

(19)日本国特許庁(JP)

(12)公表特許公報(A)

(11)公表番号
特表2024-530862
(P2024-530862A)

(43)公表日 令和6年8月27日(2024.8.27)

(51)国際特許分類		F I		テーマコード (参考)	
H O 4 W	56/00 (2009.01)	H O 4 W	56/00	1 3 0	5 K 0 6 7
H O 4 W	12/069 (2021.01)	H O 4 W	12/069		
H O 4 W	12/037 (2021.01)	H O 4 W	12/037		
H O 4 W	64/00 (2009.01)	H O 4 W	64/00		
H O 4 W	12/122 (2021.01)	H O 4 W	12/122		
		審査請求	未請求	予備審査請求	未請求 (全72頁) 最終頁に続く
(21)出願番号	特願2024-500574(P2024-500574)				
(86)(22)出願日	令和4年6月6日(2022.6.6)				
(85)翻訳文提出日	令和6年1月9日(2024.1.9)				
(86)国際出願番号	PCT/US2022/032396				
(87)国際公開番号	WO2023/009218				
(87)国際公開日	令和5年2月2日(2023.2.2)				
(31)優先権主張番号	17/386,325				
(32)優先日	令和3年7月27日(2021.7.27)				
(33)優先権主張国・地域又は機関	米国(US)				
(81)指定国・地域	AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA, RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,A T,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR ,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC, 最終頁に続く				
(71)出願人	595020643 クualコム・インコーポレイテッド QUALCOMM INCORPORATED アメリカ合衆国、カリフォルニア州 9 2 1 2 1-1 7 1 4、サン・ディエゴ、モアハウス・ドライブ 5 7 7 5				
(74)代理人	110003708 弁理士法人鈴榮特許総合事務所				
(72)発明者	エッジ、スティーブン・ウィリアム アメリカ合衆国、カリフォルニア州 9 2 1 2 1-1 7 1 4、サン・ディエゴ、モアハウス・ドライブ 5 7 7 5				
F ターム (参考)	5K067 AA33 EE02 EE10 HH36				

(54)【発明の名称】 ワイヤレスネットワークにおける信頼できる時刻の取得のための方法および装置

(57)【要約】

正確で信頼できる時刻が、ワイヤレスネットワーク内の基地局からユーザ機器（UE）によって取得される。基地局は、時刻、たとえば、UTC時刻またはGNSS時刻を取得し得、時刻をブロードキャストする前に時刻の少なくとも一部分を暗号化する。UEは、タイミングアドバンス、UEおよび基地局の既知のロケーション、またはUEと基地局との間の実測往復伝搬時間（RTT）に基づいて、UEと基地局との間の伝搬遅延を決定する。基地局から受信した時刻と伝搬遅延とに基づいて、補正済み時刻を決定することができる。基地局によってブロードキャストされる時刻に含まれているデジタル署名により、信頼性が向上する。攻撃デバイスによるブロードキャストされた時刻のスプーフィングは、伝搬遅延が予想範囲外であることに基づいて、UEによって検出され得る。

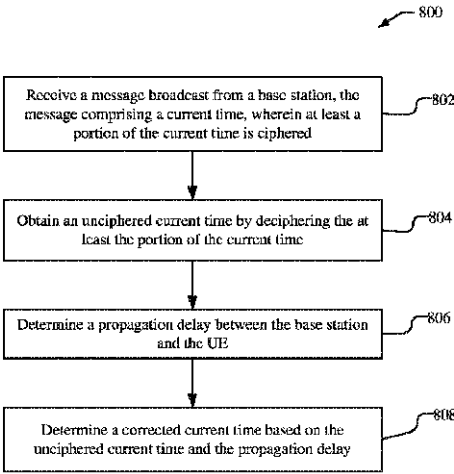


FIG. 8

【特許請求の範囲】

【請求項 1】

ワイヤレスネットワークにおける時刻の取得をサポートするためにユーザ機器（UE）によって実行される方法であって、
基地局からブロードキャストされたメッセージを受信することと、前記メッセージが現在時刻を含み、前記現在時刻の少なくとも一部分が暗号化され、
前記現在時刻の前記少なくとも前記一部分を解読することによって、平文の現在時刻を取得することと、
前記基地局と前記UEとの間の伝搬遅延を決定することと、
前記平文の現在時刻と前記伝搬遅延とに基づいて、補正済み現在時刻を決定することと、
を備える、方法。

10

【請求項 2】

前記現在時刻が、協定世界時（UTC）時刻、全地球測位システム（GPS）時刻、GLONASS時刻、Beidou時刻、Galileo時刻、全地球航法衛星システム（GNSS）時刻、またはローカル地域時刻を備える、請求項 1 に記載の方法。

【請求項 3】

前記伝搬遅延を決定することが、
前記基地局からタイミングアドバンスを取得すること、前記伝搬遅延が、前記タイミングアドバンスから決定される、
前記UEのロケーションおよび前記基地局のロケーションを取得すること、前記伝搬遅延が、前記UEの前記ロケーションと前記基地局の前記ロケーションとの間の距離に基づいて決定される、または、
前記UEと前記基地局との間の往復伝搬時間（RTT）を測定すること、前記伝搬遅延が前記RTTの半分に等しい、
のうちの1つを備える、請求項 1 に記載の方法。

20

【請求項 4】

前記UEの前記ロケーションおよび前記基地局の前記ロケーションを取得することが、システム情報ブロック（SIB）中で前記基地局の前記ロケーションのブロードキャストを前記基地局から受信すること、
前記基地局の前記ロケーションを含むロングタームエボリューション（LTE）測位プロトコル（LPP）支援データメッセージを受信すること、
前記UEの前記ロケーションを含むモバイル発信ロケーション情報要求（MO-LR）応答メッセージを受信すること、または、
前記UEの前記ロケーションを決定するために、測位セッションを実行すること、
のうちの少なくとも1つを備える、請求項 3 に記載の方法。

30

【請求項 5】

前記RTTを測定することが、
前記基地局用の第1のローカル送信時刻を示す第1のメッセージを前記基地局から受信することと、
前記基地局用の前記第1のローカル送信時刻と前記UEにおける前記第1のメッセージの受信のローカル時刻とに基づいて、前記UEにおけるローカルタイミングを前記基地局用のローカル送信時刻に関連付けることと、
ランダムアクセスチャネル（RACH）上で前記基地局に第2のメッセージを送信することと、前記第2のメッセージがランダム変数を備え、前記第2のメッセージが第1の時刻に送信され、前記第1の時刻が前記UEにおけるローカル時刻または前記基地局用の関連付けられたローカル送信時刻のいずれか一方である、
前記第2のメッセージに応答して前記基地局から第3のメッセージを受信することと、前記第3のメッセージが第2の時刻と前記ランダム変数とを備え、前記第2の時刻が、前記第2のメッセージが前記基地局において受信された前記基地局用の前記ローカル送信時

40

50

刻である、

前記第 1 の時刻と前記第 2 の時刻とに基づいて前記 R T T を決定することと、
を備える、請求項 3 に記載の方法。

【請求項 6】

前記第 3 のメッセージが暗号化される、請求項 5 に記載の方法。

【請求項 7】

前記第 3 のメッセージが、前記基地局用のデジタル署名をさらに含み、前記方法が、
前記基地局用の前記デジタル署名に基づいて前記第 3 のメッセージを認証すること、
をさらに備える、請求項 5 に記載の方法。

【請求項 8】

攻撃デバイスが、前記 U E と前記基地局との間の前記ワイヤレスネットワーク内に存在
し、前記メッセージが、リプレイ攻撃中に前記攻撃デバイスを介して受信され、前記方法
が、

前記タイミングアドバンスから、または前記 R T T を測定することによって、前記伝搬
遅延を決定することと、

前記伝搬遅延が予想範囲外であることに基づいて、前記攻撃デバイスの前記存在を検出
することと、

をさらに備える、請求項 3 に記載の方法。

【請求項 9】

前記予想範囲が、前記基地局への最大予想距離に基づく最大伝搬遅延を備える、請求項
8 に記載の方法。

【請求項 10】

前記 U E の推定ロケーションおよび前記基地局の前記ロケーションを取得することと、
前記 U E の前記推定ロケーションと前記基地局の前記ロケーションとの間の距離推定値
を決定することと、

前記距離推定値に基づいて前記予想範囲を決定することと、をさらに備える、請求項 8
に記載の方法。

【請求項 11】

前記メッセージが、基地局サブフレームまたはスロット境界への前記現在時刻の暗黙的
または明示的なアライメント、前記現在時刻の不確実性、前記現在時刻のソース、または
それらの組合せのうちの少なくとも 1 つをさらに備える、請求項 1 に記載の方法。

【請求項 12】

前記メッセージが、前記基地局用のデジタル署名をさらに含み、前記方法が、
前記基地局用の前記デジタル署名に基づいて、前記メッセージ中の前記現在時刻を認証
すること、

をさらに含む、請求項 1 に記載の方法。

【請求項 13】

前記ワイヤレスネットワークから前記基地局用の公開暗号化鍵を受信すること、前記デ
ジタル署名が、前記公開暗号化鍵に対応する秘密暗号化鍵に基づくものであり、前記現在
時刻を認証することが、前記公開暗号化鍵を使用する、

をさらに備える、請求項 12 に記載の方法。

【請求項 14】

ワイヤレスネットワークにおける時刻の取得をサポートするように構成されたユーザ機
器 (U E) であって、

前記ワイヤレスネットワーク内の基地局とワイヤレス通信するように構成されたワイヤ
レストランシーバと、

少なくとも 1 つのメモリと、

前記ワイヤレストランシーバおよび前記少なくとも 1 つのメモリに結合された少なくと
も 1 つのプロセッサと、を備え、前記少なくとも 1 つのプロセッサが、

前記ワイヤレストランシーバを介して、基地局からブロードキャストされたメッセージ

10

20

30

40

50

を受信し、前記メッセージが現在時刻を含み、前記現在時刻の少なくとも一部分が暗号化され、

前記現在時刻の前記少なくとも前記一部分を解読することによって、平文の現在時刻を取得し、

前記基地局と前記UEとの間の伝搬遅延を決定し、

前記平文の現在時刻と前記伝搬遅延とに基づいて、補正済み現在時刻を決定する、ように構成される、ユーザ機器（UE）。

【請求項15】

前記現在時刻が、協定世界時（UTC）時刻、全地球測位システム（GPS）時刻、GLONASS時刻、Beidou時刻、Galileo時刻、全地球航法衛星システム（GNSS）時刻、またはローカル地域時刻を備える、請求項14に記載のUE。

10

【請求項16】

前記少なくとも1つのプロセッサが、

前記ワイヤレスランシーバを介して、前記基地局からタイミングアドバンスを取得すること、前記伝搬遅延が前記タイミングアドバンスから決定される、

前記UEのロケーションおよび前記基地局のロケーションを取得すること、前記伝搬遅延が、前記UEの前記ロケーションと前記基地局の前記ロケーションとの間の距離に基づいて決定される、または、

前記UEと前記基地局との間の往復伝搬時間（RTT）を測定すること、前記伝搬遅延が前記RTTの半分に等しい、

20

のうちの1つによって、前記伝搬遅延を決定するように構成される、請求項14に記載のUE。

【請求項17】

前記少なくとも1つのプロセッサが、

前記ワイヤレスランシーバを介して、システム情報ブロック（SIB）中で前記基地局の前記ロケーションのブロードキャストを前記基地局から受信すること、

前記ワイヤレスランシーバを介して、前記基地局の前記ロケーションを含むロングタームエボリューション（LTE）測位プロトコル（LPP）支援データメッセージを受信すること、

前記ワイヤレスランシーバを介して、前記UEの前記ロケーションを含むモバイル発信ロケーション情報要求（MO-LR）応答メッセージを受信すること、または、

30

前記UEの前記ロケーションを決定するために、測位セッションを実行すること、

のうちの少なくとも1つによって、前記UEの前記ロケーションおよび前記基地局の前記ロケーションを取得するように構成される、請求項16に記載のUE。

【請求項18】

前記少なくとも1つのプロセッサが、

前記ワイヤレスランシーバを介して、前記基地局用の第1のローカル送信時刻を示す第1のメッセージを前記基地局から受信し、

前記基地局用の前記第1のローカル送信時刻と前記UEにおける前記第1のメッセージの受信のローカル時刻とに基づいて、前記UEにおけるローカルタイミングを前記基地局用のローカル送信時刻に関連付け、

40

前記ワイヤレスランシーバを介して、ランダムアクセスチャネル（RACH）上で前記基地局に第2のメッセージを送信し、前記第2のメッセージがランダム変数を備え、前記第2のメッセージが第1の時刻に送信され、前記第1の時刻が、前記UEにおけるローカル時刻または前記基地局用の関連付けられたローカル送信時刻のいずれか一方であり、

前記ワイヤレスランシーバを介して、前記第2のメッセージに応答して前記基地局から第3のメッセージを受信し、前記第3のメッセージが第2の時刻と前記ランダム変数とを含み、前記第2の時刻が、前記第2のメッセージが前記基地局において受信された前記基地局用の前記ローカル送信時刻であり、

前記第1の時刻と前記第2の時刻とに基づいて前記RTTを決定する、

50

ように構成されることによって、前記 R T T を測定するように構成される、請求項 1 6 に記載の U E。

【請求項 1 9】

前記第 3 のメッセージが暗号化される、請求項 1 8 に記載の U E。

【請求項 2 0】

前記第 3 のメッセージが、前記基地局用のデジタル署名をさらに含み、前記少なくとも 1 つのプロセッサが、

前記基地局用の前記デジタル署名に基づいて前記第 3 のメッセージを認証する、
ようにさらに構成される、請求項 1 8 に記載の U E。

【請求項 2 1】

攻撃デバイスが、前記 U E と前記基地局との間の前記ワイヤレスネットワーク内に存在し、前記メッセージが、リプレイ攻撃中に前記攻撃デバイスを介して受信され、前記少なくとも 1 つのプロセッサが、

前記タイミングアドバンスから、または前記 R T T を測定することによって、前記伝搬遅延を決定し、

前記伝搬遅延が予想範囲外であることに基づいて、前記攻撃デバイスの前記存在を検出する、

ようにさらに構成される、請求項 1 6 に記載の U E。

【請求項 2 2】

前記予想範囲が、前記基地局への最大予想距離に基づく最大伝搬遅延を備える、請求項 2 1 に記載の U E。

【請求項 2 3】

前記少なくとも 1 つのプロセッサが、

前記 U E の推定ロケーションおよび前記基地局の前記ロケーションを取得し、

前記 U E の前記推定ロケーションと前記基地局の前記ロケーションとの間の距離推定値を決定し、

前記距離推定値に基づいて前記予想範囲を決定する、

ようにさらに構成される、請求項 2 1 に記載の U E。

【請求項 2 4】

前記メッセージが、基地局サブフレームまたはスロット境界への前記現在時刻の暗黙的または明示的なアライメント、前記現在時刻の不確実性、前記現在時刻のソース、またはそれらの組合せのうちの少なくとも 1 つをさらに備える、請求項 1 4 に記載の U E。

【請求項 2 5】

前記メッセージが、前記基地局用のデジタル署名をさらに含み、前記少なくとも 1 つのプロセッサが、

前記基地局用の前記デジタル署名に基づいて前記メッセージ中の前記現在時刻を認証する、

ようにさらに構成される、請求項 1 4 に記載の U E。

【請求項 2 6】

前記少なくとも 1 つのプロセッサが、

前記ワイヤレスネットワークから前記基地局用の公開暗号化鍵を受信し、前記デジタル署名が、前記公開暗号化鍵に対応する秘密暗号化鍵に基づくものであり、前記現在時刻を認証することが、前記公開暗号化鍵を使用する、

ようにさらに構成される、請求項 2 5 に記載の U E。

【請求項 2 7】

ワイヤレスネットワークにおける時刻の取得をサポートするように構成されたユーザ機器 (U E) であって、

基地局からブロードキャストされたメッセージを受信するための手段と、前記メッセージが現在時刻を含み、前記現在時刻の少なくとも一部分が暗号化され、

前記現在時刻の前記少なくとも前記一部分を解読することによって、平文の現在時刻を

10

20

30

40

50

取得するための手段と、

前記基地局と前記UEとの間の伝搬遅延を決定するための手段と、

前記平文の現在時刻と前記伝搬遅延とに基づいて、補正済み現在時刻を決定するための手段と、

を備える、ユーザ機器（UE）。

【請求項28】

前記伝搬遅延を決定するための前記手段が、

前記基地局からタイミングアドバンスを取得するための手段、前記伝搬遅延が前記タイミングアドバンスから決定される、

前記UEのロケーションおよび前記基地局のロケーションを取得するための手段、前記伝搬遅延が、前記UEの前記ロケーションと前記基地局の前記ロケーションとの間の距離に基づいて決定される、または、

前記UEと前記基地局との間の往復伝搬時間（RTT）を測定するための手段、前記伝搬遅延が前記RTTの半分に等しい、

のうちの1つを備える、請求項27に記載のUE。

【請求項29】

それに記憶されているプログラムコードを含む非一時的コンピュータ可読記憶媒体であって、前記プログラムコードが、ワイヤレスネットワークにおける時刻の取得をサポートするためにユーザ機器（UE）内の少なくとも1つのプロセッサを構成するように動作可能であり、前記プログラムコードが、

基地局からブロードキャストされたメッセージを受信し、前記メッセージが現在時刻を含み、前記現在時刻の少なくとも一部分が暗号化され、

前記現在時刻の前記少なくとも前記一部分を解読することによって、平文の現在時刻を取得し、

前記基地局と前記UEとの間の伝搬遅延を決定し、

前記平文の現在時刻と前記伝搬遅延とに基づいて、補正済み現在時刻を決定する、ための命令を含む、非一時的コンピュータ可読記憶媒体。

【請求項30】

前記伝搬遅延を決定するための前記命令が、

前記基地局からタイミングアドバンスを取得すること、前記伝搬遅延が前記タイミングアドバンスから決定される、

前記UEのロケーションおよび前記基地局のロケーションを取得すること、前記伝搬遅延が、前記UEの前記ロケーションと前記基地局の前記ロケーションとの間の距離に基づいて決定される、または、

前記UEと前記基地局との間の往復伝搬時間（RTT）を測定すること、前記伝搬遅延が前記RTTの半分に等しい、

のうちの1つを行うための命令を含む、請求項29に記載の非一時的コンピュータ可読記憶媒体。

【発明の詳細な説明】

【優先権の主張】

【0001】

関連出願の相互参照

【0001】 本出願は、本出願の譲受人に譲渡され、その全体が参照により本明細書に明確に組み込まれる、2021年7月27日に出願された「METHOD AND APPARATUS FOR ACQUISITION OF RELIABLE TIME IN A WIRELESS NETWORK」と題する米国非仮特許出願第17／386,325号の利益を主張する。

【技術分野】

【0002】

分野

10

20

30

40

50

【0002】 本開示は、概して、ネットワークにおけるワイヤレス通信の分野に関し、より具体的には、ワイヤレスネットワークを介した時刻のブロードキャストおよび信頼性のある取得に関する。

【背景技術】

【0003】

情報

【0003】 ワイヤレス通信システムは、音声、ビデオ、パケットデータ、メッセージング、ブロードキャストなどの様々なタイプの通信コンテンツを提供するために広く展開されている。これらのシステムは、利用可能なシステムリソース（たとえば、時刻、周波数、および電力）を共有することにより、複数のユーザとの通信をサポートすることができ得る。このような多元接続システムの例は、符号分割多元接続（Code Division Multiple Access：CDMA）システム、時分割多元接続（Time Division Multiple Access：TDMA）システム、周波数分割多元接続（Frequency Division Multiple Access：FDMA）システム、および直交周波数分割多元接続（Orthogonal Frequency Division Multiple Access：OFDMA）システムを含む。ワイヤレス多元接続通信システムは、各々がユーザ機器（User Equipment：UE）と呼ばれることがあ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み得る。

【0004】

【0004】 これらの多元接続技術は、様々なワイヤレスデバイスが都市レベル、国家レベル、地域レベル、および世界レベルでも通信することを可能にする共通のプロトコルを提供するために、様々な遠隔通信規格において採用されている。新興の遠隔通信規格の一例として、新無線（New Radio：NR）、たとえば、5G無線アクセスが挙げられる。NRは、第3世代パートナーシッププロジェクト（Third Generation Partnership Project：3GPP（登録商標））により発布されたLTE（登録商標）モバイル規格に対する改良のセットである。NRは、スペクトル効率の向上、コストの低減、サービスの改善、新しいスペクトルの利用、ダウンリンク（DownLink：DL）およびアップリンク（UpLink：UL）上でサイクリックプレフィックス（Cyclic Prefix：CP）を用いるOFDMAを使用する他のオープン規格とのよりよい統合によって、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強力にサポートするだけでなく、ビームフォーミング、多入力多出力（Multiple-Input Multiple-Output：MIMO）アンテナ技術、およびキャリアアグリゲーションもサポートするように設計されている。

