(ASIC)、フィールドプログラマブルゲートアレイ(FPGA)もしくは他のプログラマブル論理デバイス(PLD)、ディスクリートゲートもしくはトランジスタ論理、ディスクリートハードウェア構成要素、または本明細書で説明する機能を実行するように設計されたそれらの任意の組合せを用いて実装または実行されてもよい。汎用プロセッサは、マイクロプロセッサであってもよいが、代替として、プロセッサは、任意の市販のプロセッサ、コントローラ、マイクロコントローラ、または状態機械であってもよい。プロセッサはまた、コンピューティングデバイスの組合せ、たとえばDSPとマイクロプロセッサとの組合せ、複数のマイクロプロセッサ、DSPコアと連携した1つもしくは複数のマイクロプロセッサ、または任意の他のそのような構成として実装されてもよい。

30

【0126】

ハードウェアにおいて実装される場合、例示的なハードウェア構成は、ワイヤレスノード内の処理システムを含んでもよい。処理システムは、バスアーキテクチャを用いて実装されてもよい。バスは、処理システムの特定の適用例および全体的な設計制約に応じて、任意の数の相互接続バスおよびブリッジを含んでもよい。バスは、プロセッサ、機械可読媒体、およびバスインターフェースを含む様々な回路を互いにリンクさせてもよい。バスインターフェースは、バスを介して、とりわけ処理システムにネットワークアダプタを接続するために使用されてもよい。ネットワークアダプタは、PHYレイヤの信号処理機能を実装するために使用されてもよい。ユーザ端末120(図1参照)の場合、ユーザインターフェース(たとえば、キーパッド、ディスプレイ、マウス、ジョイスティックなど)がバスに接続されてもよい。バスは、タイミングソース、周辺装置、電圧調整器、電力管理回路など

40

50

の様々な他の回路をリンクさせる場合があるが、これらの回路は当技術分野でもよく知られており、したがってこれ以上は説明しない。プロセッサは、1つまたは複数の汎用プロセッサおよび/または専用プロセッサを用いて実装されてもよい。例には、マイクロプロセッサ、マイクロコントローラ、DSPプロセッサ、およびソフトウェアを実行できる他の回路が含まれる。当業者は、特定の適用例とシステム全体に課せられた全体的な設計制約とに応じて処理システムに関する上述の機能を最も適切に実装するにはどうすべきかを認識するであろう。

【0127】

ソフトウェアにおいて実装される場合、機能は、1つまたは複数の命令またはコードとしてコンピュータ可読媒体上に記憶されるか、またはコンピュータ可読媒体を介して送信されてもよい。ソフトウェアは、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どうかにかかわらず、命令、データ、またはそれらの任意の組合せを意味するように広く解釈されるべきである。コンピュータ可読媒体は、コンピュータ記憶媒体と、ある場所から別の場所へのコンピュータプログラムの伝達を容易にする任意の媒体を含む通信媒体の両方を含む。プロセッサは、機械可読記憶媒体に記憶されたソフトウェアモジュールの実行を含む、バスおよび一般的な処理を管理することを担ってもよい。コンピュータ可読記憶媒体は、プロセッサがその記憶媒体から情報を読み取ることができ、かつその記憶媒体に情報を書き込むことができるようにプロセッサに結合されてもよい。代替として、記憶媒体は、プロセッサと一体であってもよい。例として、機械可読媒体は、送信線路、データによって変調された搬送波、および/またはワイヤレスノードとは別個の命令が記憶されたコンピュータ可読記憶媒体を含んでもよく、これらはすべて、バスインターフェースを介してプロセッサによってアクセスされる場合がある。代替としてまたは追加として、機械可読媒体またはその任意の部分は、キャッシュおよび/または汎用レジスタファイルと同様にプロセッサに統合されてもよい。機械可読記憶媒体の例は、例として挙げると、RAM(ランダムアクセスメモリ)、フラッシュメモリ、ROM(読取り専用メモリ)、PROM(プログラマブル読取り専用メモリ)、EPROM(消去可能プログラマブル読取り専用メモリ)、EEPROM(電氣的消去可能プログラマブル読取り専用メモリ)、レジスタ、磁気ディスク、光ディスク、ハードドライブ、もしくは任意の他の適切な記憶媒体、またはそれらの任意の組合せがあってもよい。機械可読媒体はコンピュータプログラム製品内で具現化されてもよい。