【0005】

【0005】 4Gまたは5GワイヤレスアクセスをUEに提供することの一部として、ワイヤレスネットワークは、現在時刻（たとえば、UTC時刻またはGPS時刻）をUEに提供することがあり、この現在時刻は、非常に正確である（たとえば、1マイクロ秒（microsecond：μs）までの正確さ）場合もあれば、あまり正確でない（たとえば、1秒までの正確さ）場合もある。たとえば、これは、他のタイミングソース（たとえば、GNSSコンスタレーションからのタイミング）が（たとえば、GNSSの場合、GNSSシステム障害、GNSS信号の利用不可能性、またはジャミングもしくはスプーフィング（spoofing）に起因して）利用不可能であるときに有用であり得る。しかしながら、このようなタイミングサポートは、それ自体が、たとえば、スプーフィングに起因して、信頼性が喪失する可能性がある。

【発明の概要】

【0006】

【0006】 正確で信頼できる時刻が、ワイヤレスネットワーク内の基地局からユーザ機器（UE）によって取得される。基地局は、時刻、たとえば、協定世界時（Coordinated Universal Time：UTC）時刻または全地球航法衛星システム（Global Navigation Satellite System：GNSS）時刻を取得し得、時刻をブロードキャストする前に時刻の少なくとも一部分を暗号化する。UEは、タイミングアドバンス、UEおよび基地

10

20

30

40

50

局の既知のロケーション、またはUEと基地局との間の実測往復伝搬時間（Round Trip Propagation Time：RTT）に基づいて、UEと基地局との間の伝搬遅延を決定する。基地局から受信した時刻と伝搬遅延とに基づいて、補正済み時刻を決定することができる。基地局によってブロードキャストされる時刻に含まれているデジタル署名により、信頼性が向上する。攻撃デバイスによるブロードキャストされた時刻のスプーフィングは、伝搬遅延が予想範囲外であることに基づいて、UEによって検出され得る。

【0007】

【0007】一実装形態では、ワイヤレスネットワークにおける時刻の取得をサポートするためにユーザ機器（UE）によって実行される方法は、基地局からブロードキャストされたメッセージを受信することであって、メッセージが現在時刻を含み、現在時刻の少なくとも一部分が暗号化される、受信することと、現在時刻の少なくとも一部分を解読することによって、平文の現在時刻を取得することと、基地局とUEとの間の伝搬遅延を決定することと、平文の現在時刻と伝搬遅延とに基づいて、補正済み現在時刻を決定することと、を含む。

10

【0008】

【0008】一実装形態では、ワイヤレスネットワークにおける時刻の取得をサポートするように構成されたユーザ機器（UE）は、ワイヤレスネットワーク内の基地局とワイヤレス通信するように構成されたワイヤレスランシーバと、少なくとも1つのメモリと、ワイヤレスランシーバおよび少なくとも1つのメモリに結合された少なくとも1つのプロセッサと、を備え、少なくとも1つのプロセッサが、ワイヤレスランシーバを介して、基地局からブロードキャストされたメッセージを受信し、メッセージが現在時刻を含み、現在時刻の少なくとも一部分が暗号化され、現在時刻の少なくとも一部分を解読することによって、平文の現在時刻を取得し、基地局とUEとの間の伝搬遅延を決定し、平文の現在時刻と伝搬遅延とに基づいて、補正済み現在時刻を決定する、ように構成される。

20

【0009】

【0009】一実装形態では、ワイヤレスネットワークにおける時刻の取得をサポートするように構成されたユーザ機器（UE）は、基地局からブロードキャストされたメッセージを受信するための手段であって、メッセージが現在時刻を含み、現在時刻の少なくとも一部分が暗号化される、受信するための手段と、現在時刻の少なくとも一部分を解読することによって、平文の現在時刻を取得するための手段と、基地局とUEとの間の伝搬遅延を決定するための手段と、平文の現在時刻と伝搬遅延とに基づいて、補正済み現在時刻を決定するための手段と、を備える。

30

【0010】

【0010】一実装形態では、それに記憶されているプログラムコードを含む非一時的コンピュータ可読記憶媒体は、プログラムコードが、ワイヤレスネットワークにおける時刻の取得をサポートするためにユーザ機器（UE）内の少なくとも1つのプロセッサを構成するように動作可能であり、プログラムコードが、基地局からブロードキャストされたメッセージを受信し、メッセージが現在時刻を含み、現在時刻の少なくとも一部分が暗号化され、現在時刻の少なくとも一部分を解読することによって、平文の現在時刻を取得し、基地局とUEとの間の伝搬遅延を決定し、平文の現在時刻と伝搬遅延とに基づいて、補正済み現在時刻を決定する、ための命令を含む。

40

【0011】

【0011】一実装形態では、ワイヤレスネットワークにおける、ユーザ機器（UE）による時刻の取得をサポートするために基地局によって実行される方法は、現在時刻を取得することと、現在時刻の少なくとも一部分を暗号化することと、現在時刻を含むメッセージをブロードキャストすることと、を含み、UEが、メッセージを受信し、現在時刻の少なくとも一部分を解読することによって平文の現在時刻を取得し、かつ基地局とUEとの間の伝搬遅延を決定し、UEが、平文の現在時刻と伝搬遅延とに基づいて、補正済み現在時刻を決定する。

【0012】

50

【0012】一実装形態では、ワイヤレスネットワークにおけるユーザ機器（UE）による時刻の取得をサポートするように構成された基地局は、ワイヤレスネットワーク内のエンティティとワイヤレス通信するように構成された外部インターフェースと、少なくとも1つのメモリと、外部インターフェースおよび少なくとも1つのメモリに結合された少なくとも1つのプロセッサと、を含み、少なくとも1つのプロセッサが、現在時刻を取得し、現在時刻の少なくとも一部分を暗号化し、現在時刻を含むメッセージをブロードキャストする、ように構成され、UEが、メッセージを受信し、現在時刻の少なくとも一部分を解読することによって平文の現在時刻を取得し、かつ基地局とUEとの間の伝搬遅延を決定し、UEが、平文の現在時刻と伝搬遅延とに基づいて、補正済み現在時刻を決定する。

【0013】

【0013】一実装形態では、ワイヤレスネットワークにおけるユーザ機器（UE）による時刻の取得をサポートするように構成された基地局は、現在時刻を取得するための手段と、現在時刻の少なくとも一部分を暗号化するための手段と、現在時刻を含むメッセージをブロードキャストするための手段と、を含み、UEが、メッセージを受信し、現在時刻の少なくとも一部分を解読することによって平文の現在時刻を取得し、かつ基地局とUEとの間の伝搬遅延を決定し、UEが、平文の現在時刻と伝搬遅延とに基づいて、補正済み現在時刻を決定する。

【0014】

【0014】一実装形態では、それに記憶されているプログラムコードを含む非一時的コンピュータ可読記憶媒体であって、プログラムコードが、ワイヤレスネットワークにおける、ユーザ機器（UE）による時刻の取得をサポートするために基地局内の少なくとも1つのプロセッサを構成するように動作可能であり、プログラムコードが、現在時刻を取得し、現在時刻の少なくとも一部分を暗号化し、現在時刻を含むメッセージをブロードキャストする、ための命令を含み、UEが、メッセージを受信し、現在時刻の少なくとも一部分を解読することによって平文の現在時刻を取得し、かつ基地局とUEとの間の伝搬遅延を決定し、UEが、平文の現在時刻と伝搬遅延とに基づいて、補正済み現在時刻を決定する、非一時的コンピュータ可読記憶媒体。

【図面の簡単な説明】

【0015】

【0015】添付の図面は、本開示の様々な態様の説明の助けとなるように提示され、態様の限定ではなく、例示のためにのみ提供される。

【図1】【0016】本開示の一態様による、ワイヤレス通信システムの高レベルシステムアーキテクチャを示す。

【図2A】【0017】基地局からのメッセージにおいてブロードキャストされ得る現在時刻のフォーマットを示す。

【図2B】【0018】基地局からブロードキャストされ得る現在時刻の暗号化を示す。

【図2C】基地局からブロードキャストされ得る現在時刻の暗号化を示す。

【図2D】基地局からブロードキャストされ得る現在時刻の暗号化を示す。

【図2E】【0019】基地局からブロードキャストされ得る現在時刻についての追加情報を示す。

【図3A】【0020】ワイヤレスネットワークにおける時刻のブロードキャストおよび取得のためのシグナリングフローを示す。

【図3B】【0021】ワイヤレスネットワークにおける時刻のブロードキャストおよび取得、ならびに基地局とUEとの間の伝搬遅延の決定のためのシグナリングフローを示す。

【図4A】【0022】攻撃デバイスが存在し、リプレイ攻撃を実行しているワイヤレスネットワークにおける時刻のブロードキャストおよび取得のためのシグナリングフローを示す。

【図4B】【0023】リプレイ攻撃の存在下で、ワイヤレスネットワークにおける時刻のブロードキャストおよび取得、ならびに基地局とUEとの間の伝搬遅延の決定のための信頼性が向上したシグナリングフローを示す。

10

20

30

40

50

【図5】[0024] ワイヤレスネットワークにおける時刻のブロードキャストおよび取得、ならびに攻撃デバイスによるリプレイ攻撃の検出のためのシグナリングフローを示す。

【図6】[0025] ワイヤレスネットワークからの現在時刻の取得をサポートするように構成されたUEの特定の例示的な特徴を示す概略ブロック図を示す。

【図7】[0026] ワイヤレスネットワークからの現在時刻の取得をサポートするように構成された基地局の特定の例示的な特徴を示す概略ブロック図を示す。

【図8】[0027] UEによって実施される、ワイヤレスネットワークにおけるUEによる時刻の取得をサポートするための例示的な方法のフローチャートを示す。

【図9】[0028] 基地局によって実施される、ワイヤレスネットワークにおけるUEによる時刻の取得をサポートするための例示的な方法のフローチャートを示す。

【0016】

[0029] 異なる図面における同じ参照ラベルを持っている要素、段階、ステップ、および／またはアクションは、互いに対応し得る（たとえば、互いに類似しており、または同一であり得る）。さらに、様々な図面の中のいくつかの要素は、数字の接頭辞と、それに続く英字または数字の接尾辞を使用して標識される。数字の接頭辞は同じであるが接尾辞が異なる要素は、同じタイプの要素の異なるインスタンスであり得る。接尾辞のない数字の接頭辞は、本明細書ではこの数字の接頭辞を付されたあらゆる要素を言及するために使用される。たとえば、基地局の異なるインスタンス110-1、110-2、110-3が図1に示されている。この場合、基地局110への言及は、基地局110-1、110-2、110-3のいずれかを指す。

【発明を実施するための形態】

【0017】

[0030] 本開示の態様は、例示の目的で提供される様々な例を対象とする以下の説明および関連する図面において提供される。本開示の範囲を逸脱することなく、代替の態様が考案され得る。加えて、本開示の周知の要素は、本開示の関連する詳細を不明瞭にしないように、詳細には説明されていないか、または省略されている。

【0018】

[0031] 「例示的」および／または「例」という語は、本明細書では、「例、事例、または例示となる」ことを意味するために使用される。本明細書で「例示的」および／または「例」として説明されるいかなる態様も、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。同様に、「本開示の態様」という用語は、本開示のすべての態様が、論じられる特徴、利点、または動作モードを含むことを必要とするとは限らない。

【0019】

[0032] 以下で説明する情報および信号が、様々な異なる技術および技法のうちのいずれかを使用して表され得ることは、当業者には理解されるであろう。たとえば、以下の説明全体にわたって言及され得るデータ、命令、コマンド、情報、信号、ビット、シンボル、およびチップは、具体的な用途、所望の設計、対応する技術などに部分的に応じて、電圧、電流、電磁波、磁場もしくは磁性粒子、光場もしくは光学粒子、またはそれらの任意の組合せによって表され得る。

【0020】

[0033] さらに、多くの態様は、たとえば、コンピューティングデバイスの要素によって実行される一連のアクションとして説明される。本明細書で説明される様々なアクションが、特定の回路（たとえば、特定用途向け集積回路（Application Specific Integrated Circuit: ASIC）によって、1つ以上のプロセッサによって実行されるプログラム命令によって、またはその両方の組合せによって実行され得ることが認識されよう。加えて、本明細書で説明される一連（単数または複数）のアクションは、実行されると、デバイスに関連付けられたプロセッサに本明細書で説明する機能性を実行させるかまたは実行するように命令する、コンピュータ命令の対応するセットを記憶している、任意の形態の非一時的コンピュータ可読記憶媒体内で完全に具現化されると見なされ得る。した

10

20

30

40

50

がって、本開示の様々な態様は、特許請求される主題の範囲内にそのすべてが入ることが企図されている、いくつかの異なる形態で具現化され得る。加えて、本明細書で説明される態様の各々に対して、任意のこのような態様の対応する形態は、たとえば、説明されるアクションを実行する「ように構成された論理」として本明細書で説明されることがある。

【0021】

【0034】 本明細書で使用される「ユーザ機器（UE）」および「基地局」という用語は、特に明記されていない限り、具体的なものであるか、またはいずれかの特定の無線アクセス技術（Radio Access Technology：RAT）に限定することを意図していない。一般に、UEは、ワイヤレス通信ネットワークを介して通信するためにユーザによって使用される任意のワイヤレス通信デバイス（たとえば、スマートフォン、ルータ、タブレットコンピュータ、ラップトップコンピュータ、消費者のアイテム、パッケージ、アセットまたは個人やペットなどのエンティティを追跡するための消費者向け追跡デバイス、ウェアラブル（たとえば、スマートウォッチ、眼鏡、拡張現実（Augmented Reality：AR）／仮想現実（Virtual Reality：VR）ヘッドセットなど）、ビークル（たとえば、自動車、オートバイ、自転車など）、モノのインターネット（Internet of Things：IoT）デバイスなど）であり得る。UEはモバイルであってよく、（たとえば、特定のときは）静止していてもよく、無線アクセスネットワーク（Radio Access Network：RAN）と通信し得る。本明細書で使用される「UE」という用語は、「アクセス端末」つまり「AT」、「クライアントデバイス」、「ワイヤレスデバイス」、「加入者デバイス」、「加入者端末」、「加入者局」、「ユーザ端末」つまり「UT」、「モバイル端末」、「移動局」、「モバイルデバイス」、またはそれらの変形として互換的に呼ばれることがある。UEは通常、RANを介してコアネットワークと通信することができ、コアネットワークを通して、UEは、インターネットなどの外部ネットワークおよび他のUEと接続され得る。当然、ワイヤードアクセスネットワーク、（たとえば、IEEE 802.11などに基づく）ワイヤレスローカルエリアネットワーク（Wireless Local Area Network：WLAN）ネットワークなどを介した、コアネットワークおよび／またはインターネットに接続する他のメカニズムもUEにとって可能である。

【0022】

【0035】 基地局は、それが展開されているネットワークに応じてUEと通信しているいくつかのRATのうちの1つに従って動作し得、代わりに、アクセスポイント（Access Point：AP）、ネットワークノード、NodeB、進化型NodeB（evolved NodeB：eNB）、新無線（NR）ノードB（gNBとも呼ばれる）などと呼ばれることがある。加えて、いくつかのシステムでは、基地局は単にエッジノードシグナリング機能を提供し得、他のシステムでは、基地局は追加の制御および／またはネットワーク管理機能を提供し得る。それを通してUEが信号を基地局へ送信することができる通信リンクは、アップリンク（UL）チャネル（たとえば、逆方向トラフィックチャネル、逆方向制御チャネル、アクセスチャネルなど）と呼ばれる。それを通して基地局が信号をUEへ送信することができる通信リンクは、ダウンリンク（DL）チャネルまたは順方向リンクチャネル（たとえば、ページングチャネル、制御チャネル、ブロードキャストチャネル、順方向トラフィックチャネルなど）と呼ばれる。本明細書で使

【0023】

【0036】 「基地局」という用語は、単一の物理送信ポイント、または、同位置に配置されていてもいなくてもよい複数の物理送信ポイントを指すことがある。たとえば、「基地局」という用語が単一の物理送信ポイントを指す場合、その物理送信ポイントは、基地局のセルに対応する基地局のアンテナであってもよい。「基地局」という用語が複数の同位置に配置されている物理送信ポイントを指す場合、その物理送信ポイントは、基地局のアンテナのアレイであってもよい（たとえば、多入力多出力（MIMO）システムにお

るような、または基地局がビームフォーミングを採用する場合)。「基地局」という用語が複数の同位置に配置されていない物理送信ポイントを指す場合、その物理送信ポイントは、分散アンテナシステム(Distributed Antenna System: DAS)(搬送媒体を介して共通ソースに接続されている、空間的に分離されたアンテナのネットワーク)またはリモートラジオヘッド(Remote Radio Head: RRH)(サービング基地局に接続されているリモート基地局)であってもよい。代わりに、同位置に配置されていない物理送信ポイントは、UEから測定レポートを受信するサービング基地局と、その基準RF信号をUEが測定している隣接基地局であってもよい。

【0024】

【0037】 協定世界時(UTC)などの正確で信頼できる時刻の取得は、発電および配電、電気通信、交通機関、株式取引のタイムスタンプなどの現代経済の多くの重要なインフラストラクチャおよび部門、ならびに多くの他の重要なユースケースおよび重要でないユースケースにとって不可欠であり得る。たとえば、高度に正確な時刻は、全地球航法衛星システム(GNSS)信号から得られることが多い。しかしながら、GNSSは、いくつかのロケーション、たとえば、屋内では利用不可能であり得るか、または、たとえば、スプーフィングまたはジャミングに起因して故障し得る。

10

【0025】

【0038】 全地球航法衛星システム(GNSS)の障害(たとえば、スプーフィングまたはジャミング)に対するフォールバックとしてのワイヤレスネットワークによる信頼できるタイミング提供のサポートは、3GPPおよび他の規格開発機構(Standards Development Organization: SDO)において重要な領域になりつつある。GNSSタイミング障害を克服することの他にも、ワイヤレスネットワークを介したタイミング取得の使用はまた、GNSSが時々利用不可能である屋内で使用され得る。ワイヤレスネットワークを介したタイミング提供のための重要な要素は、高精度および高信頼性であり、たとえば、タイミングのスプーフィングを回避し、受信したタイミングが正しくかつ正確であるかどうかを受信者が分かるようにすることである。

20

【0026】

【0039】 本明細書で説明されるように、正確で信頼できる時刻は、少なくとも一部分が暗号化された現在時刻を含むメッセージを基地局がブロードキャストするワイヤレスネットワークを介して取得され得る。現在時刻は、たとえば、協定世界時(UTC)時刻、全地球測位システム(Global Positioning System: GPS)時刻、GLONASS時刻、Beidou時刻、Galileo時刻、全地球航法衛星システム(GNSS)時刻、またはローカル地域時刻(たとえば、米国における東部標準時(Eastern Standard Time: EST)または太平洋夏時間(Pacific Daylight Time: PDT))であり得る。受信エンティティ、たとえば、UEは、現在時刻を解釈し得る。しかしながら、ブロードキャストメッセージの伝搬時間に起因して、UEによって取得された平文の現在時刻は正確でない可能性がある。したがって、UEは、たとえば、基地局から取得されたタイミングアドバンス、UEおよび基地局の既知のロケーション、またはUEと基地局との間の実測往復伝搬時間(RTT)に基づいて、基地局とそれ自体との間の伝搬遅延を決定し得る。次いで、平文の現在時刻と伝搬遅延とに基づいて、補正済み現在時刻を決定することができる。現在時刻の信頼性は、たとえば、ブロードキャストメッセージに含まれている基地局のデジタル署名を使用して認証され得る。さらに、UEは、現在時刻を持っているメッセージが、攻撃デバイスを介さずに、たとえば、リプレイ攻撃を介さずに、基地局から直接受信したものであると判断することによって、現在時刻の信頼性をさらに検証することができる。たとえば、UEおよび基地局は、伝搬遅延を決定するためにRTT測定手順を実行し得、UEは、たとえば、実測RTTを、基地局までの予想距離に基づくRTTの予想範囲と比較することによって、リプレイ攻撃を使用する攻撃デバイスがないことを検証し得る。

30

40

【0027】

【0040】 ワイヤレスネットワークは、1つ以上のGNSSコンスタレーションから正

50

確な時刻を決定することができる基準デバイスもしくは基準ネットワーク、ワイヤレスネットワークの1つ以上の内部クロックソース（たとえば、原子時計）、または、たとえばネットワークタイムプロトコル（Network Time Protocol：NTP）を使用して時刻を提供し得る外部サーバクロックソースを含み得る、正確な現在時刻を取得するための様々な既知の技法を使用し得ることに留意されたい。

【0028】

【0041】 図1は、本明細書で説明されるような、UEによるワイヤレスネットワークを介した信頼できる時刻の取得をサポートする非ローミング5G NRネットワークに基づくアーキテクチャを示す。図1は、UE102と、次世代無線アクセスネットワーク（Next Generation Radio Access Network：NG-RAN）112を含む第5世代（Fifth Generation：5G）ネットワークの構成要素と、を備える通信システム100を示し、構成要素は、新無線（NR）NodeBまたはgNB110-1、110-2、110-3とも呼ばれる基地局（Base Station：BS）、次世代進化型NodeB（next generation evolved NodeB：ng-eNB）114、および外部クライアント130と通信している5Gコアネットワーク（5G Core Network：5GCN）150を含む。gNB110のアーキテクチャは、たとえば、gNB中央ユニット（gNB Central Unit：gNB-CU）、1つ以上のgNB分散ユニット（gNB Distributed Unit：gNB-DU）、および1つ以上のgNB遠隔ユニット（gNB Remote Unit：gNB-RU）のうちの1つ以上を含む機能部分に分割されてもよく、これらのうちのどれも、gNB110の他の部分と物理的に同位置に配置されてもよく、または物理的に分離されてもよい。5Gネットワークは、新無線（NR）ネットワークとも呼ばれ得る。NG-RAN112は、NR RANまたは5G RANと呼ばれることもあり、5GCN150は、次世代（Next Generation：NG）コアネットワーク（Next Generation（NG）Core network：NGC）と呼ばれることがある。通信システム100は、さらに、GPS、GLONASS、GalileoもしくはBeidouのような全地球航法衛星システム（GNSS）、または、IRNSS、EGNOSもしくはWAASなど、何らかの他のローカルまたは地域的衛星測位システム（Satellite Positioning System：SPS）用のスペースビークル（Space Vehicle：SV）190からの情報を利用し得る。通信システム100の追加の構成要素について、以下で説明する。通信システム100は、追加または代替の構成要素を含み得る。

【0029】

【0042】 図1は、UE102用のサービングgNB110-1と、隣接gNB110-2、110-3、およびng-eNB114とを示す。隣接gNBは、UE102のロケーション特定をサポートするために、UE102によって送信されてきたアップリンク（UL）信号を受信および測定することが可能であり、ならびに／または、UE102によって受信および測定され得るダウンリンク（DL）基準信号（Reference Signal：RS）、たとえば、測位基準信号（Positioning Reference Signal：PRS）を送信することが可能である、gNBであり得る。

【0030】

【0043】 図1は、様々な構成要素の一般化された例示のみを与え、構成要素のいずれかまたはすべてが適宜利用されてもよく、それらの各々が、必要に応じて複製され、または省略されてもよいことに留意されたい。具体的には、1つのUE102のみが図示されているが、多くのUE（たとえば、数百、数千、数百万など）が通信システム100を利用してもよいことが理解されよう。同様に、通信システム100は、より多数またはより少数のSV190、gNB110-1、110-2、外部クライアント130、および／または他の構成要素を含み得る。通信システム100の中の様々な構成要素を接続する図示の接続は、追加（中間）の構成要素、直接もしくは間接的な物理接続および／もしくはワイヤレス接続、ならびに／または追加のネットワークを含み得る、データおよびシグナリング接続を含む。さらに、構成要素は、所望の機能性に応じて、並べ替えられ、組み合わせられ、分離され、置換され、および／または省略されてもよい。

【0031】

【0044】 図1は5Gベースのネットワークを示すが、同様のネットワーク実装および構成が、3G、4Gとも呼ばれるロングタームエボリューション（LTE）、およびIEEE 802.11 Wi-Fiなどの他の通信技術に使用されてもよい。たとえば、ワイヤレスローカルエリアネットワーク（WLAN）、たとえば、IEEE 802.11無線インターフェースが使用される場合、UE102は、NG-RANではなく、アクセスネットワーク（Access Network：AN）と通信してもよく、したがって、構成要素112は、本明細書では、「RAN」、「（R）AN」、または「（R）AN 112」という用語で表され、ANまたはRANと呼ばれることがある。AN（たとえば、IEEE 802.11 AN）の場合、ANは、（たとえば、5GCN150内の）（図1に示されていない）AMF154に接続されている非3GPPインターワーキング機能（Non-3GPP Interworking Function：N3IWF）に接続され得る。

10

【0032】

【0045】 UE102は、任意の電子デバイスであり得、デバイス、モバイルデバイス、ワイヤレスデバイス、モバイル端末、端末、移動局（Mobile Station：MS）、セキュアユーザプレーンロケーション（Secure User Plane Location：SUPL）対応端末（Secure User Plane Location（SUPL）Enabled Terminal：SET）と呼ばれるか、または、何らかの他の名前と呼ばれることがある。UE102は、スタンダードデバイスであり得るか、あるいは、監視または追跡されることになっているである別のデバイス、たとえば、工場ツール内に埋め込まれ得る。その上、UE102は、スマートウォッチ、デジタルグラス、フィットネスモニタ、スマートカー、スマートアプライアンス、セルフォン、スマートフォン、ラップトップ、タブレット、PDA、消費者のアイテム、パッケージ、アセット、または個人およびペットなどのエンティティを追跡するための消費者向け追跡デバイス、制御デバイス、または何らかの他のポータブルデバイスもしくは可動デバイスに対応し得る。UE102は、単一エンティティを含んでもよく、または、たとえば、ユーザが、オーディオ、ビデオ、および／もしくはデータI/Oデバイス、ならびに／または身体センサおよび別個のワイヤラインモデムもしくはワイヤレスモデムを利用し得るような、パーソナルエリアネットワークなどにおける複数のエンティティを含んでもよい。必ずしもそうではないが、UE102は通常、GSM（登録商標）、符号分割多元接続（CDMA）、広帯域CDMA（Wideband CDMA：WCDMA（登録商標））、LTE、高レートパケットデータ（High Rate Packet Data：HRPD）、（Wi-Fiとも呼ばれる）IEEE 802.11 Wi-Fi、Bluetooth（登録商標）（BT）、世界規模相互運用マイクロ波アクセス（Worldwide Interoperability for Microwave Access：WiMAX）、5G新無線（NR）（たとえば、NG-RAN112および5GC150の使用して）などの、1つ以上の無線アクセス技術（RAT）を使用するワイヤレス通信をサポートし得る。UE102はまた、たとえば、デジタル加入者ライン（Digital Subscriber Line：DSL）またはパケットケーブルを使用して他のネットワーク（たとえば、インターネット）に接続し得るワイヤレスローカルエリアネットワーク（WLAN）を使用してワイヤレス通信をサポートし得る。これらのRATのうちの1つ以上の使用は、UE102が、（たとえば図1に示されていない5GCN150の要素を介して、または場合によってはゲートウェイモバイルロケーションセンター（Gateway Mobile Location Center：GMLC）160を介して）外部クライアント130と通信することを可能にし、および／または外部クライアント130が、（たとえば、GMLC160を介して）UE102に関するロケーション情報を受信することを可能にする。

20

30

40

【0033】

【0046】 UE102は、NG-RAN112を含み得るワイヤレス通信ネットワークとの接続状態に入り得る。一例では、UE102は、gNB110-1など、NG-RAN112中のセルラートランシーバにワイヤレス信号を送信するか、またはセルラートランシーバからワイヤレス信号を受信することによって、セルラー通信ネットワークと通信

50

し得る。トランシーバは、UE 102のほうへユーザプレーンおよび制御プレーンプロトコル終端を提供し、基地局、基地トランシーバ局、無線基地局、無線トランシーバ、無線ネットワークコントローラ、トランシーバ機能、基地局サブシステム（Base Station Subsystem：BSS）、拡張サービスセット（Extended Service Set：ESS）と呼ばれるか、または何らかの他の好適な用語で呼ばれることがある。

【0034】

【0047】 特定の実装形態では、UE 102は、ロケーション関連測定値を取得することが可能な回路構成および処理リソースを有し得る。UE 102によって取得されるロケーション関連測定値は、GPS、GLONASS、GalileoまたはBeidouなど、衛星測位システム（SPS）または全地球航法衛星システム（GNSS）に属する衛星ビークル（SV）190から受信した信号測定値を含み得、および／あるいは、（たとえば、gNBなどの）既知のロケーションに固定されている地上波送信機から受信した信号測定値を含み得る。次いで、UE 102、またはUE 102の測定値の送り先であり得るgNB 110-1は、たとえば、GNSS、支援型GNSS（Assisted GNSS：AGNSS）、アドバンスドフォワードリンクトリラレーション（Advanced Forward Link Trilateration：AFLT）、放射角度（Angle of Departure：AOD）、到着時間差（Time Difference Of Arrival：TDOA）、往復時間（RTT）、（WiFiとも呼ばれる）WLAN測位、または拡張セルID（Enhanced Cell ID：ECID）、あるいはそれらの組合せなど、いくつかの測位方法のいずれか1つを使用して、これらのロケーション関連測定値に基づいて、UE 102についてのロケーション推定値を取得し得る。これらの技法（たとえば、AGNSS、AFLT、AODおよびTDOA）のうちのいくつかでは、擬似範囲またはタイミング差が、UE 102において、パイロット、測位基準信号（PRS）、あるいは送信機または衛星によって送信され、UE 102において受信される他の測位関連信号に少なくとも部分的に基づいて、既知のロケーションにおいて固定されている3つ以上の地上波送信機（たとえばgNB）と相対的に、または正確に知られている軌道データを持っている4つ以上のSV 190と相対的に、あるいはそれらの組合せと相対的に測定され得る。

【0035】

【0048】 図1中のロケーションサーバは、たとえば、ロケーション管理機能（Location Management Function：LMF）152またはセキュアユーザプレーンロケーション（SUPL）ロケーションプラットフォーム（Secure User Plane Location（SUPL）Location Platform：SLP）162に対応し得、AGNSS、AFLT、AOD、TDOA、RTTおよびECIDなどの測位技法を容易にするために、たとえば、測定されることになっている信号に関する情報（たとえば、予想信号タイミング、信号コーディング、信号周波数、信号ドップラー）、地上波送信機（たとえばgNB）のロケーションおよび識別情報、ならびに／またはGNSS SVの信号、タイミングおよび軌道情報を含む測位支援データをUE 102に提供することができ得る。この容易化は、UE 102による信号収集および測定精度を改善することと、いくつかの場合には、UE 102がロケーション測定値に基づいてその推定ロケーションを算出することを可能にすることとを含み得る。たとえば、ロケーションサーバ（たとえばLMF 152またはSLP 162）は、特定のイベント会場などの特定の1つ以上の領域中のセルラートランシーバおよび／またはローカルトランシーバのロケーションおよび識別情報を示す、基地局アルマナック（Base Station Almanac：BSA）とも呼ばれる、アルマナックを備え得、送信電力および信号タイミングなど、セルラー基地局またはAP（たとえばgNB）によって送信される信号を記述する情報を提供し得る。UE 102は、セルラートランシーバおよび／またはローカルトランシーバから受信した信号についての信号強度（たとえば受信信号強度指示（Received Signal Strength Indication：RSSI））測定値を取得し得、ならびに／あるいは信号対雑音比（Signal to Noise ratio：S/N）、基準信号受信電力（Reference Signal Received Power：RSRP）、基準信号受信品質（Reference Signal Received Quality：RSRQ）、到着時間（Time Of

Arrival: T O A)、到着角度 (Angle Of Arrival: A O A)、放射角度 (A O D)、送受信時間差 (Receive time-Transmission time difference: R x - T x)、または U E 1 0 2 とセルラートランシーバ (たとえば g N B) もしくはローカルトランシーバ (たとえば W i F i アクセスポイント (A P)) との間の往復信号伝搬時間 (R T T) を取得し得る。U E 1 0 2 は、U E 1 0 2 についてのロケーションを決定するために、ロケーションサーバ (たとえば L M F 1 5 2 または S L P 1 6 2) から受信した、または N G - R A N 1 1 2 中の基地局 (たとえば g N B 1 1 0 - 1、1 1 0 - 2) によってブロードキャストされた支援データ (たとえば、G N S S アルマナックおよび / または G N S S エフェメリス情報などの地上アルマナックデータまたは G N S S 衛星データ) とともにこれらの測定値を用い得る。

10

【0036】

【0049】 いくつかの実装形態では、ネットワークエンティティは、U E 1 0 2 のロケーション特定を支援するために使用される。たとえば、g N B 1 1 0 - 1、1 1 0 - 2 など、ネットワーク中のエンティティは、U E 1 0 2 によって送信されてきた U L 信号を測定し得る。U L 信号は、U L 測位基準信号 (P R S) または U L サウンディング基準信号 (Sounding Reference Signal: S R S) などの U L 基準信号を含むかまたは備え得る。ロケーション測定値を取得するエンティティ (たとえば g N B 1 1 0 - 1、1 1 0 - 2) は、次いで、U E 1 0 2 または L M F 1 5 2 にロケーション測定値を転達し得、U E 1 0 2 または L M F 1 5 2 は、複数のトランシーバペアについての実時間差 (Real Time Differences: R T D) を求めるためにその測定値を用い得る。U L 信号を使用し得るロケーション測定値の例は、R S S I、R S R P、R S R Q、T O A、R x - T x、A O A および R T T を含み得る。

20

【0037】

【0050】 U E 1 0 2 のロケーションの推定値は、ロケーション、ロケーション推定値、ロケーションフィックス、フィックス、位置、位置推定値、または位置フィックスと呼ばれることもあり、地理的なものであってもよく、したがって、高度成分 (たとえば、標高、および地面、床面、または地下からの高さまたは深さ) を含むことも含まないこともある、U E 1 0 2 のロケーション座標 (たとえば、緯度および経度) を提供する。代わりに、U E 1 0 2 のロケーションは、シビックロケーションとして (たとえば、住所、または、特定の部屋もしくはフロアなどの建物の中のいくつかの地点または狭いエリアの呼称として) 表現されてもよい。

30

【0038】

【0051】 図 1 に示されているように、N G - R A N 1 1 2 中の g N B のペアは、たとえば、図 1 に示されているように、直接的に、または他の g N B 1 1 0 - 1、1 1 0 - 2 を介して間接的に、互いに接続され得る。5 G ネットワークへのアクセスは、U E 1 0 2 と、g N B 1 1 0 - 1、1 1 0 - 2 のうちの 1 つ以上との間のワイヤレス通信を介して U E 1 0 2 に提供され、g N B 1 1 0 - 1、1 1 0 - 2 は、5 G (たとえば N R) を使用する U E 1 0 2 のために 5 G C N 1 5 0 へのワイヤレス通信アクセスを提供し得る。図 1 では、U E 1 0 2 用のサービング g N B は、g N B 1 1 0 - 1 であると仮定されるが、他の g N B (たとえば、g N B 1 1 0 - 2、1 1 0 - 3、または n g - e N B 1 1 4) は、U E 1 0 2 が別のロケーションに移動する場合にサービング g N B としての機能を果たし得るか、または U E 1 0 2 に追加のスルーアウトおよび帯域幅を提供するための 2 次 g N B としての機能を果たし得る。

40

【0039】

【0052】 上記のように、図 1 は、5 G 通信プロトコルに従って通信するように構成されたノードを示すが、たとえば L T E プロトコルなど、他の通信プロトコルに従って通信するように構成されたノードも使用され得る。別のプロトコルを使用して通信するように構成されたこのようなノードは、少なくとも部分的に、5 G C N 1 5 0 によって制御され得る。したがって、N G - R A N 1 1 2 は、g N B、L T E をサポートする進化型ノード B (e N B)、あるいは他のタイプの基地局またはアクセスポイントの任意の組合せを含

50

み得る。一例として、NG-RAN112は、UE102にLTEワイヤレスアクセスを提供し、AMF154などの5GC150中のエンティティに接続し得る1つ以上のng-eNB114を含み得る。

【0040】

【0053】 gNB110-1、110-2、110-3、およびng-eNB114は、測位機能性のためにロケーション管理機能（LMF）152と通信し得る、アクセスおよびモビリティ管理機能（Access and Mobility Management Function：AMF）154と通信することができる。AMF154は、セル変更とハンドオーバーを含む、UE102のモビリティをサポートし得、UE102へのシグナリング接続をサポートすることと、場合によっては、UPF158によってサポートされるUE102用のプロトコルデータユニット（Protocol Data Unit：PDU）セッションを確立およびリリースするのを助けることとに関与し得る。AMF154の他の機能は、以下を含み得る。NG-RAN112からの制御プレーン（Control Plane：CP）インターフェースの終了、UE102などのUEからの非アクセス層（Non-Access Stratum：NAS）シグナリング接続の終了、NAS暗号化および完全性保護、登録管理、接続管理、到達可能性管理、モビリティ管理、アクセス認証および認可。

【0041】

【0054】 gNB110-1は、UE102がNG-RAN112にアクセスするとき、UE102の測位をサポートし得る。gNB110-1はまた、たとえば、GMLC160から直接または間接的に受信した、UE102についてのロケーションサービス要求を処理し得る。いくつかの実施形態では、gNB110-1を実装するノード／システムは、加えてまたは代わりに、拡張サービングモバイルロケーションセンター（Enhanced Serving Mobile Location Center：E-SMLC）またはセキュアユーザプレーンロケーション（SUP-L）ロケーションプラットフォーム（SLP）162など、他のタイプのロケーション特定サポートモジュールを実装し得る。いくつかの実施形態では、（UE102のロケーションの導出を含む）測位機能性の少なくとも一部は、（たとえば、ワイヤレスノードによって送信されてきた信号についての信号測定値と、UE102に提供される支援データとを使用して）UE102において実施され得ることに留意されたい。

【0042】

【0055】 GMLC160は、外部クライアント130から受信したUE102についてのロケーション情報要求をサポートし得、このようなロケーション情報要求をUE102用のサービングAMF154に転送し得る。AMF154は、次いで、ロケーション情報要求をgNB110-1またはLMF152のいずれかに転送し得、gNB110-1またはLMF152は、（たとえば外部クライアント130からの要求に従って）UE102についての1つ以上のロケーション推定値を取得し得、ロケーション推定値（単数または複数）をAMF154に返し得、AMF154は、GMLC160を介して外部クライアント130にロケーション推定値（単数または複数）を返し得る。GMLC160は、外部クライアント130のサブスクリプション情報を含んでいることがあり、外部クライアント130からのUE102についてのロケーション情報要求を認証および認可し得る。GMLC160は、さらに、UE102についてのロケーション情報要求をAMF154に送信することによってUE102についてのロケーションセッションを始動し得、ロケーション情報要求中に、UE102についての識別情報と、（たとえば、現在のロケーション、あるいは周期的またはトリガーされたロケーションのシーケンスなどの）要求されているロケーションのタイプとを含め得る。

【0043】

【0056】 図示のように、統合データ管理（Unified Data Management：UDM）161が、GMLC160に接続され得る。UDM161は、LTEアクセスのためのホーム加入者サーバ（Home Subscriber Server：HSS）に類似しており、必要に応じて、UDM161は、HSSと組み合わせられ得る。UDM161は、UE102に関す

るユーザ関連およびサブスクリプション関連の情報を含む中央データベースであり、以下の機能、すなわち、UE認証、UE識別、アクセス認可、登録およびモビリティ管理、サブスクリプション管理、ならびにショートメッセージサービス管理を実行し得る。

【0044】

【0057】 図1にさらに示されているように、外部クライアント130は、GMLC160および／またはSLP162を介してコアネットワーク150に接続され得る。外部クライアント130は、オプションで、インターネット175を介して、コアネットワーク150に、および／または5GCN150の外部にあるSLP164に接続され得る。外部クライアント130は、サーバ、ウェブサーバ、またはパーソナルコンピュータ、UEなどのユーザデバイスであり得る。

10

【0045】

【0058】 GMLC160およびAMF154に、ネットワーク公開機能（Network Exposure Function：NEF）163が接続され得る。いくつかの実装形態では、NEF163は、外部クライアント130またはアプリケーション機能（Application Function：AF）132と直接通信するように接続され得る。NEF163は、5GCN150およびUE102に関する能力およびイベントの、外部クライアント130またはAF132への安全な公開をサポートし得、外部クライアント130またはAF132から5GCN150への情報の安全な提供を可能にし得る。たとえば、NEF163はまた、UE102の現在または既知の最後のロケーションを取得するように機能し得、UE102のロケーションの変化の指示、またはUE102が利用可能（もしくは到達可能）になったときの指示を取得し得る。外部クライアント130またはAF132は、UE102に関するロケーション情報を取得するためにNEF163にアクセスし得る。