【0128】

ソフトウェアモジュールは、単一の命令または多くの命令を含んでもよく、いくつかの異なるコードセグメントにわたって、異なるプログラム間で、また複数の記憶媒体にわたって分散されてもよい。コンピュータ可読媒体は、いくつかのソフトウェアモジュールを含んでもよい。ソフトウェアモジュールは、プロセッサなどの装置によって実行されると、処理システムに様々な機能を実行させる命令を含む。ソフトウェアモジュールは、送信モジュールと受信モジュールとを含んでもよい。各ソフトウェアモジュールは、単一の記憶デバイス内に存在しても、または複数の記憶デバイスにわたって分散されてもよい。例として、トリガイベントが発生したときに、ソフトウェアモジュールは、ハードドライブからRAMにロードされてもよい。ソフトウェアモジュールの実行中、プロセッサは、アクセス速度を高めるために、命令のうちのいくつかをキャッシュにロードしてもよい。1つまたは複数のキャッシュラインが、次いでプロセッサによって実行されるように汎用レジスタファイルにロードされてもよい。以下でソフトウェアモジュールの機能に言及する場合、そのような機能は、そのソフトウェアモジュールからの命令を実行するときにプロセッサによって実装されることが理解されよう。

【0129】

また、任意の接続が、適切にコンピュータ可読媒体と呼ばれる。たとえば、ソフトウェアが、同軸ケーブル、光ファイバケーブル、ツイストペア、デジタル加入者回線(DSL)、または赤外線(IR)、無線、およびマイクロ波などのワイヤレス技術を使用して、ウェブサイト、サーバ、または他のリモートソースから送信される場合、同軸ケーブル、光ファ

10

20

30

40

50

イバーケーブル、ツイストペア、DSL、または赤外線、無線、およびマイクロ波などのワイヤレス技術は、媒体の定義に含まれる。本明細書で使用するディスク(disk)およびディスク(disc)は、コンパクトディスク(disc)(CD)、レーザディスク(disc)、光ディスク(disc)、デジタル多用途ディスク(disc)(DVD)、フロッピー(登録商標)ディスク(disk)、およびBlu-ray(登録商標)ディスク(disc)を含み、ディスク(disk)は、通常、データを磁気的に再生し、ディスク(disc)は、レーザを用いてデータを光学的に再生する。したがって、いくつかの態様では、コンピュータ可読媒体は、非一時的コンピュータ可読媒体(たとえば、有形媒体)を含んでもよい。加えて、他の態様の場合、コンピュータ可読媒体は、一時的コンピュータ可読媒体(たとえば、信号)を含んでもよい。上記の組合せもコンピュータ可読媒体の範囲に含まれるべきである。

10

【0130】

さらに、本明細書で説明する方法および技法を実行するためのモジュールおよび/または他の適切な手段は、適用可能な場合、ユーザ端末および/または基地局によってダウンロードおよび/または別の方法で取得されてもよいことを理解されたい。たとえば、そのようなデバイスは、本明細書で説明する方法を実行するための手段の転送を容易にするためにサーバに結合されてもよい。代替的に、本明細書で説明する様々な方法は、ユーザ端末および/または基地局が記憶手段(たとえば、RAM、ROM、コンパクトディスク(CD)またはフロッピー(登録商標)ディスクなどの物理的記憶媒体など)をデバイスに結合または提供すると様々な方法で取得することができるように、記憶手段を介して提供されてもよい。さらに、本明細書で説明する方法および技法をデバイスに提供するための任意の他の適切な技法が利用されてもよい。

20

【0131】

特許請求の範囲が上記で示した厳密な構成および構成要素に限定されないことを理解されたい。特許請求の範囲の範囲から逸脱することなく、上記で説明した方法および装置の構成、動作、および詳細において、様々な修正、変更、および変形が加えられてもよい。

【符号の説明】

【0132】

100 ワイヤレスネットワーク

102a マクロセル

102b マクロセル

102c マクロセル

102x ピコセル

102y フェムトセル

102z フェムトセル

110 BS、基地局

110a BS

110b BS

110c BS、マクロBS

110r 中継局

110x BS

110y BS

110z BS

118 PDNゲートウェイ

120 UE、ユーザ機器

120a UE

120r UE

120y UE

130 ネットワークコントローラ

200 分散型無線アクセスネットワーク(RAN)、分散型RAN、ローカルアーキテクチャ、アーキテクチャ

30

40

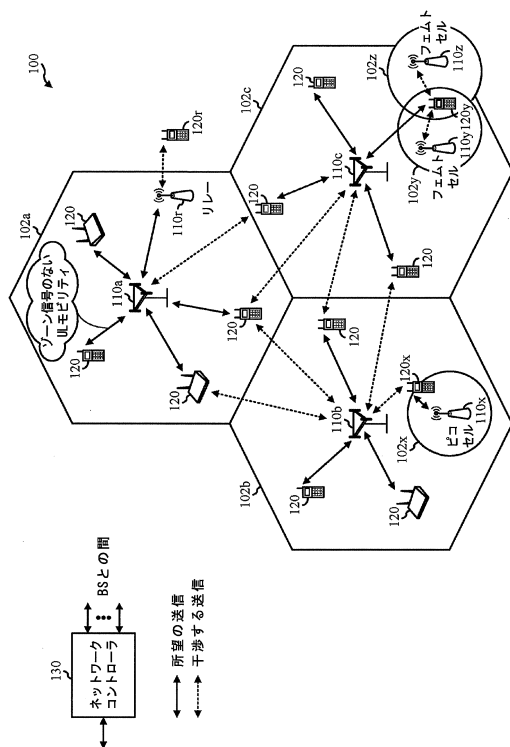
50

202	アクセスノードコントローラ(ANC)	
204	次世代コアネットワーク(NG-CN)	
206	5Gアクセスノード	
208	TRP、DU	
210	次世代AN(NG-AN)	
220	送信プロセッサ	
234	アンテナ	
238	受信プロセッサ	
240	コントローラ/プロセッサ	
252	アンテナ	10
258	受信プロセッサ	
264	送信プロセッサ	
280	コントローラ/プロセッサ	
300	分散型RAN	
302	集中型コアネットワークユニット(C-CU)	
304	集中型RANユニット(C-RU)	
306	DU	
412	データソース	
420	プロセッサ、送信プロセッサ	
430	プロセッサ、送信(TX)多入力多出力(MIMO)プロセッサ	20
432	変調器	
432a ~ 432t	変調器(MOD)	
434	アンテナ	
434a ~ 434t	アンテナ	
436	MIMO検出器	
438	プロセッサ、受信プロセッサ	
439	データシンク	
440	コントローラ/プロセッサ、プロセッサ	
442	メモリ	
444	スケジューラ	30
452	アンテナ	
452a ~ 452r	アンテナ	
454	復調器	
454a ~ 454r	復調器(DEMOD)	
456	MIMO検出器	
458	プロセッサ、受信プロセッサ	
460	データシンク	
462	データソース	
464	プロセッサ、送信プロセッサ	
466	プロセッサ、TX MIMOプロセッサ	40
480	コントローラ/プロセッサ	
482	メモリ	
500	図	
505-a	第1のオプション	
505-b	第2のオプション	
510	無線リソース制御(RRC)レイヤ	
515	パケットデータコンバージェンスプロトコル(PDCP)レイヤ	
520	無線リンク制御(RLC)レイヤ	
525	媒体アクセス制御(MAC)レイヤ	
530	物理(PHY)レイヤ	50