20

【0046】

【0059】 LMF152とgNB110-1とは、新無線測位プロトコルA（New Radio Position Protocol A：NRPPa）を使用して通信し得る。NRPPaメッセージがgNB110-1とLMF152との間で転達されることで、NRPPaは3GPP TS38.455において定義されているものであり得る。さらに、LMF152とUE102とは、3GPP TS37.355において定義されているLTE測位プロトコル（LTE Positioning Protocol：LPP）を使用して通信し得、LPPメッセージは、UE102用のサービングAMF154とサービングgNB110-1とを介してUE102とLMF152との間で転達される。LPPプロトコルは、支援型GNSS（A-GNSS）、リアルタイムキネマティック（Real Time Kinematic：RTK）、ワイヤレスローカルエリアネットワーク（WLAN）、到着角度（AOA）、到着時間差（TDOA）、往復時間（RTT）、および／または拡張セル識別情報（ECID）など、UE支援および／またはUEベースの位置特定方法を使用するUE102の測位をサポートするために使用され得る。NRPPaプロトコルは、（gNB110-1、110-2、110-3、もしくはng-eNB114によって取得されたかまたはそれらから受信した測定値とともに使用されるとき）ECIDなど、ネットワークベースの測位方法を使用してUE102の測位をサポートするために使用され得、および／または、TDOAのサポートのためのgNBからの測位基準信号（PRS）送信を定義するパラメータなど、gNB110からのロケーション関連情報を取得するためにLMF152によって使用され得る。

30

40

【0047】

【0060】 gNB110-1、110-2、110-3、またはng-eNB114は、たとえば3GPP技術仕様（Technical Specification：TS）38.413において定義されているように、次世代アプリケーションプロトコル（Next Generation Application Protocol：NGAP）を使用して、AMF154と通信し得る。NGAPは、AMF154がUE102のロケーションをUE102用のgNB110-1に要求することを可能にし得、gNB110-1がUE102についてのロケーションをAMF154に返すことを可能にし得る。

50

【0048】

【0061】 gNB 110-1、110-2、110-3、またはng-eNB 114は、たとえば3GPP TS 38.423において定義されているように、Xnアプリケーションプロトコル(Xn Application Protocol: XNAP)を使用して互いに通信し得る。XNAPは、あるgNB 110が、別のgNB 110に、UE 102についてのULロケーション測定値を取得し、ULロケーション測定値を返すことを要求することを可能にし得る。XNAPはまた、gNB 110が、別のgNB 110に、ダウンリンク(DL)RSまたはPRSを送信することを要求することを可能にして、UE 102が送信されてきたDL RSまたはPRSのDLロケーション測定値を取得することを可能にし得る。

10

【0049】

【0062】 gNB (たとえば、gNB 110-1)は、たとえば、3GPP TS 38.331において定義されているように、無線リソース制御(Radio Resource Control: RRC)プロトコルを使用してUE 102と通信し得る。RRCは、gNB (たとえばgNB 110-1)が、gNB 110-1によっておよび／あるいは他のgNB 110-2、110-3、またはng-eNB 114によって送信されてきたDL RSまたはDL PRSのロケーション測定値をUE 102に要求し、それらのロケーション測定値の一部または全部を返すことを可能にし得る。RRCはまた、gNB (たとえばgNB 110-1)が、UE 102に、UL RSまたはPRSを送信することを要求することを可能にして、gNB 110-1または他のgNB 110-2、110-3、あるいはng-eNB 114が、送信されてきたUL RSまたはPRSのULロケーション測定値を取得することを可能にし得る。

20

【0050】

【0063】 図示のように、セッション管理機能(Session Management Function: SMF) 156は、AMF 154とUPF 158とを接続する。SMF 156は、UE 102のためのPDUSセッションの確立、修正およびリリースを管理し、UE 102のためのIPアドレス割振りおよび管理を実施し、UE 102のための動的ホスト構成プロトコル(Dynamic Host Configuration Protocol: DHCP)サーバの役割を果たし、UE 102のためにUPF 158を選択し、制御し得る。

【0051】

30

【0064】 ユーザプレーン機能(User Plane Function: UPF) 158は、UE 102のための音声およびデータベアラをサポートし得、インターネット175などの他のネットワークへのUE 102の音声およびデータアクセスを可能にし得る。UPF 158の機能は、データネットワークへの相互接続の外部PDUSセッションポイント、パケット(たとえばインターネットプロトコル(Internet Protocol: IP))のルーティングおよび転送、パケットの検査およびポリシールール適用のユーザプレーン部分、ユーザプレーンのサービス品質(Quality of Service: QoS)の処理、ならびにダウンリンクパケットのバッファリングおよびダウンリンクデータ通知のトリガーを含み得る。UPF 158は、SLP 162に接続されて、オープンモバイルアライアンス(Open Mobile Alliance: OMA)に定義されているSUPLロケーションソリューションを使用してUE 102のロケーションのサポートを可能にし得る。SLP 162は、さらに、外部クライアント130に接続されるかまたは外部クライアント130からアクセス可能であり得る。

40

【0052】

【0065】 UE 102による信頼できる時刻の取得をサポートするために、gNB 110および／またはng-eNB 114のうちの1つ以上は、1つ以上のGNSSコンスタレーションに属するスペースビークル(SV)からの信号を受信し、復号し、処理することができるGNSS受信機を含み得る。たとえば、信号は、ナビゲーション信号であり得、正確な時刻(たとえば、GPS時刻またはUTC時刻)を示し得る。いくつかの他の場合には、gNB 110は、正確なGNSS時刻をgNB 110に提供することができるG

50

NSS基準ネットワークに接続され得る。さらに、gNB110（および／またはng-eNB114）は、（i）GNSS受信機を有さず、GNSS基準ネットワークに接続されていない、またはGNSS受信機を有するが、現在GNSS SVから信号を受信することができないgNB110またはng-eNB114に正確な時刻を提供することと、（ii）1つ以上のgNB110（またはng-eNB114）による時刻決定が（たとえば、外部ジャミングまたはスプーフィングに起因して）誤っている可能性があるかどうかを検出するために、時刻情報を比較することと、および／または（iii）複数のgNB110からの時刻決定を組み合わせる（たとえば、平均化する）ことによってタイミング精度を高めることと、のために、タイミング情報を交換することができ得る。加えてまたは代わりに、1つ以上のgNB110および／またはng-eNB114が、AMF154またはUPF158から（たとえば、NTPを使用して）正確なタイミング情報を受信することができる。今度は、AMF154および／またはUPF158は、同様に正確な時刻のソース（たとえば、原子時計）を含むか、またはそれに接続され得るか、あるいは何らかの外部時刻ソース（たとえば、政府機関によって所有および運営されるGNSS基準ネットワークまたはセキュアサーバ）から時刻を受信し得るUDM161またはNEF163のような何らかの他のエンティティから、正確なタイミングを受信することができる。gNB110またはng-eNB114によって取得される（たとえば、AMF154またはUPF158を介してUDM161またはNEF163から受信される）タイミング情報は、（たとえば、政府運営の原子時計ソースまたはGNSS基準ネットワークを識別することができる）時刻のソースの識別情報を含み得、精度のレベルを示すことができる（たとえば、時刻が1マイクロ秒、1ミリ秒（ms）、または1秒まで正確であることを示すことができる）。gNB110もしくはng-eNB114による正確な現在時刻の決定、またはgNB110もしくはng-eNB114への正確な現在時刻の提供は、本明細書で説明されるように、gNBまたはng-eNBが正確な時刻をUE102に提供することを可能にし得る。

10

20

【0053】

【0066】 図1は、非ローミングUEのためのネットワークアーキテクチャを示すが、好適な周知の変更がなされた対応するネットワークアーキテクチャがローミングUEのために提供され得ることを理解されたい。

【0054】

30

【0067】 上記で説明したように、正確で信頼できる時刻の取得は、現代経済の多くの重要なインフラストラクチャおよびセクタ、ならびに多くの他の重要なユースケースおよび重要でないユースケースにとって不可欠であり得る。たとえば、非常に正確な時刻が、SV190からのGNSS信号から、UE102などのUEによって受信され得る。しかしながら、いくつかの状況では、SV190からの信号は、屋内またはアーバンキャニオンロケーションなどでは利用不可能であり得る。加えて、SV190からの信号は、スプーフィングまたはジャミングなどの攻撃に起因して利用不可能であり得る。

【0055】

【0068】 現在時刻は、ワイヤレスシステム100を介してUE102によって取得されてもよい。たとえば、gNB110は、UE102によって受信され得、現在時刻を含み得るメッセージをブロードキャストし得る。gNB110は、たとえば、前に説明したように、SV190からの信号から、またはコアネットワーク150内のAMF154もしくはUPF158などのエンティティからの信号から、現在時刻を取得することができる。例として、現在時刻は、UTC時刻、GPS時刻、GLONASS時刻、Beidou時刻、Galileo時刻、GNSS時刻、またはローカル時刻（たとえば、ESTまたはPDT）であり得る。gNB110は、1つ以上のメッセージにおいて、たとえば、システム情報ブロック（System Information Block：SIB）において、現在時刻をUE102に周期的に提供することができる。

40

【0056】

【0069】 図2Aは、例として、gNB110からのメッセージにおいてブロードキャ

50

ストされ得る現在時刻 200 のフォーマットを示す。現在時刻 200 は、UTC 時刻、GPS 時刻、GLONASS 時刻、Beidou 時刻、Galileo 時刻、GNSS 時刻、またはローカル時刻（たとえば、EST または PDT）などであり得る。現在時刻 200 は、ISO 8601 または任意の他の所望のフォーマットに従って表され得る。図 2 A に示すように、UTC 時刻の場合、現在時刻 200 は、年 (yyyy)、月 (MM)、週 (ww)、日 (D)、時 (hh)、分 (mm)、秒 (ss)、および秒の端数 (f...) を含み得る。秒の端数 (f...) は、小数であってもよく、必要なだけの小数位を含んでもよい。UTC 時刻は、周知のように、秒 (ss) フィールドに対して、それぞれ、「60」値を含めるか、または「59」値を省略することによって、うるう秒の加算または減算に対応することができる。当然、必要に応じて、たとえば、週は含めず、日は 2 桁 (DD) で表すなど、他のフォーマットを使用してもよい。GPS 時刻、Galileo 時刻、または Beidou 時刻の場合、時刻は、何らかの開始時刻（たとえば、GPS の場合、1980 年 1 月 5 日から 6 日の UTC 00:00（真夜中））から経過した秒数として表され得る。さらに、場合によっては、現在時刻 200 は、以前に提供された時刻からの時間間隔として提供されることもある。

10

【0057】

【0070】 gNB 110 によってブロードキャストされたタイミング情報は、完全に暗号化され得るか、またはタイミング情報の一部分が暗号化され得る。暗号化された時刻を受信するサブスクリプションを有する UE 102 は、gNB 110 から、または 5GCN 150 内のエンティティ（たとえば、AMF 154）から暗号化鍵を受信することができ、暗号化鍵は、たとえば、UE 102 が 5GCN 150 への登録を実行するとき（たとえば、AMF 154 によって）提供され得る。UE 102 は、暗号化鍵を使用して、暗号化されたタイミング情報または暗号化されたタイミング情報の一部分を解読し得る。暗号化は、アメリカ国立標準技術研究所 (United States National Institute of Standards and Technology: NIST) によって定義される高度暗号化標準 (Advanced Encryption Standard: AES) アルゴリズムのうちの 1 つなどの任意の暗号化アルゴリズムを使用してもよい。たとえば、一実施形態では、AES カウンタモードアルゴリズムを使用することができる。この場合、異なるカウンタが、現在時刻を搬送する各ブロードキャストメッセージ（または SIB）において使用され得る。ブロードキャストメッセージ中の暗号化されたビットの数が、暗号鍵中のビットの数よりも少ないことがあるので（たとえば、図 2 C および図 2 D について以下で説明する変形形態の場合）、場合によっては、（たとえば、AES カウンタモードの場合）共通暗号文ストリームを使用して連続ブロードキャストメッセージ（または連続ブロードキャストメッセージの部分）を暗号化し、各ブロードキャストメッセージに使用されている暗号文ストリームの部分を示すことが、より容易、より便利、またはより安全であり得る。

20

30

【0058】

【0071】 gNB 110 による暗号化は、たとえば、非常に正確なタイミング情報のサブスクリプションベースのサービスを可能にし、タイミング情報の信頼性を保証することを支援することができる。いくつかの実装形態では、下位ビットまたはフィールドのみが暗号化され得、これは、暗号化鍵を有さない UE 102 が近似時刻（たとえば、小数秒のみが暗号化される場合、1 秒までの正確さの時刻）を取得することを可能にし、一方、暗号化鍵を有する UE 102 は、より正確な時刻（たとえば、1 μ s までの正確さの時刻）を取得することができる。

40

【0059】

【0072】 図 2 B、図 2 C、および図 2 D は、例として、gNB 110 からのメッセージ内でブロードキャストされる現在の UTC 時刻 200 のフォーマットを示し、陰影は、現在時刻 200 の暗号化された部分を表す。図 2 B に示すように、現在時刻 200 のすべてが暗号化され得る。一方で、図 2 C において陰影で示されるように、秒の端数のみが暗号化され得、これは、任意の UE 102 が 1 秒の精度で現在時刻を取得することを可能にするが、暗号化鍵を有する UE 102 は、より正確な時刻を取得し得る。図 2 D は、たと

50

例えば、10分の1、100分の1、1000分の10000分の1などの秒の端数の個々の単位を示す現在時刻200の拡張フォーマットを示し、いくつかの端数（たとえば、10分の1および100分の1）が暗号化され得ず、より低い位（たとえば、1000分の1以下）が暗号化され得ることを陰影で示す。

【0060】

【0073】 図2Eは、UE102にブロードキャストされるメッセージ（たとえば、SIB）中に現在時刻とともにgNB110によって含められ得る追加情報を示す。情報は、現在時刻（たとえば、図2A～図2DのいずれかにおけるようなUTC）、gNB110におけるローカル送信時刻（以下で説明するように、これは、現在時刻をより正確に示すために使用され得、メッセージ送信がgNB110のローカル送信時刻フレームおよび／またはサブフレーム構造に関連付けられているか、またはその一部である場合、その包含または指示は暗黙的であり得る）、現在時刻のソース（たとえば、GPS、Galileo、GLONASS、Beidou、GNSS、ローカル原子時計、原子時計を備えている外部サーバ、GNSS基準ネットワーク、gNB110のローカル時計）、および／または現在時刻の精度もしくは不確実性（たとえば、1秒、1ms、または1μs）、場合によっては、デジタル署名（Digital Signature: DigSig）を含むことができる。デジタル署名（DigSig）の目的は、UE102によって受信される現在時刻の信頼性を改善することであり得、信頼性は、特にクリティカルユースケースの場合、重要な考慮事項であり得る。現在時刻情報をより信頼できるものにするために、ワイヤレスネットワーク（たとえば、5GCN150）に接続されているUE102はまず、既存の（たとえば、3GPP）セキュリティメカニズムを使用してワイヤレスネットワークを認証し、ワイヤレスネットワークへの（たとえば、サービングgNB110-1および／またはサービングAMF154への）安全な（たとえば、暗号化された）接続を確立することができる。次いで、ネットワークエンティティ（たとえば、サービングAMF154またはサービングgNB110-1）が、1つのgNB110（たとえば、サービングgNB110-1）またはgNB110の多くもしくはすべてに適用可能な公開暗号化鍵（公開鍵とも呼ばれる）をUE102に提供することができる。次いで、gNB110が、（たとえば、SIBメッセージ中で）現在時刻をブロードキャストし、ネットワークのみに知られている（秘密鍵（private key）とも呼ばれる）対応する秘密暗号化鍵に基づいて現在時刻を認証するために、デジタル署名（DigSig）を含めることができる。認証は、余分なシグナリングおよび処理を低減するために、低頻度でのみ（たとえば、毎分または5分ごとに1回DigSigを含めることによって）実行されてもよい。デジタル署名が公開鍵を使用してUE102によって認証された場合、UE102は、受信した現在時刻を信頼することができる。ネットワークおよびUEは、RSAアルゴリズムまたはデジタル許可基準型アルゴリズム（Digital Signature Algorithm: DSA）に基づくものなど、デジタル署名の任意の標準化されたタイプを使用することができる。

【0061】

【0074】 上記のようにデジタル署名を使用する公開鍵－秘密鍵形式の認証は、（図2B～図2Dに示されるような）現在時刻の全部または一部の暗号化に基づく認証よりも信頼性が高い可能性があることに留意されたい。これは、暗号化が、通常、攻撃デバイスによって（たとえば、ワイヤレスネットワークから、またはUE102から）容易に取得され得る、gNB110とUE102の両方に知られている単一の暗号化鍵に基づくからである。しかしながら、公開鍵と秘密鍵とのペアでは、秘密鍵はUE102に開示されず、ワイヤレスネットワーク内でのみ知ることができる。

【0062】

【0075】 図3Aは、gNB110およびUE102を含むワイヤレスネットワークにおける信頼できる時刻のブロードキャストおよび取得のためのシグナリングフロー300を示し、縦軸は（時刻が下向きに進む）時刻を表し、横軸はエンティティ間の距離を表す。図3Aは、非限定的な例として与えられるものである。たとえば、図3Aは、5Gネットワークエンティティ、すなわち、gNB110またはng-eNB114の使用を示す

が、必要に応じて、eNBがgNB110の代わりに使用され得るLTEネットワークなど、他のタイプのネットワークが使用され得る。加えて、追加のシグナリングおよびプロセスが存在し得ること、およびgNB110によって送信されるメッセージが追加の構成要素を含み得ることが理解されよう。

【0063】

【0076】 図示のように、現在時刻Tまたはそれに近い（その $1\mu s$ または $1ms$ 以内の）時刻において、gNB110は、時刻 $T+\Delta$ においてUE102によって受信されるメッセージ302をブロードキャストする。メッセージ302は、システム情報ブロック（SIB）中に含まれ得、現在時刻Tを含み、gNB110における関連付けられたローカル送信時刻 t の暗黙的または明示的な指示（たとえば、次のサブフレームの開始または現在のサブフレームの終了など）を含み得る。関連付けは、ローカル時刻が正確に t であるとき、現在時刻が正確にTであるというものであり得る。暗黙のローカル時刻 t は、（たとえば）3GPP TSにおいて定義されているものであり得、メッセージ302に明示的に含まれていないことがある。ローカル時刻 t は、現在時刻Tのより正確な伝達を可能にすることができ、必ずしもgNB110が正確に時刻Tにおいてメッセージ302をブロードキャストすることを必要としない。ローカル時刻 t がなければ、gNB110は、時刻Tにおいて、または可能な限り時刻Tの近い時刻において、メッセージ302をブロードキャストする必要がある得、UE102は、メッセージ302の到着をタイムスタンプする必要がある得。現在時刻Tは、たとえば、UTC時刻、GPS時刻、GLONASS時刻、Beidou時刻、Galileo時刻、GNSS時刻またはローカル地域時刻（たとえば、ESTまたはPDT）であり得る。たとえば、gNB110は、前に説明したように、現在時刻Tを取得することができ、たとえば、SV190または図1に示すAMF154などの別のネットワークエンティティからTを周期的に取得することができ、SV190または他のネットワークエンティティからの更新の間の短い期間にローカルクロックを使用して時刻Tを維持することができる。ローカルクロックは、たとえば、NG-RAN112内のgNB110のローカル送信時刻 t を維持することもできる。上記で説明したように、現在時刻Tの少なくとも一部分は、図2B～図2Dについて説明したように、gNB110によって暗号化され得る。

【0064】

【0077】 いくつかの実装形態では、メッセージ302は、たとえば図2Eについて説明したように、追加情報を含み得る。一例では、メッセージ302は、gNB110によって送信されてきたサブフレーム境界またはスロット境界との現在時刻Tのアライメント（または関連付け）を示し得る（たとえば、上記のような）ローカル時刻 t を含むかまたは参照し得る。一例では、メッセージ302は、現在時刻Tの不確実性を含み得る。一例では、メッセージ302は、現在時刻Tのソース、たとえば、現在時刻TがSVまたはネットワークエンティティから取得されたかどうか、および現在時刻がUTC時刻、GPS時刻、GLONASS時刻、Beidou時刻、Galileo時刻、GNSS時刻などであるかどうかを含み得る。メッセージ302は、さらなる追加情報（たとえば、図2Eについて説明したデジタル署名）および／または上記の任意の組合せを含み得る。

【0065】

【0078】 現在時刻Tを持っているブロードキャストメッセージ302が、gNB110から信号伝搬遅延 Δ 後にUE102に到着するので、時刻 $T+\Delta$ においてUE102によって取得されたメッセージ302内の現在時刻Tは、いくつかのユースケースの場合十分に正確でない可能性がある。これは、メッセージ302が暗黙的または明示的なローカル時刻 t を含むか否かにかかわらず適用され得る。ローカル時刻 t が（暗黙的または明示的に）含まれていないとき、UE102は、現在時刻Tが、 $T+\Delta$ におけるメッセージ302の受信時刻（たとえば、メッセージ302の開始またはメッセージ302の終了の受信時刻）に当たると仮定するだけでよい。したがって、 Δ に等しい誤差を有し得る。ローカル時刻 t が（暗黙的にまたは明示的に）含まれているかまたは示されているとき、UE102は、現在または次のサブフレームまたはスロットの開始または終了など、gNB1