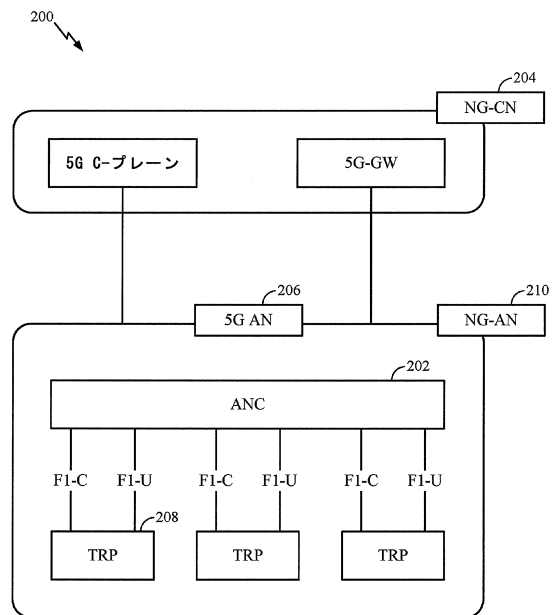
600 図
 602 制御部分
 604 DLデータ部分
 606 共通UL部分
 700 図
 702 制御部分
 704 ULデータ部分
 706 共通UL部分
 800 5Gアーキテクチャ
 900 5Gアーキテクチャ
 1000 動作
 1100 動作
 1300 動作
 1400 動作

【図面】

【図 1】



【図 2】



10

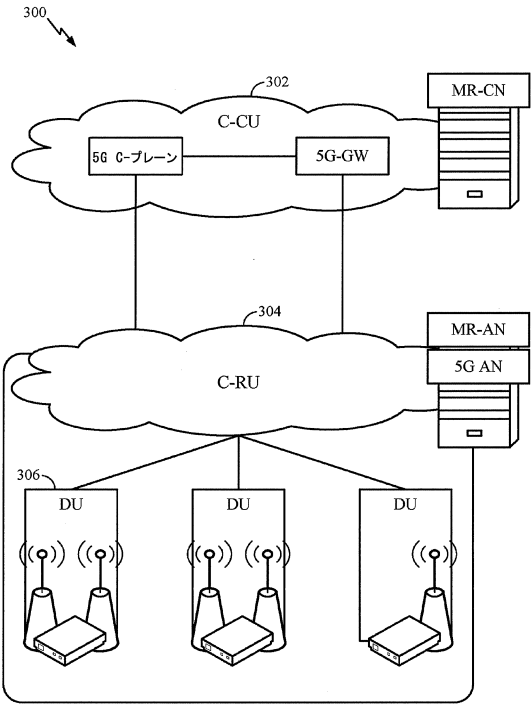
20

30

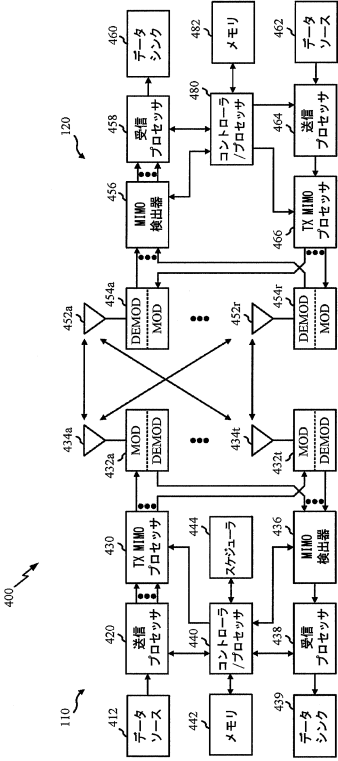
40

50

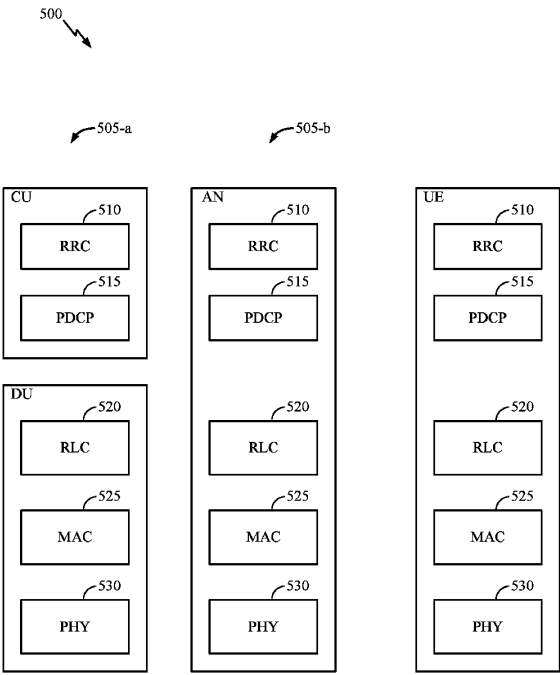
【図 3】



【図 4】



【図 5】



【図 6】

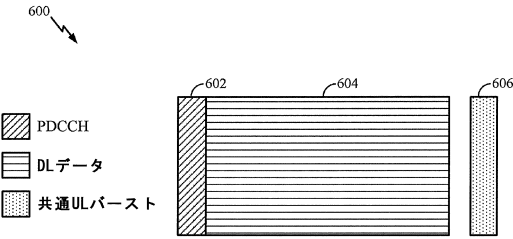


FIG. 5

10

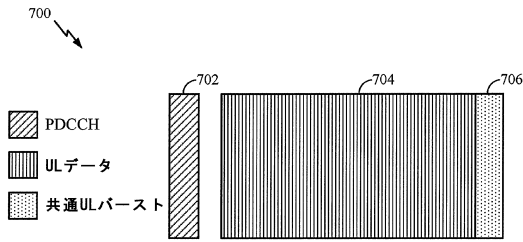
20

30

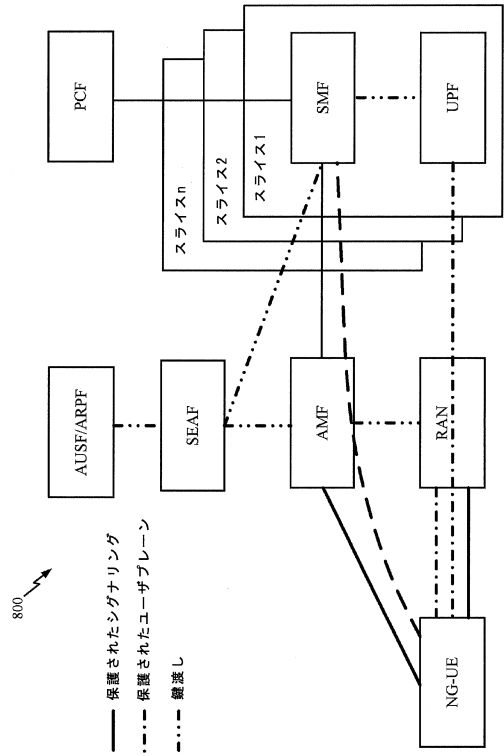
40

50

【図 7】



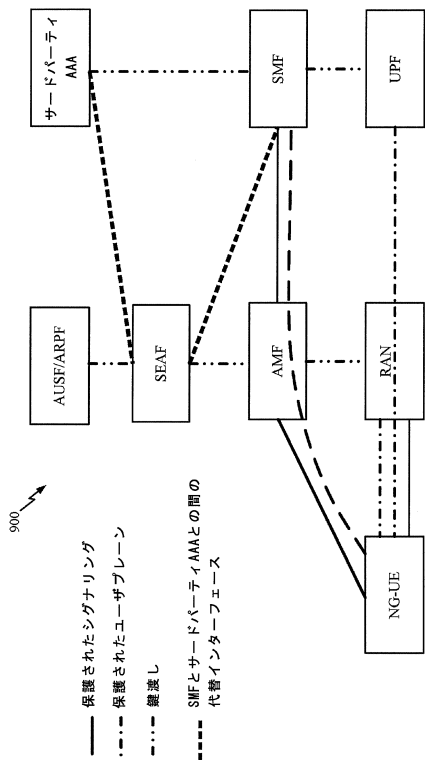
【図 8】



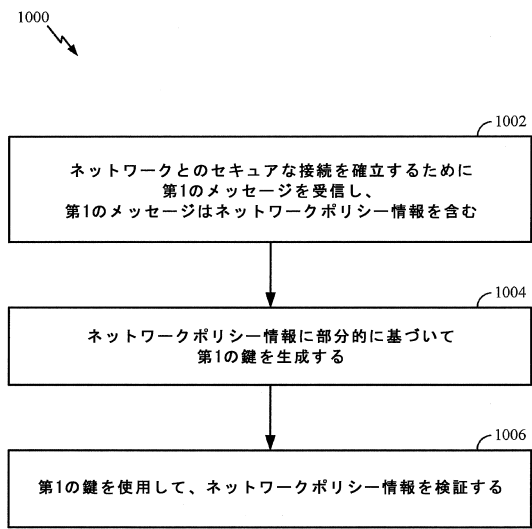
10

20

【図 9】



【図 10】

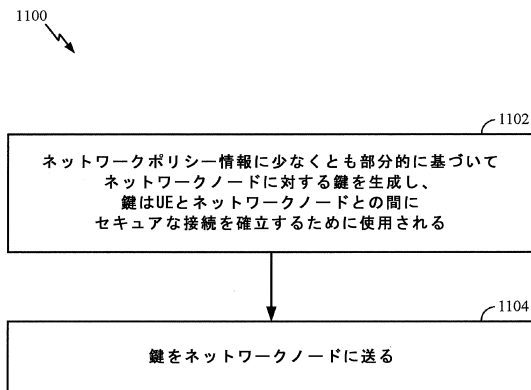


30

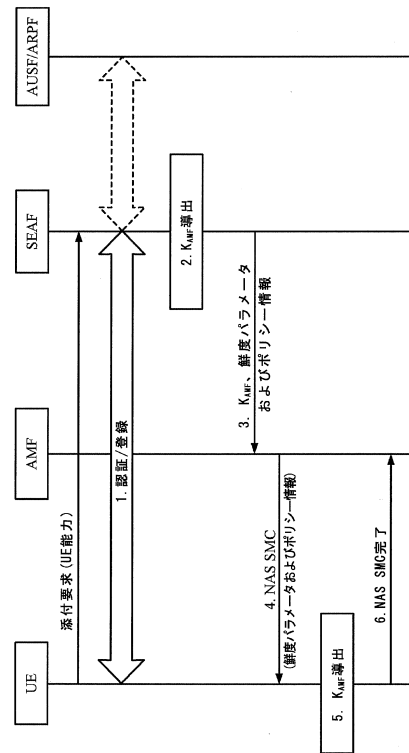
40

50

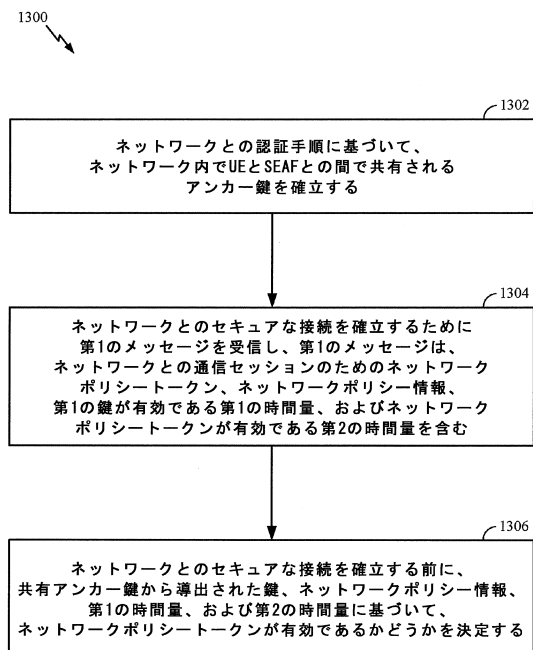
【図 1 1】



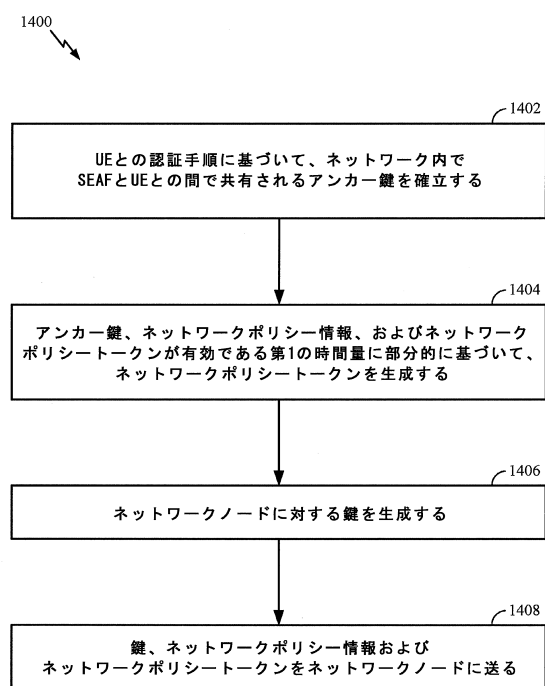
【図 1 2】



【図 1 3】



【図 1 4】



10

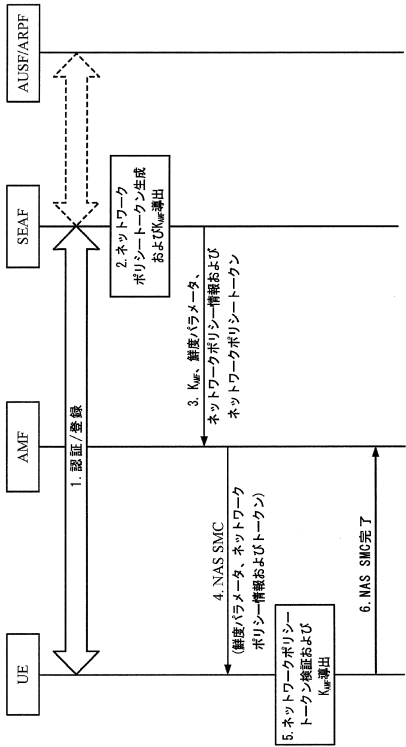
20