10から受信した特定の送信時刻 t に現在時刻 T を関連付け得る。この関連付けは、通常、 $gNB110$ での送信に対して正しいが、ローカル送信時刻 t 指示（たとえば、サブフレームまたはスロットの開始または終了）が $UE102$ に到着したとき、時間 Δ だけ遅延される。これは再び Δ の誤差を引き起こす。

【0066】

【0079】したがって、非常に正確な現在時刻 T の提供は、 $UE102$ がそれ自身と $gNB110$ との間の伝搬遅延 Δ を決定する能力を必要とし得る。伝搬遅延 Δ の情報を用いて、 $UE102$ は、ブロードキャストメッセージ302の $UE102$ による受信時刻、または暗黙的もしくは明示的なローカル時刻 t の $UE102$ による受信時刻のいずれかにおいて、受信した現在時刻 T に伝搬遅延 Δ を加算して、正しい現在時刻 $T + \Delta$ を取得し得る。

【0067】

【0080】 $UE102$ は、様々な方法で、ブロードキャスト $gNB110$ とそれ自体との間の伝搬遅延 Δ を決定し得る。たとえば、 $UE102$ は、NR無線インターフェースの無線リソース制御（RRC）プロトコルまたは媒体アクセス制御（Medium Access Control: MAC）プロトコルのメッセージなど、別のメッセージ（図3Aに図示せず）中で $gNB110$ からタイミングアドバンス（Timing Advance: TA）を取得し得る。TAは、 $UE102$ による $gNB110$ への送信が、 $gNB110$ から受信した送信タイミングより先行するべき時間間隔を示し得る。たとえば、 $UE102$ がローカルUE時刻 $T1$ において $gNB110$ から新しいサブフレームの開始を受信した場合、 $UE102$ は、 $UE102$ がローカルUE時刻 $T1 - TA$ において $gNB110$ に向けて新しいサブフレームの開始を送信するように、 $gNB110$ に向けた送信タイミングをサポートし得る。TA値は、各 $UE102$ に対して個別であり得、すべてのサポートされる $UE102$ からの送信が $gNB110$ によって同期された方式で受信される（たとえば、 $gNB110$ が、すべてのサポートされる $UE102$ から新しいサブフレームの開始を同時に受信する）ことを確実にするために $gNB110$ によって使用され得る。場合によっては、 $gNB110$ における異なる $UE102$ からの送信の到着時刻を同期させるための使用に影響を及ぼすことなく、すべての $UE102$ によってタイミングアドバンスオフセットがTA値に加算され得る。（周知のように）通常、TA値は、 $UE102$ と $gNB110$ との間の往復信号伝搬時間（RTT）に等しい。よって、一方向伝搬遅延は、TA値の半分として取得され得る（したがって、 $\Delta = TA / 2$ ）。タイミングアドバンスを使用することの制限は、 $UE102$ が通常、RRC CONNECTED状態にあり、 $gNB110$ へのRRCシグナリング接続を有する必要があることである。したがって、タイミングアドバンスの使用は、 $gNB110$ から現在時刻 T を受信するRRC IDLE状態またはRRC INACTIVE状態にある $UE102$ には適しない可能性がある。

【0068】

【0081】別の実装形態では、 $UE102$ は、既知の測位技法を使用して、 $gNB110$ までの範囲、たとえば距離を決定することができ、その範囲を、ワイヤレス信号の速度に基づいて伝搬遅延 Δ に変換することができる（ $\Delta = \text{範囲} / c$ 、ここで、 c は光速とする）。

【0069】

【0082】たとえば、いくつかの実装形態では、 $UE102$ は、たとえば、UEベースの測位技法において、A-GNSS、Wi-Fi、DL-TDOA、DL-AOD、マルチセルRTT、ECIDなど、既知の測位技法を使用して、ロケーションサーバ（たとえば、LMF152またはSLP162）との測位セッションにおいてそのロケーションを取得し得、ブロードキャスト $gNB110$ のロケーションを取得し得る。 $UE102$ は、 $UE102$ のロケーションと $gNB110$ のロケーションとの間の距離に基づいて、 $gNB110$ までの範囲を決定し得る。いくつかの実装形態では、 $gNB110$ のロケーションは、 $gNB110$ のロケーションを含む $gNB110$ からのブロードキャストSIBメッセージから、または測位セッション中に $gNB110$ を介してロケーションサーバ（た

例えば、LMF152またはSLP162)から受信したgNB110のロケーションを含むLPP支援データメッセージから、UE102によって取得され得る。UE102のロケーションは、モバイル発信ロケーション情報要求(Mobile Originated Location Request: MO-LR)に応答して、たとえば、UE支援測位技法において、A-GNSS、Wi-Fi、DL-TDOA、DL-AOD、マルチセルRTT、ECIDなどの既知の測位技法を使用して、ロケーションサーバ、たとえば、LMF152またはSLP162によって決定され得、ロケーションサーバは、次いで、MO-LR応答メッセージ中でロケーションをUE102に送り得る。UE102のロケーションはまた、UEベースのまたはスタンドアロンの測位技法において、GNSS、A-GNSS、Wi-Fi、DL-TDOA、DL-AOD、マルチセルRTT、ECIDなど、既知の測位技法を使用して、ロケーションサーバとやり取りすることなしにUE102によって決定され得る。

10

【0070】

【0083】別の例では、UE102は、UE102とgNB110との間の往復伝搬時間(RTT)に基づいて、gNB110までの範囲を決定し得る(たとえば、伝搬遅延 Δ は、RTTの半分である)。RTTは、したがって、伝搬遅延 Δ は、たとえば、ランダムアクセスチャネル(Random Access Channel: RACH)を使用して測定され得る。高精度現在時刻Tのサブスクリプションを持っているUEのみにRACH手順を制限するために、gNB RACH応答メッセージの暗号化は、高精度現在時刻のサブスクリプションを持っているUEのみに知られている暗号化鍵を使用して実行され得る。たとえば、図2B~図2Dのように現在時刻の一部または全部を暗号化するためと、gNB RACH応答メッセージの一部または全部を暗号化するためとの両方に、同じ暗号化鍵が使用され得る。これは、RTT決定をサポートするためにgNB110にかかる負荷を制限し得る。

20

【0071】

【0084】図3Bは、図3Aと同様であり、gNB110とUE102との間の伝搬遅延 Δ を決定するためのRTT手順を含む、ワイヤレスネットワークにおける信頼できる時刻のブロードキャストおよび取得のためのシグナリングフロー350を示す。図3Bは、非限定的な例として与えられるものである。たとえば、追加のシグナリングおよびプロセスが存在し得ること、ならびにgNB110とUE102との間で送信されるメッセージが追加の構成要素を含み得ることが理解されよう。図3Bに示される手順の利点は、それが、タイミングアドバンスが利用可能でない可能性があるRRC IDLEまたはRRC INACTIVE状態にあるUE102によって使用され得ることである。

30

【0072】

【0085】図示のように、図3Aに示されるメッセージ302と同様に、現在時刻Tまたはそれに近い時刻において、gNB110は、時刻 $T + \Delta$ においてUE102によって受信されるメッセージ352をブロードキャストする。メッセージ352は、図3Aのメッセージ302と同じまたは同様であり得る。したがって、メッセージ352はSIB中に含められ得、現在時刻Tの少なくとも一部分は暗号化され得、メッセージ352は、gNB110における暗黙的または明示的なローカルNR送信時刻 t 、基地局サブフレームまたはスロット境界への現在時刻Tのアライメントの暗黙的または明示的な指示、現在時刻Tの不確実性、現在時刻Tのソース、またはそれらの組合せなどの追加情報を含み得る。UE102は、以前に取得された暗号化鍵に基づいて、現在時刻T、および暗号化される場合には追加情報を解読して、平文の現在時刻T(および平文の追加情報)を取得することができる。

40

【0073】

【0086】gNB110は、gNB110において、ローカル時刻 t においてUE102にメッセージまたは信号354を送信することができる。メッセージまたは信号354は、たとえば、同期信号ブロック(Synchronization Signal Block: SSB)またはチャネル状態情報基準信号(Channel State Information Reference Signal: CSI-RS)であり得る。メッセージまたは信号354は、送信のローカル時刻 t を含

50

み得るか、またはそれを示し得る。UE 102は、受信したローカル送信時刻 t と、メッセージまたは信号354のUE 102におけるローカル受信時刻とに基づいて、UEにおけるローカルタイミング、たとえば、UE 102の内部タイミングソースまたは内部クロックを、gNB 110のローカル送信時刻に関連付け得る。

【0074】

【0087】メッセージまたは信号354に回答して、UE 102は、たとえば、RACH要求メッセージであるRRCメッセージであり得るメッセージ356をgNB 110に送り得る。メッセージ356は、gNB 110用のRACH上でUE 102によって送信され得る。UE 102は、メッセージ356中に、ランダム変数(Random Variable: RV)、たとえば、8~16ビットを含むランダムビット列を含め得る。メッセージ356は、UEのローカル時刻またはgNB 110の関連付けられたローカル送信時刻のいずれか一方であり得る、(たとえば、メッセージ356の開始または終了の送信の時刻に対応し得る)第1の時刻に送信される。メッセージ356は、第2の時刻、たとえば、ローカル時刻 $t + 2\Delta$ においてgNB 110によって受信される。図3Bは、UE 102におけるメッセージまたは信号354の受信時に発生するものとして第1の時刻を示しており、したがって、第1の時刻は、メッセージまたは信号354に含まれているか、またはそれによって示されているローカル時刻 t に対応することに留意されたい。しかしながら、第1の時刻が、メッセージまたは信号354のUE 102への到着の直後(たとえば、1~100ms後)に発生することも可能であり、この場合、第1の時刻は、UE 102によって知られており、かつ t を超えているgNB 110の何らかのローカル送信時刻に対応することができる。

【0075】

【0088】gNB 110は、メッセージ356の到着時刻(たとえば、メッセージ356の開始または終了の到着時刻)を取得し(たとえば、測定し)、メッセージ356に回答して応答メッセージ358をUE 102に返す。応答メッセージ358は、たとえば、gNB 110用の共通制御チャネル(Common Control Channel: CCH)上で送信されるRRCメッセージであり得る。上記で説明したように、RACH手順を高精度現在時刻 T のサブスクリプションを持っているUEのみに制限するために、応答メッセージ358は、高精度現在時刻のサブスクリプションを持っているUEのみに知られている暗号化鍵を使用して暗号化され得る。したがって、UE 102は、暗号化される場合、応答メッセージ358の一部または全部を解読し得る。応答メッセージ358は、メッセージ356からのランダム変数(RV)を含み、第2の時刻、たとえば、gNB 110におけるメッセージ356の受信のローカル時刻(この例では $t + 2\Delta$)を含み得る。同じメッセージの時刻が、メッセージの同じ部分、たとえばメッセージの開始または終了に当たるように、送信時刻および受信時刻は、本明細書で説明されるすべての手順において一貫して測定される必要があることに留意されたい。したがって、ここで説明される第1および第2の時刻は、両方ともメッセージ356の開始に当たり得、または両方ともメッセージ356の終了に当たり得る。

【0076】

【0089】UE 102は、応答メッセージ358を受信し、ランダム変数(RV)を認識する。次いで、UE 102は、第1の時刻(たとえば、 t の既知の値)と応答メッセージ358から取得された第2の時刻(たとえば、この例では $t + 2\Delta$)とに基づいて、伝搬遅延 Δ を取得することができる。伝搬遅延 Δ の情報をを用いて、UE 102は、ブロードキャストメッセージ352の受信時刻、またはメッセージ352に暗黙的または明示的に含まれているか、または示されている場合には関連付けられたローカル時刻 t のいずれかにおいて、メッセージ352中で受信した現在時刻 T に伝搬遅延 Δ を加算して、正しい現在時刻 $T + \Delta$ を取得し得る。メッセージ354、356、および358によって示されるRTT手順(ならびにUE 102のロケーションを決定するための任意の測位手順)は、必ずしもメッセージ352の受信後に行われるとは限らないことを理解されたい。たとえば、伝搬遅延 Δ を取得するためにRTT手順(または測位手順)が実行されるが、これは

現在時刻 T の受信の前に行われてもよく後に行われてもよい。さらに、 RTT 手順（または測位手順）は、 $UE102$ が移動していないか、またはゆっくりと移動している場合、必ずしも現在時刻 T の受信に時間的に近接して実行される必要はない。

【0077】

【0090】 $UE102$ が応答メッセージ 358 を（たとえば、メッセージ 356 を送信した後に何らかの最大予想応答時間が経過しても）受信していない場合、 $UE102$ は、後の時刻 t' にメッセージ 356（図 3B に図示せず）を再送信し、応答メッセージ 358 と同様の応答メッセージ（図 3B に図示せず）を受信するのを待つことができる。これは、たとえば、干渉に起因して、またはメッセージ 356 の送信用の $UE102$ からの送信電力が低すぎることに起因して、 $gNB110$ がメッセージ 356 を正しく受信していない場合に発生し得る。メッセージ 356 の再送信について、 $gNB110$ が応答メッセージ 358 と同様の応答メッセージを送信すると仮定すると、 $UE102$ は、時刻 t の代わりに時刻 t' を用いて、上記のように伝搬遅延 Δ を得ることができる。

【0078】

【0091】 $UE102$ によって受信された現在時刻 T の信頼性は、特にクリティカルユースケースの場合、重要な考慮事項であり得る。現在時刻情報を信頼できるものにするために、ワイヤレスネットワークに接続されている $UE102$ はまず、既存のセキュリティメカニズムを使用してワイヤレスネットワークを認証し得る。次いで、ネットワークエンティティ（たとえば、 $AMF154$ または $gNB110$ ）は、1つの $gNB110$ （たとえば、サービング $gNB110-1$ ）または $gNB110$ の多くもしくはすべてに適用可能な公開暗号化鍵を $UE102$ に提供することができる。次いで、 $gNB110$ は、たとえば、 SIB メッセージ 302 または 352 中で現在時刻 T をブロードキャストし、ネットワークのみに知られている対応する秘密鍵に基づいて現在時刻 T を認証するためのデジタル署名（ $DigSig$ ）を含めることができる。認証は、余分なシグナリングおよび処理を低減するために、低頻度でのみ（たとえば、毎分または 5 分ごとに 1 回）実行されてもよい。 $UE102$ は、デジタル署名が公開鍵を使用して認証された場合、受信した現在時刻 T を信頼することができる。

【0079】

【0092】 したがって、現在時刻 T とともに含められるデジタル署名の使用は、現在時刻 T の信頼性を向上させ得る。含まれている現在時刻 T が $gNB110$ によってまだ送信されていない将来の時刻である場合、攻撃エンティティは、攻撃エンティティによって $UE102$ に向けて送信される、メッセージ 302 またはメッセージ 352 と同様のメッセージに正しいデジタル署名を含めることができないので、デジタル署名は、たとえば、リプレイ攻撃を除く、何らかの攻撃エンティティによる現在時刻 T のスプーフィングを防止することができる。しかしながら、リプレイ攻撃では、攻撃エンティティは、 $gNB110$ からブロードキャストされた現在時刻 T を取得し、後の（遅延後の）時刻において現在時刻 T およびデジタル署名を $UE102$ に再送信し、それによって、正しい現在時刻よりも以前の $UE102$ 内の不正確な時刻を誘発し得る。例として、図 1 では、攻撃デバイス 108 は、 $gNB110-1$ から（デジタル署名などとともに）現在時刻 T を含むブロードキャストメッセージを受信し得、リプレイ攻撃中にメッセージを $UE102$ に送り得る。デジタル署名はリプレイされるメッセージに含まれているため、デジタル署名だけではリプレイ攻撃を検出することができない。したがって、 $UE102$ が攻撃デバイス 108 からリプレイされたメッセージを受信すると、 $UE102$ は、現在時刻が $T + \Delta$ であると信じ得る。実際には、遅延のために現在時刻がもっと後の時刻であり得る。

【0080】

【0093】 図 4A は、図 3A と同様であり、攻撃デバイス 108 が存在し、リプレイ攻撃を実行している、 $gNB110$ および $UE102$ を含むワイヤレスネットワークにおける信頼できる時刻のブロードキャストおよび取得のためのシグナリングフロー 400 を示す。

【0081】

[0094] 図示のように、現在時刻 T またはそれに近い（その $1\ \mu\text{s}$ または 1ms 以内の）時刻において、 $gNB110$ は、時刻 $T + \Delta$ において、またはそれに近い時刻において、 $UE102$ によって受信されるメッセージ 402 をブロードキャストする。メッセージ 402 は、図 3A および図 3B について説明したメッセージ 302 および 352 と同じまたは同様であり得る。したがって、メッセージ 402 は、 SIB メッセージであり得、現在時刻 T 、オプションの暗黙的または明示的なローカル時刻 t 、およびデジタル署名（ $DigSig$ ）を含み得る。メッセージ 402 は、基地局サブフレームまたはスロット境界への現在時刻 T のアライメント、現在時刻の不確実性、現在時刻のソース、またはそれらの組合せをさらに含むか、または示し得る。攻撃デバイス 108 は、メッセージ 402 を受信し得、遅延 $\Delta 1$ 後、リプレイ攻撃中に、時刻 $T + \Delta + \Delta 1$ において $UE102$ によって受信されるメッセージ 403 を送り得る。遅延 Δ は、 $gNB110$ から攻撃デバイス 108 への伝搬時間と攻撃デバイス 108 から $UE102$ への伝搬時間との合計を含むことができる。遅延 $\Delta 1$ は、攻撃デバイス 108 におけるメッセージ 402 の受信（たとえば、開始）とメッセージ 403 の送信（たとえば、開始）との間の遅延を含むことができる。メッセージ 403 は、メッセージ 402 のコピーであり得、したがって、（ $gNB110$ によって少なくとも部分的に暗号化され得る）現在時刻 T 、ならびに $gNB110$ 用のデジタル署名（ $DigSig$ ）を含み得る。 $UE102$ は、現在時刻の少なくとも一部分を解読して、平文の現在時刻を取得し得る。

10

[0082]

[0095] $UE102$ による攻撃デバイス 108 の検出がない場合、 $UE102$ は、メッセージ 403 中で受信した現在時刻 T に不適切に依存する可能性があり、この現在時刻は少なくとも $\Delta 1$ の誤差を有する可能性がある。したがって、 $UE102$ にとって、現在時刻 T を持っているメッセージが、たとえば、リプレイ攻撃中に、攻撃デバイス 108 を介して受信したのではなく、 $gNB110$ から直接受信したと判定することによって、現在時刻 T の信頼性を検証することが望ましい場合がある。

20

[0083]

[0096] 現在時刻 T の信頼性の検証は、 $UE102$ と $gNB110$ との間の伝搬遅延が予想範囲内にあるか、または予想値に等しいことを周期的に検証することによって、 $UE102$ によって実行され得る。 $UE102$ が $RRC\ CONNECTED$ 状態にある場合、 $UE102$ は、 $gNB110$ からタイミングアドバンス（ TA ）を周期的に受信することができ、これは、前に説明したように、（ TA の半分として）伝搬遅延を決定するために使用され得る。 $gNB110$ と $RRC\ CONNECTED$ にある $UE102$ との間の通信は、攻撃デバイス 108 が解読または修正することが不可能な（または非常に困難な）方法で暗号化され得るので、攻撃デバイス 108 は、タイミングアドバンスを偽造またはスプーフすることが不可能であり得、よって、リプレイ攻撃が実行される場合、 $UE102$ は、タイミングアドバンスを受信し得、次いで、 $UE102$ は、攻撃デバイス 108 が存在し得るかどうかを判定するために、以下でさらに説明されるようにタイミングアドバンスを処理することができる。

30

[0084]

[0097] しかしながら、 $UE102$ が $RRC\ IDLE$ または $RRC\ INACTIVE$ 状態にある場合、 $UE102$ は、 $gNB110$ からタイミングアドバンスを受信していない可能性があり、図 3B について説明したものと同様の手順を使用して $gNB110$ との伝搬遅延を測定する必要があるが、攻撃デバイス 108 が存在するときにその検出を可能にするためにいくつかの追加が加えられる。次いで、 $UE102$ は、図 3B に示されるものと同様に、 $RACH$ 手順を使用して、 $gNB110$ から $UE102$ への伝搬遅延 Δ を周期的に取得することができる。攻撃デバイス 108 が $RACH$ 手順をブロックするか、または不正の $RACH$ 応答を返す場合、 $UE102$ は、これを検出し（たとえば、デジタル署名または $RACH$ 応答の欠如を使用して）、攻撃デバイス 108 の存在を判定することができる。たとえば、 $gNB110$ は、 $RACH$ 応答メッセージをも、現在時刻を持っているブロードキャストメッセージをも、デジタル署名する、すなわちデジタル署

40

50

名 (D i g S i g) を含めることができる。したがって、効果的な攻撃のために、攻撃デバイス 108 は、中間者としての役割を果たすことによって R A C H 手順を可能にする必要がある。攻撃デバイス 108 が中間者リプレイ攻撃を成功裏に実行することができる場合、攻撃デバイス 108 によって伝搬遅延に挿入される誤差は、たとえば、U E 102 から g N B 110 までの可能な最大範囲によって制限される、たとえば、 $100\mu s$ 未満または $10\mu s$ 未満など、必然的に小さくなる。その上、U E 102 は、任意の可能な誤差を、たとえば、 $1\mu s$ 未満にさらに低減し得る、予想伝搬遅延を実測伝搬遅延と比較することによって、現在時刻誤差が非常に小さいときであってもスプーフィングを検出し得る。この技術は以下にさらに詳述される。

【0085】

【0098】 図 4 B は、図 4 A と同様であり、攻撃デバイス 108 が存在し、リプレイ攻撃を実行しているワイヤレスネットワークにおけるブロードキャストおよび信頼できる時刻の取得、および R T T 手順を使用したリプレイ攻撃の検出のためのシグナリングフロー 450 を示す。図 4 B は、非限定的な例として与えられるものである。たとえば、追加のシグナリングおよびプロセスが存在し得ること、ならびに g N B 110 と U E 102 との間で送信されるメッセージが追加の構成要素を含み得ることが理解されよう。R T T および伝搬遅延を決定するための図 4 B における手順は、通常図 4 B に、U E 102 によって取得される時刻およびタイミング測定値に影響を及ぼす攻撃デバイス 108 が存在することを除いて、U E 102 および g N B 110 の視点から見た図 3 B について説明した手順と同じであり得る。図 4 B に示される手順の利点は、それが、R R C I D L E または R R C I N A C T I V E 状態にあり、タイミングアドバンスが利用可能でない可能性がある U E 102 によって使用され得ることである。

【0086】

【0099】 図 4 B に示すように、図 4 A に示されるメッセージ 402 および 403 と同様に、現在時刻 T またはそれに近い時刻において、g N B 110 はメッセージ 452 をブロードキャストし、このメッセージは攻撃デバイス 108 によって受信され、コピーされ、遅延 $\Delta 1$ の後、リプレイ攻撃中に、メッセージ 453 として U E 102 に送信され、これにより、U E 102 は時刻 $T + \Delta + \Delta 1$ においてコピーされたメッセージ 453 内の現在時刻 T を受信することとなる。メッセージ 452 (したがってメッセージ 453) は、その一部分が暗号化され得る現在時刻 T、ならびに g N B 110 におけるオプションの明示的または暗黙的なローカル N R 送信時刻 t 、およびデジタル署名 (D i g S i g) を含む。メッセージ 452 (したがって、メッセージ 453) は、基地局サブフレームまたはスロット境界への現在時刻 T のアライメントの暗黙的または明示的指示、現在時刻 T の不確実性、現在時刻 T のソース、またはそれらの組合せをさらに含み得る。U E 102 は、現在時刻 T の少なくとも一部分を解読して、平文の現在時刻 T を取得し得る。

【0087】

【0100】 図 3 B において説明した R T T 手順と同様に、g N B 110 は、g N B 110 におけるローカル時刻 t において、メッセージまたは信号 454 (たとえば、S S B メッセージまたは C S I - R S 信号) を U E 102 に送信し得る。メッセージまたは信号 454 は、攻撃デバイス 108 によって受信され、コピーされ、遅延 $\Delta 1$ の後にメッセージまたは信号 455 として U E 102 に送信される。メッセージまたは信号 454、したがってメッセージまたは信号 455 は、g N B 110 による送信のローカル時刻 t を含むかまたは示すことができ、U E 102 は、g N B 110 からの時刻 t に一致するようにその内部タイミングを設定することができる。攻撃デバイス 108 は、U E 102 によって検出されることなく、メッセージ 453 の送信および (後述する) メッセージ 459 の送信における遅延 $\Delta 1$ に対する、メッセージまたは信号 455 の送信における遅延 $\Delta 1$ を変化させることができず、したがって、U E は、攻撃デバイス 108 の存在または g N B 110 からの送信に少なくとも何らかの重大なエラーが生じたことを推測することができることに留意されたい。攻撃デバイス 108 が遅延 $\Delta 1$ を変化させる場合、U E 102 は、U E 102 内のローカル時刻ソースと比較して、(通常、メッセージまたは信号 455 なら

びにメッセージ453および459内で暗黙的または明示的に搬送される) gNB110におけるローカル送信時刻 t の対応する変動を検出することができる。UE102内のローカル時刻ソースは、gNB110内のローカル時刻 t ほど正確ではない可能性があるが、攻撃デバイス108が遅延 $\Delta 1$ を変化させた場合に、UE102の視点から見た発生し得るgNB110のローカル時刻 t の大幅な(たとえば、 $10\mu s$ 以上の)変化を検出するのに十分に正確であり得る。

【0088】

【0101】 メッセージまたは信号455に応答して、UE102は、たとえば、RACH要求メッセージであるRRCメッセージであり得るメッセージ456をgNB110に送り得る。メッセージ456は、gNB110用のRACH上でUE102によって送信され得る。UE102は、メッセージ456中に、ランダム変数(RV)、たとえば、8~16ビットを含むランダムビット列を含め得る。メッセージ456は、UEのローカル時刻またはgNB110の関連付けられたローカル送信時刻のいずれか一方であり得る第1の時刻に送信される。攻撃デバイス108は、メッセージ456を受信し、遅延 $\Delta 2$ の後にコピーされたメッセージ457をgNB110に送信することができる。したがって、gNB110は、ここでは第2の時刻と呼ぶローカル時刻 $t + 2\Delta + \Delta 1 + \Delta 2$ においてコピーされたメッセージ457を受信する。遅延 $\Delta 2$ が遅延 $\Delta 1$ に等しい場合、攻撃デバイス108によって挿入された遅延 $2 \times \Delta 1$ を含む、信号453の受信の総伝搬遅延 $\Delta + \Delta 1$ は、UE102とgNB110との間の往復時間(RTT)に基づいて、UE102によって決定され得る。したがって、遅延 $\Delta 2$ は $\Delta 1$ と異なると推定し得る。また、図4Bは(図3Bと同様に)、UE102におけるメッセージまたは信号455の受信時に発生するものとして第1の時刻を示しており、したがって、第1の時刻は、メッセージまたは信号455に含まれているか、またはそれによって示されている時刻 t に対応することに留意されたい。しかしながら、第1の時刻が、メッセージまたは信号455のUE102への到着の直後(たとえば、 $1 \sim 100ms$ 後)に発生することも可能であり、この場合、第1の時刻は、UE102によって知られており、かつ t を超えているgNB110の何らかのローカル送信時刻に対応することができる。

【0089】

【0102】 gNB110は、コピーされたメッセージ457の到着時刻を取得し(たとえば、測定し)(すなわち、第2の時刻を測定し)、応答メッセージ458、たとえば、gNB110用のCCH上で送信されるRRCメッセージをUE102に返す。応答メッセージ458は、ランダム変数(RV)、デジタル署名(DigSig)、および図4Bでは、コピーされたメッセージ457のgNB110におけるローカル受信時刻 $t + 2\Delta + \Delta 1 + \Delta 2$ である第2の時刻を含む。応答メッセージ458は、gNB110によって暗号化され得る。攻撃デバイス108は、応答メッセージ458を受信し、応答メッセージ458のコピーであるメッセージ459を、たとえば遅延 $\Delta 1$ の後に、UE102に送信する。応答メッセージ458にデジタル署名(DigSig)を含めることにより、gNB110が応答メッセージ458を発信したことが検証される。したがって、デジタル署名検証が失敗するとUE102がメッセージ459の変更を検出するので、攻撃デバイス108は、応答メッセージ458を変更することができない。さらに、応答メッセージがないことからUE102が攻撃を検出するので、攻撃デバイス108は、応答メッセージ458をブロックすることができない。したがって、UE102は、ランダム変数(RV)および(図4BにおいてgNB110におけるコピーされたメッセージ457の受信のローカル時刻 $t + 2\Delta + \Delta 1 + \Delta 2$ に対応する)第2の時刻を持っている、コピーされた応答メッセージ459を受信する。UE102は、伝搬遅延を $\Delta + (\Delta 1 + \Delta 2) / 2$ として取得し得る。

【0090】

【0103】 図3Bのシグナリングフロー350と同様に、UE102が(たとえば、メッセージ456を送信した後に何らかの最大予想応答時間が経過しても)コピーされた応答メッセージ459を受信していない場合、UE102は、後の時刻 t' においてメッセ

ージ 4 5 6 (図 4 B に図示せず) を再送信し、コピーされた応答メッセージ 4 5 9 と同様の応答メッセージ (図 4 B に図示せず) を受信するのを待つことができる。これは、たとえば、干渉または U E 1 0 2 によるメッセージ 4 5 7 の送信または攻撃デバイス 1 0 8 によるコピーされたメッセージ 4 5 6 の送信のいずれかの低送信電力に起因して、g N B 1 1 0 がコピーされたメッセージ 4 5 7 を正しく受信していない場合に起こり得る。メッセージ 4 5 6 の再送信について、g N B 1 1 0 が応答メッセージ 4 5 8 と同様の応答メッセージを送信すると仮定すると、U E 1 0 2 は、時刻 t の代わりに時刻 t' を用いて、上記のように伝搬遅延 $\Delta + (\Delta 1 + \Delta 2) / 2$ を取得することができる。

【0091】

【0104】 攻撃デバイス 1 0 8 が大きすぎる遅延 $\Delta 1$ および / または $\Delta 2$ を伝搬遅延中に挿入する場合、U E 1 0 2 は攻撃を検出することができる。たとえば、ワイヤレスセルは、伝搬時間の可能な量を制限する限られたサイズを有する。中継なしの U E 1 0 2 と g N B 1 1 0 との間の最大可能範囲は、たとえば、大きいセルサイズに基づいて 3 0 k m であり得、これは、約 1 0 0 μ s の伝搬遅延に変換される。通常、地方地域でのみ行われ得る中継が存在するとき、最大可能範囲は (たとえば、1 0 0 k m に) 増加し得、この場合、U E 1 0 2 は、既知の環境 (たとえば、都市、郊外、もしくは地方)、またはネットワーク事業者もしくは U E ベンダーによって U E 1 0 2 に環境が構成され得る、U E 1 0 2 のおおよその既知のロケーションに基づいて、最大可能範囲の予想を調整することができる。したがって、U E 1 0 2 が 1 0 0 μ s を超える総伝搬遅延を検出し、かつ中継が存在していない場合、U E 1 0 2 は、攻撃デバイスが伝搬遅延に追加の遅延を挿入した可能性があり、したがって、メッセージ 4 5 3 中で受信した現在時刻 T は信頼できず、破棄されるべきであると推測することができる。U E 1 0 2 はさらに、攻撃を検出するために、より小さいまたはより大きい閾値、たとえば、都市もしくは郊外環境での 1 0 μ s、または中継が存在し得る田舎環境での 1 m s を使用し得る。したがって、検出を回避するために、攻撃デバイス 1 0 8 は、図 4 B に示す手順をブロックすることも、応答メッセージ 4 5 8 をスプーフィングすることもできず、その結果、攻撃デバイス 1 0 8 が伝搬遅延に挿入できる誤差の量は、伝搬遅延を検証するために U E 1 0 2 によって使用される、ほとんどの環境で 1 0 ~ 1 0 0 μ s であり得る閾値未満に制限される。

【0092】

【0105】 加えて、U E 1 0 2 が、たとえば、前の位置推定からそれ自体のロケーションを知っており、かつ g N B 1 1 0 のロケーションを知っている場合、U E 1 0 2 は、2 つのロケーション間の距離に基づいて、予想伝搬遅延 Δ を独立して決定することができる。次いで、U E 1 0 2 は、伝搬遅延の予想値 Δ と、(たとえば、図 4 B の手順に従って、またはタイミングアドバンスを使用して取得される) 伝搬遅延の実測値 Δ との間の不一致に基づいて、攻撃デバイス 1 0 8 によるスプーフィングを検出し得る。不一致が閾値、たとえば、1 μ s よりも大きい場合、U E 1 0 2 は、攻撃デバイスが伝搬遅延に追加の遅延を挿入した可能性があり、したがって、メッセージ 4 5 3 中で受信した現在時刻 T は信頼できず、破棄されるべきであると決定することができる。(リプレイまたは中間者攻撃のために) 攻撃デバイス 1 0 8 によって加えられる遅延は通常、実測伝搬遅延を検証するために U E 1 0 2 によって使用される閾値 (たとえば、1 μ s) よりもはるかに大きいので、この追加のロケーションベース検証を用いて、U E 1 0 2 は、攻撃デバイス 1 0 8 の存在または不在を高い確率で検証することができる。

【0093】

【0106】 前に説明したように、U E 1 0 2 が R R C C O N N E C T E D 状態にあるときに g N B 1 1 0 によって U E 1 0 2 に提供されるタイミングアドバンス値を用いて U E 1 0 2 によって、伝搬遅延が取得されるとき、上記のような実測伝搬遅延と予想伝搬遅延との比較はまた、U E 1 0 2 によって実行され得る。攻撃デバイスが U E 1 0 2 に対して中間者攻撃を実行している場合、(たとえば、図 4 B に示すように) U E 1 0 2 と g N B 1 1 0 との間のすべてのシグナリングが攻撃デバイス 1 0 8 によって受信され、コピーされ、転送され、かつ g N B 1 1 0 によるタイミングアドバンス決定が攻撃デバイス 1 0

8によって追加された遅延を含むので、gNB110によってUE102に提供されるタイミングアドバンスもまた遅延 $\Delta 1$ および $\Delta 2$ を含む。次いで、UE102は、伝搬遅延をタイミングアドバンスの半分として取得し、これを、UE102とgNB110との間の最大可能範囲に基づく予想値、またはUE102とgNB110との既知のロケーションに基づくUE102とgNB110との間の算出された範囲と比較することができる。次いで、攻撃デバイス108の存在の推論は、図4BのRTT手順について前に説明したものと全く同じであり得る。

【0094】

【0107】 UE102は、攻撃デバイス108の存在または不在を判定するための手段として、伝搬遅延の代わりに、UE102とgNB110との間のRTTを（たとえば、図4Bの手順に）使用ができることに留意されたい。RTTは、伝搬遅延の2倍であり、したがって、伝搬遅延と同様にUE102によって測定または取得され得る。同様に、RTTの予想範囲は、伝搬遅延の予想範囲の2倍になる。よって、攻撃デバイス108の存在を検出するための伝搬遅延の使用に関する本明細書の様々な記述は、RTTの使用にも適用することができる。

【0095】

【0108】 図5は、UE102、gNB110、およびLMF152、ならびに攻撃デバイス108によるリプレイ攻撃の検出を含むワイヤレスネットワークにおける信頼できる時刻のブロードキャストおよび取得のためのシグナリングフロー500を示す。

【0096】

【0109】 段階1では、UE102は、UE102とgNB110との間の予想範囲を決定する。予想範囲の決定は、たとえば、UE102およびgNB110の既知のロケーションに基づき得る。UE102のロケーションは、DL-TDOA、DL-AOD、マルチセルRTT、A-GNSS、Wi-Fi、ECIDなど、既知の測位技法を使用して、UE102とLMF152（または図5に示されていないSLP162）との間の測位セッションを使用して、UE102によって、またはLMF152によって決定され得る（次いで、LMF152はロケーションをUE102に与え得る）。UE102は、gNB110のロケーションを、LMF152から（もしくはSLP162から）、gNB110から（たとえば、現在時刻Tを含むメッセージもしくは他のブロードキャストメッセージ中にgNB110によって含まれている場合）、またはgNBロケーションが近似的に決定されているPLMN用のインターネットウェブサーバから利用可能な情報から取得し得る。それによって、いくつかの実装形態では、UE102は、UE102とgNB110との間の予想範囲を決定することができる。他の実装形態では、LMF152が、予想範囲を決定することができ、予想範囲をUE102に与えることができる。

【0097】

【0110】 段階2では、gNB110は、現在時刻Tを、gNB110におけるローカル送信時刻tの暗黙的または明示的な指示およびデジタル署名（DigSig）とともに、たとえばSIBメッセージ中でブロードキャストし、これは、攻撃デバイス108によって受信および記憶され得る。

【0098】

【0111】 段階3では、攻撃デバイス108は、遅延 $\Delta 1$ の後に、ローカル送信時刻tの暗黙的または明示的な指示およびデジタル署名（DigSig）とともに、現在時刻Tを持っているSIBメッセージのコピーをUE102に送信する。

【0099】

【0112】 段階4では、UE102は、攻撃デバイスによって挿入された遅延（たとえば、 $\Delta + (\Delta 1 + \Delta 2) / 2$ ）を含む、UE102とgNB110との間の総伝搬遅延を取得する。総伝搬遅延は、たとえば、（たとえば、UE102がRRC IDLEまたはRRC INACTIVE状態にある場合）図4Bで説明したように測定され得るか、または（たとえば、UE102がRRC CONNECTED状態にある場合）gNB110によって与えられたタイミングアドバンスからUE102によって決定され得る。

【0100】

【0113】 段階5では、UE102は、段階1で取得した予想範囲と、段階4で測定した総伝搬遅延（たとえば $\Delta + (\Delta 1 + \Delta 2) / 2$ ）とに基づいて、攻撃デバイス108の存在を検出し得る。たとえば、予想伝搬遅延は、UE102とgNB110との間の予想範囲に基づいて決定され得、予想伝搬遅延は、段階4からの実測伝搬遅延と比較され得る。閾値（たとえば、 $100\mu s$ 、 $10\mu s$ 、または $1\mu s$ ）よりも大きい不一致は、攻撃デバイスの存在と、段階2で受信した現在時刻の非信頼性を示し得る。別の例では、実測範囲は、段階4で測定された総伝搬遅延に基づいて決定され、UE102とgNB110との間の予想範囲と比較され得る。閾値距離（たとえば、 30 km 、 3 km 、または 300 メートル ）よりも大きい不一致は、攻撃デバイスの存在と、段階2で受信した現在時刻の非信頼性を示し得る。

10

【0101】

【0114】 したがって、UE102は、ワイヤレスネットワークにおいて正確な現在時刻を受信し得、現在時刻が信頼できるものであることを検証することができる。スプーフィングが発生した場合、UE102は、スプーフィングを検出し、したがって、受信した現在時刻が信頼できないものであることを知り得るか、またはスプーフィングによって正常に挿入された誤差の量が最小限（たとえば、 $100\mu s$ 、 $10\mu s$ 、または $1\mu s$ 未満）で、UE102によって取得される現在時刻を著しく損なわない可能性がある。

【0102】

【0115】 図6は、本明細書で説明されるように、ワイヤレスネットワークからの現在時刻の取得をサポートするために構成された、たとえば、図1、図3A、図3B、図4A、図4B、および図5に示すUE102であり得る、UE600の特定の例示的な特徴を示す概略ブロック図を示す。UE600は、たとえば、図3A、図3B、図4A、図4B、および図5に示される信号フロー、図8に示されるプロセスフロー、ならびに本明細書で開示されるアルゴリズムを実行し得る。UE600は、たとえば、1つ以上の接続606（たとえば、バス、配線、ファイバ、リンクなど）を用いて非一時的コンピュータ可読媒体620およびメモリ604に動作可能に結合され得る、1つ以上のプロセッサ602と、メモリ604と、WWANトランシーバ610およびWLANTランシーバ612として図示されている少なくとも1つのワイヤレストランシーバ（たとえば、ワイヤレスネットワークインターフェース）などの外部インターフェースと、SPS受信機615と、1つ以上のセンサ613と、を含み得る。SPS受信機615は、たとえば、図1に示されているSV190からSPS信号を受信し、処理し得る。1つ以上のセンサ613は、たとえば、1つ以上の加速度計、1つ以上のジャイロスコープ、磁力計などを含み得る慣性測定ユニット（Inertial Measurement Unit: IMU）であり得る。UE600はさらに、ユーザがそれを通じてUEとインターフェースし得る、ディスプレイ、キーパッド、またはディスプレイ上の仮想キーパッドなどの他の入力デバイスを含み得るユーザインターフェースなど、示されていない追加のアイテムをさらに含み得る。特定の例示的な実装形態では、UE600の全部または一部が、チップセットおよび／またはそれに類するものの形態であり得る。

20

30

【0103】

【0116】 少なくとも1つのワイヤレストランシーバは、WWAN通信システム用のトランシーバ610およびWLAN通信システム用のトランシーバ612であってもよく、または、WWANとWLANの両方用の複合トランシーバであってもよい。WWANトランシーバ610は、ワイヤレス信号を（たとえば、1つ以上のアップリンクチャネルおよび／または1つ以上のサイドリンクチャネル上で）送信および／または（たとえば、1つ以上のダウンリンクチャネルおよび／または1つ以上のサイドリンクチャネル上で）受信し、ワイヤレス信号からワイヤード（たとえば、電気および／または光）信号に、およびワイヤード（たとえば、電気および／または光）信号からワイヤレス信号に信号を変換するために、1つ以上のアンテナ611に結合された送信機610tおよび受信機610rを含み得る。WLANTランシーバ612は、ワイヤレス信号を（たとえば、1つ以上の