30

40

50

【図 15】



10

20

30

40

50

フロントページの続き

(33)優先権主張国・地域又は機関

米国(US)

1 2 1 - 1 7 1 4 ・ サン ・ ディエゴ ・ モアハウス ・ ドライヴ ・ 5 7 7 5

(72)発明者 アナンド ・ パラニガウンダー

アメリカ合衆国 ・ カリフォルニア ・ 9 2 1 2 1 - 1 7 1 4 ・ サン ・ ディエゴ ・ モアハウス ・ ドライヴ ・ 5 7 7 5

審査官 伊東 和重

(56)参考文献

Qualcomm Incorporated , pCR to provide a normative text for the AMF key derivation/refresh[online] , 3GPP TSG SA WG3 #88 , 3GPP , 2017年08月11日 , S3-172010 , 検索日[2022.08.16],Internet URL:http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_88_Dali/Docs/S3-172010.zip

Qualcomm Incorporated , Some corrections and clarification to the authentication text[online] , 3GPP TSG SA WG3 #88 , 3GPP , 2017年08月11日 , S3-172145 , 検索日[2022.08.16],Internet URL:http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_88_Dali/Docs/S3-172145.zip

Huawei, Hisilicon , Solution for IMSI Privacy while meeting LI Requirements[online] , 3GPP TSG SA WG3 #87 , 3GPP , 2017年05月19日 , S3-171510 , 検索日[2022.08.16],Internet URL:http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_87_Ljubljana/Docs/S3-171510.zip

Qualcomm Incorporated , pCR to provide a normative text for the AMF key derivation/refresh[online] , 3GPP TSG SA WG3 #88Bis , 3GPP , 2017年10月02日 , S3-172387 , 検索日[2022.08.16],Internet URL:http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_88Bis_Singapore/Docs/S3-172387.zip

(58)調査した分野 (Int.Cl. , D B 名)

H 0 4 B 7 / 2 4 - 7 / 2 6

H 0 4 W 4 / 0 0 - 9 9 / 0 0

H 0 4 L 9 / 0 8

3 G P P T S G R A N W G 1 - 4

S A W G 1 - 4

C T W G 1 , 4