40

50

アップリンクチャネルおよび／または1つ以上のサイドリンクチャネル上で)送信および／または(たとえば、1つ以上のダウンリンクチャネルおよび／または1つ以上のサイドリンクチャネル上で)受信し、ワイヤレス信号からワイヤード(たとえば、電気および／または光)信号に、およびワイヤード(たとえば、電気および／または光)信号からワイヤレス信号に信号を変換するために、1つ以上のアンテナ611または別個のアンテナに結合された送信機612tおよび受信機612rを含み得る。送信機610tおよび612tは、個別の構成要素もしくは複合／統合された構成要素であり得る複数の送信機を含んでもよく、ならびに／または、受信機610rおよび612rは、個別の構成要素もしくは複合／統合された構成要素であり得る複数の受信機を含んでもよい。WWANトランシーバ610は、6G新無線(NR)、移動体用グローバルシステム(Global System for Mobiles: GSM)、ユニバーサル移動体通信システム(Universal Mobile Telecommunications System: UMTS)、高度携帯電話システム(Advanced Mobile Phone System: AMPS)、符号分割多元接続(Code Division Multiple Access: CDMA)、広帯域CDMA(Wideband CDMA: WCDMA)、ロングタームエボリューション(Long-Term Evolution: LTE)、LTEダイレクト(LTE Direct: LTE-D)、3GPP LTE-V2X(PC5)などの様々な無線アクセス技術(RAT)に従って、信号を(たとえば、基地局および／または1つ以上の他のデバイスと)通信するように構成され得る。新無線(NR)は、ミリ波周波数および／またはサブ6GHz周波数を使用し得る。WLANTランシーバ612は、3GPP LTE-V2X(PC5)、(IEEE 802.11pを含む)IEEE 802.11、Wi-Fi、Wi-Fiダイレクト(Wi-Fi-D)、Bluetooth(登録商標)、Zigbee(登録商標)などの様々な無線アクセス技術(RAT)に従って、信号を(たとえば、アクセスポイントおよび／または1つ以上の他のデバイスと)通信するように構成され得る。トランシーバ610および612は、たとえば、トランシーバ610および612と少なくとも部分的に統合され得る、光接続および／または電気接続によって、トランシーバインターフェースに通信可能に結合され得る。

10

20

30

40

50

【0104】

【0117】 いくつかの実施形態では、UE600は、内部または外部にあり得るアンテナ611を含み得る。UEアンテナ611は、ワイヤレストランシーバ610および612によって処理される信号を送信および／または受信するために使用され得る。いくつかの実施形態では、UEアンテナ611はワイヤレストランシーバ610および612に結合され得る。いくつかの実施形態では、UE600によって受信される(送信される)信号の測定は、UEアンテナ611とワイヤレストランシーバ610および612との接続点において実行され得る。たとえば、受信される(送信される)RF信号の測定基準点は、受信機610r(送信機610t)の入力(出力)端子およびUEアンテナ611の出力(入力)端子であり得る。複数のUEアンテナ611またはアンテナアレイを備えているUE600では、アンテナコネクタは、複数のUEアンテナの集約出力(入力)を表す仮想的な点と見なされ得る。いくつかの実施形態では、UE600は、信号強度とTOA測定値とを含めて、受信した信号を測定し得、生の測定値は、1つ以上のプロセッサ602によって処理され得る。

【0105】

【0118】 1つ以上のプロセッサ602は、ハードウェアと、ファームウェアと、ソフトウェアとの組合せを使用して実装され得る。たとえば、1つ以上のプロセッサ602は、媒体620および／またはメモリ604などの非一時的コンピュータ可読媒体上に1つ以上の命令またはプログラムコード608を実装することによって、本明細書で説明される機能を実行するように構成され得る。いくつかの実施形態では、1つ以上のプロセッサ602は、UE600の動作に関連するデータ信号計算手順またはプロセスの少なくとも一部分を実行するように構成可能な1つ以上の回路を表し得る。

【0106】

【0119】 媒体620および／またはメモリ604は、1つ以上のプロセッサ602に

よって実行されると、本明細書で開示される技法を実行するようにプログラムされた専用コンピュータとして1つ以上のプロセッサ602を動作させる実行可能コードまたはソフトウェア命令を含む、命令またはプログラムコード608を記憶し得る。UE600に示されるように、媒体620および／またはメモリ604は、本明細書で説明される方法を実行するように1つ以上のプロセッサ602によって実装され得る1つ以上の構成要素またはモジュールを含み得る。構成要素またはモジュールが、1つ以上のプロセッサ602によって実行可能な媒体620の中のソフトウェアとして示されているが、構成要素もしくはモジュールはメモリ604内に記憶されていてもよく、または、1つ以上のプロセッサ602の内もしくはプロセッサ外のどちらか一方にある専用ハードウェアであってもよいことを理解されたい。

10

【0107】

【0120】いくつかのソフトウェアモジュールおよびデータテーブルが、媒体620および／またはメモリ604の中に常駐し、本明細書で説明される通信と機能性の両方を管理するために1つ以上のプロセッサ602によって利用され得る。UE600に示されるような媒体620および／またはメモリ604のコンテンツの編成は例示的なものにすぎず、したがって、モジュールおよび／またはデータ構造の機能性は、UE600の実装形態に応じて異なる方法で組み合わせられ、分離され、および／または構造化され得ることを理解されたい。

【0108】

【0121】媒体620および／またはメモリ604は、1つ以上のプロセッサ602によって実行されると、基地局によってブロードキャストされたSIBメッセージなどのメッセージ中の現在時刻を、たとえば、ワイヤレスランシーバ610を介して受信するように1つ以上のプロセッサ602を構成する現在時刻モジュール622を含み得る。1つ以上のプロセッサ602は、受信した現在時刻と決定された伝搬遅延とに基づいて、補正済み現在時刻を決定するようにさらに構成され得る。現在時刻の少なくとも一部分が暗号化され得る。現在時刻は、たとえば、UTC時刻、GPS時刻、GLONASS時刻、BeiDou時刻、Galileo時刻、GNSS時刻であり得る。メッセージは、基地局用のローカル送信時刻をさらに含み得る。1つ以上のプロセッサ602は、基地局サブフレームまたはスロット境界への現在時刻のアライメント、現在時刻の不確実性、現在時刻のソース、またはそれらの組合せのうちの少なくとも1つなどの追加情報をメッセージ中で受信するようにさらに構成され得る。1つ以上のプロセッサ602は、メッセージ中で基地局のデジタル署名を受信するようにさらに構成され得る。

20

30

【0109】

【0122】媒体620および／またはメモリ604は、1つ以上のプロセッサ602によって実行されると、現在時刻の少なくとも一部分を含む基地局からのメッセージを解読して、平文の現在時刻を取得し、および／またはUEと基地局との間の伝搬遅延を決定するために基地局から受信したメッセージを解読するように1つ以上のプロセッサ602を構成するセキュリティモジュール624を含み得る。1つ以上のプロセッサ602は、メッセージ中に含まれている基地局用のデジタル署名に基づいて、基地局から送られてきたメッセージを認証するようにさらに構成され得る。1つ以上のプロセッサ602は、たとえば、ワイヤレスネットワークに接続し、それを認証した後に、たとえば、ワイヤレスランシーバ610を介して、ワイヤレスネットワークから基地局用の公開暗号化鍵を受信するように構成され得、公開暗号化鍵は、メッセージおよびデジタル署名を解読するために使用され得る。

40

【0110】

【0123】媒体620および／またはメモリ604は、1つ以上のプロセッサ602によって実行されると、基地局とUEとの間の伝搬遅延を決定するように1つ以上のプロセッサ602を構成する伝搬遅延モジュール626を含み得る。たとえば、1つ以上のプロセッサ602は、ワイヤレスを介して基地局からタイミングアドバンスを受信し、タイミングアドバンスを伝搬遅延として使用するように構成され得、すなわち、伝搬遅延はタイ

50

ミングアドバンスに等しい。別の例では、1つ以上のプロセッサ602は、たとえば、測位セッションからUEのロケーションおよび基地局のロケーションを取得し、UEのロケーションと基地局のロケーションとの間の距離に基づいて伝搬遅延を決定し得る。1つ以上のプロセッサ602は、SIB中で基地局のロケーションを持っているブロードキャストを基地局から受信する、基地局のロケーションを含むLPP支援データメッセージを受信する、UEのロケーションを含むMO-LR応答メッセージを受信する、測位セッションを実行してUEのロケーションを決定する、またはそれらの組合せを行う、ように構成されることによって、UEのロケーションおよび基地局のロケーションを取得するように構成され得る。別の例では、1つ以上のプロセッサ602は、UEと基地局との間のRTTを測定し、RTTの半分に基づいて伝搬遅延を決定するように構成され得る。たとえば、1つ以上のプロセッサ602は、図3Bおよび図4Bに示されるRTT手順を実行するように構成され得る。1つ以上のプロセッサ602は、トランシーバ610を介して、基地局用のローカル送信時刻を含む第1のメッセージを基地局から受信するように構成され得、たとえば、受信した基地局用のローカル送信時刻とUEにおけるメッセージの受信のローカル時刻とに基づいて、UEにおけるローカルタイミングを基地局用のローカル送信時刻に関連付け得る。1つ以上のプロセッサ602は、トランシーバ610を介して、ランダム変数を含むRACH要求メッセージなどの第2のメッセージを基地局に送信し、それに応答して、トランシーバ610を介して、ランダム変数と、要求メッセージが基地局において受信された基地局用のローカル送信時刻とを含む第3のメッセージ、たとえば、RACH応答メッセージを基地局から受信するように構成され得る。第3のメッセージは暗号化され得、基地局用のデジタル署名を含み得る。1つ以上のプロセッサ602は、第1の時刻および第3のメッセージ中で基地局によって提供される時刻に基づいてRTTを決定するように構成され得る。

10

20

30

40

【0111】

【0124】媒体620および／またはメモリ604は、1つ以上のプロセッサ602によって実行されると、サービング基地局を通して、たとえば、ワイヤレストランシーバ610を介してロケーションサーバとの、測位能力要求メッセージを受信することと、基地局から測位支援データおよび／またはブロードキャストロケーション情報を受信することと、ロケーション情報の要求を受信することと、1つ以上の基地局から受信したTDOA、AOD、マルチRTT、ECIDなどのPRS信号の測位測定を実行することとを含む測位セッションに参与し、たとえば、UE支援測位プロセスの測位測定値などのロケーション情報を報告するか、またはUEベースの測位プロセスの位置推定値を決定するように、1つ以上のプロセッサ602を構成する測位セッションモジュール628を含み得る。

【0112】

【0125】媒体620および／またはメモリ604は、1つ以上のプロセッサ602によって実行されると、ワイヤレスネットワークにおける攻撃デバイスの存在を検出するように1つ以上のプロセッサ602を構成する攻撃検出モジュール630を含み得る。攻撃デバイスの存在は、伝搬遅延が予想範囲外であると決定される実測RTTに基づいて検出され得る。予想範囲は、たとえば、基地局までの最大予想距離に基づく最大RTT値であり得る。予想範囲は、たとえば、たとえば測位セッションにおいて決定されるUEの推定ロケーションと、基地局のロケーションとの間の決定される距離に基づいて決定され得る。

【0113】

【0126】本明細書で説明される方法は、用途に応じて様々な手段によって実装され得る。たとえば、これらの方法は、ハードウェア、ファームウェア、ソフトウェア、またはこれらの任意の組合せで実装され得る。ハードウェア実装形態の場合、1つ以上のプロセッサ602は、1つ以上の特定用途向け集積回路(ASIC)、デジタル信号プロセッサ(Digital Signal Processor: DSP)、デジタル信号処理デバイス(Digital Signal Processing Device: DSPD)、プログラマブル論理デバイス(Programmable Logic Device: PLD)、フィールドプログラマブルゲートアレイ(Field Program

50

mable Gate Array：FPGA）、プロセッサ、コントローラ、マイクロコントローラ、マイクロプロセッサ、電子デバイス、本明細書で説明される機能を実行するように設計された他の電子ユニット、またはそれらの組合せで実装され得る。

【0114】

【0127】ファームウェアおよび／またはソフトウェアの実装形態の場合、方法は、本明細書で説明される機能を実行する（たとえば、手順、機能などの）モジュールを用いて実装され得る。命令を有形に具現化する任意の機械可読媒体が、本明細書で説明される方法の実装に使用され得る。たとえば、ソフトウェアコードは、1つ以上のプロセッサ602に接続され、1つ以上のプロセッサ602によって実行される非一時的コンピュータ可読媒体620またはメモリ604内に記憶されていてもよい。メモリは、1つ以上のプロセッサの内部に、または1つ以上のプロセッサの外部に実装されてもよい。本明細書で使用する「メモリ」という用語は、任意のタイプの長期メモリ、短期メモリ、揮発性メモリ、不揮発性メモリ、またはその他のメモリを指し、特定のタイプのメモリもしくは特定のメモリ数に限定するものではなく、または、メモリが格納されている媒体を特定のタイプに限定するものではない。

【0115】

【0128】ファームウェアおよび／またはソフトウェアで実装される場合、機能は、媒体620および／またはメモリ604などの非一時的コンピュータ可読媒体上に1つ以上の命令またはプログラムコード608として記憶されていてもよい。例は、データ構造を用いて符号化されたコンピュータ可読媒体、およびコンピュータプログラムコード608を用いて符号化されたコンピュータ可読媒体を含む。たとえば、その上に記憶されているプログラムコード608を含む非一時的コンピュータ可読媒体は、開示されている実施形態に一致する方法を用いた、UEによるワイヤレスネットワークからの現在時刻の取得をサポートするためのプログラムコード608を含み得る。非一時的コンピュータ可読媒体620は、物理コンピュータ記憶媒体を含む。記憶媒体は、コンピュータによってアクセスされ得る任意の利用可能な媒体であり得る。限定ではなく例として、このような非一時的コンピュータ可読媒体は、RAM、ROM、EEPROM（登録商標）、CD-ROMまたは他の光学ディスク記憶装置、磁気ディスク記憶装置または他の磁気記憶デバイス、あるいは命令またはデータ構造の形態で所望のプログラムコード608を記憶するために使用することができ、コンピュータによってアクセスされ得る任意の他の媒体を含むことができる。本明細書で使用する「disk」および「disc」は、コンパクトディスク（Compact Disc：CD）、レーザーディスク（登録商標）（laser disc）、光学ディスク（optical disc）、デジタル多用途ディスク（Digital Versatile Disc：DVD）、フロッピー（登録商標）ディスク（floppy disk）およびBlue-rayディスク（Blu-ray（登録商標）disc）を含むが、「disk」は通常、データを磁気的に再生し、「disc」は、レーザーを用いてデータを光学的に再生する。上記の組合せも、コンピュータ可読媒体の範囲内に含まれるものとする。

【0116】

【0129】コンピュータ可読媒体620上での記憶に加えて、命令および／またはデータは、通信装置内に含まれている伝送媒体上の信号として提供され得る。たとえば、通信装置は、命令およびデータを示す信号を有するワイヤレストランシーバ610を含み得る。命令およびデータは、1つ以上のプロセッサに、請求項に概説されている機能を実行させるように構成される。すなわち、通信装置は、開示されている機能を実行するための情報を示す信号を持っている送信媒体を含む。

【0117】

【0130】メモリ604は、任意のデータ記憶メカニズムを表し得る。メモリ604は、たとえば、1次メモリおよび／または2次メモリを含み得る。1次メモリは、たとえば、ランダムアクセスメモリ、読み取り専用メモリなどを含み得る。この例では1つ以上のプロセッサ602とは別個であるものとして示されているが、1次メモリの全部または一部が1つ以上のプロセッサ602内で提供されてもよいこと、または別様にそれと同位置

に配置され／結合されてもよいことを理解されたい。２次メモリは、たとえば、１次メモリと同じかまたは類似のタイプのメモリ、および／または、たとえば、ディスクドライブ、光学ディスクドライブ、テープドライブ、ソリッドステートメモリドライブなどの１つ以上のデータ記憶デバイスもしくはシステムを含み得る。

【０１１８】

【０１３１】 特定の実装形態では、２次メモリは、非一時的コンピュータ可読媒体 ６２０ を動作可能に受け入れてもよく、または別様に結合するように構成可能であってもよい。したがって、特定の例示的な実装形態では、本明細書で提示されている方法および／または装置は、全体的または部分的に、その上に記憶されているコンピュータ実装可能プログラムコード ６０８ を含み得るコンピュータ可読媒体 ６２０ の形態を取ってもよく、コンピュータ実装可能プログラムコードは、１つ以上のプロセッサ ６０２ によって実行されると、本明細書で説明されるような例示的な動作の全部または部分を実行するように動作可能に有効化され得る。コンピュータ可読媒体 ６２０ はメモリ ６０４ の一部であり得る。

【０１１９】

【０１３２】 図 ７ は、 gNB 、 $ng-eNB$ （たとえば eNB （たとえば、 $ng-eNB$ １１４）または eNB ）であり得、たとえば、図 １、図 ３Ａ、図 ３Ｂ、図 ４Ａ、図 ４Ｂ、および図 ５ に示す gNB １１０ であり得る、基地局 ７００ の特定の例示的な特徴を示す概略ブロック図を示す。基地局 ７００ は、たとえば、本明細書で説明されるように、現在時刻のブロードキャストと UE による現在時刻の取得とをサポートするように構成される。基地局 ７００ は、たとえば、図 ３Ａ、図 ３Ｂ、図 ４Ａ、図 ４Ｂ、および図 ５ に示される信号フロー、ならびに図 ９ に示されるプロセスフロー、および本明細書で開示されるアルゴリズムを実行するように構成され得る。基地局 ７００ は、１つ以上の接続 ７０６（たとえば、バス、回線、ファイバ、リンクなど）を用いて非一時的コンピュータ可読媒体 ７２０ およびメモリ ７０４ に動作可能に結合され得る、たとえば、１つ以上のプロセッサ ７０２ と、メモリ ７０４ と、トランシーバ ７１０（たとえば、ワイヤレスネットワークインターフェース）と外部インターフェース ７１６（たとえば、他の基地局および／またはコアネットワークへのワイヤラインまたはワイヤレスネットワークインターフェース）とを含み得る通信インターフェースと、 SPS 受信機 ７１５ と、を含み得る。基地局 ７００ は、たとえば、ユーザがそれを通じて UE とインターフェースし得る、ディスプレイ、キーパッド、またはディスプレイ上の仮想キーパッドなどの他の入力デバイスを含み得るユーザインターフェースなど、示されていない追加のアイテムをさらに含み得る。特定の例示的な実装形態では、基地局 ７００ の全部または一部が、チップセットおよび／またはそれに類するものの形態であり得る。トランシーバ ７１０ は、たとえば、１つ以上のタイプのワイヤレス通信ネットワークを介して１つ以上の信号を送信することを可能にされた送信機 ７１２ と、１つ以上のタイプのワイヤレス通信ネットワークを介して送信されてきた１つ以上の信号を受信するための受信機 ７１４ とを含み得る。外部インターフェース ７１６ は、 RAN 内の他の基地局または図 １ に示される AMF １５４ および LMF １５２ などのネットワークエンティティに接続可能なワイヤードまたはワイヤレスインターフェースであり得る。 SPS 受信機 ７１５ は、たとえば、図 １ に示される SV １９０ から SPS 信号を受信し処理して、たとえば、 UTC 時刻、 GPS 時刻、 $GLONASS$ 時刻、 $Beidou$ 時刻、 $Galileo$ 時刻、および $GNSS$ 時刻などの現在時刻を取得し得る。

【０１２０】

【０１３３】 いくつかの実施形態では、基地局 ７００ は、内部にあっても外部にあってもよいアンテナ ７１１ を含み得る。アンテナ ７１１ は、トランシーバ ７１０ によって処理される信号を送信および／または受信するために使用され得る。いくつかの実施形態では、アンテナ ７１１ は、トランシーバ ７１０ に結合され得る。いくつかの実施形態では、基地局 ７００ によって受信される（送信される）信号の測定は、アンテナ ７１１ とトランシーバ ７１０ の接続点において実行され得る。たとえば、受信される（送信される） RF 信号の測定基準点は、受信機 ７１４（送信機 ７１２）の入力（出力）端子およびアンテナ ７１１ の出力（入力）端子であり得る。複数のアンテナ ７１１ またはアンテナアレイを備えて

いる基地局 700 では、アンテナコネクタは、複数のアンテナの集約出力（入力）を表す仮想的な点であると見なされ得る。いくつかの実施形態では、基地局 700 は、信号強度と T O A 測定値とを含めて、受信した信号を測定し得、生の測定値は、1 つ以上のプロセッサ 702 によって処理され得る。

【0121】

【0134】 1 つ以上のプロセッサ 702 は、ハードウェアと、ファームウェアと、ソフトウェアとの組合せを使用して実装され得る。たとえば、1 つ以上のプロセッサ 702 は、媒体 720 および／またはメモリ 704 などの非一時的コンピュータ可読媒体上に 1 つ以上の命令またはプログラムコード 708 を実装することによって、本明細書で説明される機能を実行するように構成され得る。いくつかの実施形態では、1 つ以上のプロセッサ 702 は、基地局 700 の動作に関連するデータ信号算出手順またはプロセスの少なくとも一部分を実行するように構成可能な 1 つ以上の回路を表し得る。

10

【0122】

【0135】 媒体 720 および／またはメモリ 704 は、1 つ以上のプロセッサ 702 によって実行されると、本明細書で開示される技法を実行するようにプログラムされた専用コンピュータとして 1 つ以上のプロセッサ 702 を動作させる実行可能コードまたはソフトウェア命令を含む、命令またはプログラムコード 708 を記憶し得る。基地局 700 に示されるように、媒体 720 および／またはメモリ 704 は、本明細書で説明される方法を実行するように 1 つ以上のプロセッサ 702 によって実装され得る 1 つ以上の構成要素またはモジュールを含み得る。構成要素またはモジュールが、1 つ以上のプロセッサ 702 によって実行可能な媒体 720 の中のソフトウェアとして示されているが、構成要素またはモジュールはメモリ 704 内に記憶されていてもよく、または、1 つ以上のプロセッサ 702 の内もしくはプロセッサ外のどちらか一方にある専用ハードウェアであってもよいことを理解されたい。

20

【0123】

【0136】 いくつかのソフトウェアモジュールおよびデータテーブルが、媒体 720 および／またはメモリ 704 の中に常駐し、本明細書で説明される通信と機能性の両方を管理するために 1 つ以上のプロセッサ 702 によって利用され得る。基地局 700 に示されるような媒体 720 および／またはメモリ 704 のコンテンツの編成は例示的なものにすぎず、したがって、モジュールおよび／またはデータ構造の機能性は、基地局 700 の実装形態に応じて異なる方法で組み合わせられ、分離され、および／または構造化され得ることを理解されたい。

30

【0124】

【0137】 媒体 720 および／またはメモリ 704 は、1 つ以上のプロセッサ 702 によって実行されると、たとえば、S P S 受信機 715 を介して S V 190 から、または外部インターフェース 716 を介して A M F 154 などのネットワークエンティティから、現在時刻を取得するように 1 つ以上のプロセッサ 702 を構成する現在時刻モジュール 722 を含み得る。現在時刻は、たとえば、U T C 時刻、G P S 時刻、G L O N A S S 時刻、B e i d o u 時刻、G a l i l e o 時刻、G N S S 時刻であり得る。1 つ以上のプロセッサ 702 は、たとえば、ワイヤレストランシーバ 710 を介して、S I B メッセージなどのメッセージ中で現在時刻をブロードキャストするようにさらに構成され得る。現在時刻の少なくとも一部分が暗号化され得る。ブロードキャストメッセージは、基地局用のローカル送信時刻をさらに含み得る。1 つ以上のプロセッサ 702 は、サブフレームまたはスロット境界への現在時刻のアライメント、現在時刻の不確実性、現在時刻のソース、またはそれらの組合せのうちの少なくとも 1 つなどの追加情報をメッセージ中でブロードキャストするようにさらに構成され得る。1 つ以上のプロセッサ 702 は、基地局用のデジタル署名を持っているメッセージをブロードキャストするようにさらに構成され得る。

40

【0125】

【0138】 媒体 720 および／またはメモリ 704 は、1 つ以上のプロセッサ 702 によって実行されると、現在時刻の少なくとも一部分を含む基地局からのメッセージ、およ

50

び／またはUEと基地局との間の伝搬遅延を決定するためにUEに送信されるメッセージを暗号化するように1つ以上のプロセッサ702を構成するセキュリティモジュール724を含み得る。1つ以上のプロセッサ702は、UEへの1つ以上のメッセージ中に基地局用のデジタル署名を含めるようにさらに構成され得る。1つ以上のプロセッサ702は、トランシーバ710を介して、基地局用の公開暗号化鍵をUEに送信するようにさらに構成され得、デジタル署名は、公開暗号化鍵に対応する秘密暗号化鍵に基づくものである。

【0126】

【0139】媒体720および／またはメモリ704は、1つ以上のプロセッサ702によって実行されると、伝搬遅延の決定においてUEを支援するように1つ以上のプロセッサ702を構成する伝搬遅延モジュール726を含み得る。たとえば、1つ以上のプロセッサ702は、タイミングアドバンスを取得し、ワイヤレスを介してUEに送信するように構成され得、伝搬遅延はタイミングアドバンスに等しい。別の例では、1つ以上のプロセッサ702は、UEのロケーションと基地局のロケーションとのうちの少なくとも一方を含むメッセージをUEに送り得、伝搬遅延は、UEのロケーションと基地局のロケーションとの間の距離に基づいて決定され得る。1つ以上のプロセッサ702は、たとえば、SIB中で基地局のロケーションをブロードキャストする、基地局のロケーションを含むLPP支援データメッセージを転送する、UEのロケーションを含むMO-LR応答メッセージをUEに送信する、UEとUE用のロケーション実行との間でのLPPメッセージを転達して、UEのロケーションを決定する、またはそれらの組合せを行う、ように構成され得る。別の例では、1つ以上のプロセッサ702は、UEと基地局との間のRTTの測定においてUEを支援するように構成され得、伝搬遅延はRTTの半分に等しい。たとえば、1つ以上のプロセッサ702は、図3Bおよび図4Bに示されるRTT手順を実行するように構成され得る。1つ以上のプロセッサ702は、トランシーバ710を介して、基地局用のローカル送信時刻を持っている第1のメッセージをUEに送信するように構成され得る。1つ以上のプロセッサ702は、トランシーバ710を介して、ランダム変数を含むRACH要求メッセージなどの第2のメッセージをUEから受信し、それに応答して、トランシーバ710を介して、ランダム変数と、基地局が要求メッセージを受信したローカル送信時刻とを含む第3のメッセージ、たとえば、RACH応答メッセージをUEに送信するように構成され得る。第3のメッセージは暗号化され得、基地局用のデジタル署名を含み得る。

【0127】

【0140】媒体720および／またはメモリ704は、1つ以上のプロセッサ702によって実行されると、たとえば、ワイヤレストランシーバ710および外部インターフェース716を介して、UEおよびロケーションサーバとの測位セッションに参与するように1つ以上のプロセッサ702を構成する測位セッションモジュール728を含み得る。測位セッションは、たとえば、LPP測位メッセージを転達することと、測定のためにUEにPRS信号を送信することと、および／またはUEからアップリンクPRS信号を受信および測定することと、外部インターフェース716を介してロケーションサーバに、またはトランシーバ710を介してUEに、UL測定値を転送することと、を含み得る。

【0128】

【0141】本明細書で説明される方法は、用途に応じて様々な手段によって実装され得る。たとえば、これらの方法は、ハードウェア、ファームウェア、ソフトウェア、またはこれらの任意の組合せで実装され得る。ハードウェア実装形態の場合、1つ以上のプロセッサ702は、1つ以上の特定用途向け集積回路(ASIC)、デジタル信号プロセッサ(DSP)、デジタル信号処理デバイス(DSPD)、プログラマブル論理デバイス(PLD)、フィールドプログラマブルゲートアレイ(FPGA)、プロセッサ、コントローラ、マイクロコントローラ、マイクロプロセッサ、電子デバイス、本明細書で説明される機能を実行するように設計された他の電子ユニット、またはそれらの組合せで実装され得る。

【0129】

【0142】 ファームウェアおよび／またはソフトウェアの実装形態の場合、方法は、本明細書で説明される機能を実行する（たとえば、手順、機能などの）モジュールを用いて実装され得る。命令を有形に具現化する任意の機械可読媒体が、本明細書で説明される方法の実装に使用され得る。たとえば、ソフトウェアコードは、1つ以上のプロセッサ702に接続され、1つ以上のプロセッサ702によって実行される非一時的コンピュータ可読媒体720またはメモリ704内に記憶されていてもよい。メモリは、1つ以上のプロセッサの内部に、または1つ以上のプロセッサの外部に実装されてもよい。本明細書で使用する「メモリ」という用語は、任意のタイプの長期メモリ、短期メモリ、揮発性メモリ、不揮発性メモリ、またはその他のメモリを指し、特定のタイプのメモリもしくは特定のメモリ数に限定するものではなく、または、メモリが格納されている媒体を特定のタイプに限定するものではない。

10

【0130】

【0143】 ファームウェアおよび／またはソフトウェアで実装される場合、機能は、媒体720および／またはメモリ704などの非一時的コンピュータ可読媒体上に1つ以上の命令またはプログラムコード708として記憶されていてもよい。例は、データ構造を用いて符号化されたコンピュータ可読媒体、およびコンピュータプログラムコード708を用いて符号化されたコンピュータ可読媒体を含む。たとえば、その上に記憶されているプログラムコード708を含む非一時的コンピュータ可読媒体は、開示されている実施形態に一致する方法を用いた、現在時刻のブロードキャスト、およびUEによる現在時刻をサポートするためのプログラムコード708を含み得る。非一時的コンピュータ可読媒体720は、物理コンピュータ記憶媒体を含む。記憶媒体は、コンピュータによってアクセスされ得る任意の利用可能な媒体であり得る。限定ではなく例として、このような非一時的コンピュータ可読媒体は、RAM、ROM、EEPROM、CD-ROMまたは他の光学ディスク記憶装置、磁気ディスク記憶装置または他の磁気記憶デバイス、あるいは命令またはデータ構造の形態で所望のプログラムコード708を記憶するために使用することができ、コンピュータによってアクセスされ得る任意の他の媒体を含むことができる。本明細書で使用する「disk」および「disc」は、コンパクトディスク（Compact Disc：CD）、レーザーディスク（laser disc）、光学ディスク（optical disc）、デジタル多用途ディスク（Digital Versatile Disc：DVD）、フロッピーディスク（floppy disk）およびBlu-rayディスク（Blu-ray disc）を含むが、「disk」は通常、データを磁氣的に再生し、「disc」は、レーザーを用いてデータを光学的に再生する。上記の組合せも、コンピュータ可読媒体の範囲内に含まれるものとする。

20

30

【0131】

【0144】 コンピュータ可読媒体720上での記憶に加えて、命令および／またはデータは、通信装置内に含まれている伝送媒体上の信号として提供され得る。たとえば、通信装置は、命令およびデータを示す信号を有するトランシーバ710を含み得る。命令およびデータは、1つ以上のプロセッサに、請求項に概説されている機能を実行させるように構成される。すなわち、通信装置は、開示されている機能を実行するための情報を示す信号を持っている送信媒体を含む。

40

【0132】

【0145】 メモリ704は、任意のデータ記憶メカニズムを表し得る。メモリ704は、たとえば、1次メモリおよび／または2次メモリを含み得る。1次メモリは、たとえば、ランダムアクセスメモリ、読み取り専用メモリなどを含み得る。この例では1つ以上のプロセッサ702とは別個であるものとして示されているが、1次メモリの全部または一部が1つ以上のプロセッサ702内で提供されてもよいこと、または別様にそれと同位置に配置され／結合されてもよいことを理解されたい。2次メモリは、たとえば、1次メモリと同じかまたは類似のタイプのメモリ、および／または、たとえば、ディスクドライブ、光学ディスクドライブ、テープドライブ、ソリッドステートメモリドライブなどの1つ

50

以上のデータ記憶デバイスもしくはシステムを含み得る。

【0133】

【0146】 特定の実装形態では、2次メモリは、非一時的コンピュータ可読媒体720を動作可能に受け入れてもよく、または別様に結合するように構成可能であってもよい。したがって、特定の例示的な実装形態では、本明細書で提示されている方法および／または装置は、全体的または部分的に、その上に記憶されているコンピュータ実装可能プログラムコード708を含み得るコンピュータ可読媒体720の形態を取ってもよく、コンピュータ実装可能プログラムコードは、1つ以上のプロセッサ702によって実行されると、本明細書で説明されるような例示的な動作の全部または部分を実行するように動作可能に有効化され得る。コンピュータ可読媒体720はメモリ704の一部であり得る。

10

【0134】

【0147】 図8は、開示されている実装形態に一致する方法を用いた、図1、図3A、図3B、図4A、図4B、図5、および図6に示されるユーザ機器(UE)102などのUEによって実行される、ワイヤレスネットワークにおけるUEによる信頼できる時刻の取得をサポートするための例示的な方法800のフローチャートを示す。

【0135】

【0148】 ブロック802では、UEは、基地局(たとえば、gNB110またはng-eNB114)からブロードキャストされたメッセージを受信し、メッセージは、たとえば、図3Aのメッセージ302、図3Bのメッセージ352、図4Aのメッセージ402および403、ならびに図4Bのメッセージ452および453に示すように、現在時刻を含み、現在時刻の少なくとも一部分が暗号化される。現在時刻は、たとえば、協定世界時(UTC)時刻、全地球測位システム(GPS)時刻、GLONASS時刻、Beidou時刻、Galileo時刻、全地球航法衛星システム(GNSS)時刻、またはローカル地域時刻を含み得る。メッセージは、たとえば図2Eについて説明したように、基地局サブフレームまたはスロット境界への現在時刻の暗黙的または明示的なアライメント、現在時刻の不確実性、現在時刻のソース、またはそれらの組合せのうちの少なくとも1つをさらに含み得る。基地局からブロードキャストされたメッセージを受信するための手段であって、メッセージが現在時刻を含み、現在時刻の少なくとも一部分が暗号化される、手段が、たとえば、図6に示すように、UE600内の、ワイヤレスランシーバ610と、専用のハードウェアを備えているか、またはメモリ604および／または媒体620内の、たとえば、現在時刻モジュール622内の実行可能コードまたはソフトウェア命令を実行する1つ以上のプロセッサ602とを含み得る。

20

30

【0136】

【0149】 ブロック804では、UEは、たとえば、図2B～図2E、図3A、図3B、図4A、および図4Bにおいて説明したように、現在時刻の少なくとも一部分を解読することによって、平文の現在時刻を取得する。現在時刻の少なくとも一部分を解読することによって、平文の現在時刻を取得するための手段が、たとえば、図6に示すように、UE600内の、専用のハードウェアを備えているか、またはメモリ604および／または媒体620内の、たとえば、セキュリティモジュール624内の実行可能コードまたはソフトウェア命令を実行する1つ以上のプロセッサ602とを含み得る。

40

【0137】

【0150】 ブロック806では、UEは、たとえば、図3A、図3B、図4Aおよび図4Bにおいて説明したように、基地局とUEとの間の伝搬遅延を決定する。基地局とUEとの間の伝搬遅延を決定するための手段が、たとえば、図6に示すように、UE600内の、ワイヤレスランシーバ610と、専用のハードウェアを備えているか、またはメモリ604および／または媒体620内の、たとえば、伝搬遅延モジュール626内の実行可能コードまたはソフトウェア命令を実行する1つ以上のプロセッサ602とを含み得る。

。

【0138】

【0151】 ブロック808では、UEは、たとえば、図3A、図3B、図4Aおよび図

50

4 Bにおいて説明したように、平文の現在時刻と伝搬遅延とに基づいて、補正済み現在時刻を決定する。平文の現在時刻と伝搬遅延とに基づいて、補正済み現在時刻を決定するための手段が、たとえば、図6に示すように、UE 600内の、専用のハードウェアを備えているか、またはメモリ604および／または媒体620内の、たとえば、セキュリティモジュール624内の実行可能コードまたはソフトウェア命令を実行する1つ以上のプロセッサ602を含み得る。

【0139】

【0152】一実装形態では、たとえば、図3Aおよび図3Bで説明したように、UEは、基地局からタイミングアドバンスを取得することによって伝搬遅延を決定し得、伝搬遅延は、タイミングアドバンスから決定される（たとえば、タイミングアドバンスの値の半分として決定される）。基地局からタイミングアドバンスを取得するための手段であって、伝搬遅延がタイミングアドバンスから決定される、手段が、たとえば、図6に示すように、UE 600内の、ワイヤレスランシーバ610と、専用のハードウェアを備えているか、またはメモリ604および／または媒体620内の、たとえば、伝搬遅延モジュール626内の実行可能コードまたはソフトウェア命令を実行する1つ以上のプロセッサ602とを含み得る。

【0140】

【0153】一実装形態では、UEは、UEのロケーションおよび基地局のロケーションを取得することによって伝搬遅延を決定し得、伝搬遅延は、たとえば、図3A、図3B、図4Aおよび図4Bにおいて説明したように、UEのロケーションと基地局のロケーションとの間の距離に基づいて決定される。UEのロケーションおよび基地局のロケーションを取得するための手段であって、伝搬遅延がUEのロケーションと基地局のロケーションとの間の距離に基づいて決定される、手段が、たとえば、図6に示すように、UE 600内の、ワイヤレスランシーバ610と、専用のハードウェアを備えているか、またはメモリ604および／または媒体620内の、たとえば、伝搬遅延モジュール626内の実行可能コードまたはソフトウェア命令を実行する1つ以上のプロセッサ602とを含み得る。図3Aについて説明したように、UEは、システム情報ブロック（SIB）中の基地局のロケーションのブロードキャストを基地局から受信すること、基地局のロケーションを含むロングタームエボリューション（LTE）測位プロトコル（LPP）支援データメッセージを受信すること、UEのロケーションを含むモバイル発信ロケーション情報要求（MO-LR）応答メッセージを受信すること、または、測位セッションを実行してUEのロケーションを決定すること、のうちの少なくとも1つによって、UEのロケーションおよび基地局のロケーションを取得し得る。システム情報ブロック（SIB）中の基地局のロケーションのブロードキャストを基地局から受信するための手段が、たとえば、図6に示すように、UE 600内の、ワイヤレスランシーバ610と、専用のハードウェアを備えているか、またはメモリ604および／または媒体620内の、たとえば、測位セッションモジュール628内の実行可能コードまたはソフトウェア命令を実行する1つ以上のプロセッサ602とを含み得る。基地局のロケーションを含むロングタームエボリューション（LTE）測位プロトコル（LPP）支援データメッセージを受信するための手段が、たとえば、図6に示すように、UE 600内の、ワイヤレスランシーバ610と、専用のハードウェアを備えているか、またはメモリ604および／または媒体620内の、たとえば、測位セッションモジュール628内の実行可能コードまたはソフトウェア命令を実行する1つ以上のプロセッサ602とを含み得る。UEのロケーションを含むモバイル発信ロケーション情報要求（MO-LR）応答メッセージを受信するための手段が、たとえば、図6に示すように、UE 600内の、ワイヤレスランシーバ610と、専用のハードウェアを備えているか、またはメモリ6

10

20

30

40

50

04 および／または媒体 620 内の、たとえば、測位セッションモジュール 628 内の実行可能コードまたはソフトウェア命令を実行する 1 つ以上のプロセッサ 602 とを含み得る。

【0141】

【0154】 一実装形態では、UE は、UE と基地局との間の往復伝搬時間 (RTT) を測定することによって伝搬遅延を決定し得、伝搬遅延は、たとえば、図 3A、図 3B、図 4A および図 4B において説明したように、RTT の半分に等しい。UE と基地局との間の往復伝搬時間 (RTT) を測定するための手段であって、伝搬遅延が RTT の半分に等しい、手段が、たとえば、図 6 に示すように、UE 600 内の、ワイヤレストランシーバ 610 と、専用のハードウェアを備えているか、またはメモリ 604 および／または媒体 620 内の、たとえば、伝搬遅延モジュール 626 内の実行可能コードまたはソフトウェア命令を実行する 1 つ以上のプロセッサ 602 とを含み得る。

10

【0142】

【0155】 一実装形態では、UE は、たとえば、図 3B 中のメッセージ 354 および図 4B 中のメッセージ 455 によって示されるように、基地局用の第 1 のローカル送信時刻を示す第 1 のメッセージを基地局から受信することによって、RTT を測定し得る。基地局用の第 1 のローカル送信時刻を示す第 1 のメッセージを基地局から受信するための手段が、たとえば、図 6 に示すように、UE 600 内の、ワイヤレストランシーバ 610 と、専用のハードウェアを備えているか、またはメモリ 604 および／または媒体 620 内の、たとえば、伝搬遅延モジュール 626 内の実行可能コードまたはソフトウェア命令を実行する 1 つ以上のプロセッサ 602 とを含み得る。UE は、たとえば、図 3B および図 4B において説明したように、基地局用の第 1 のローカル送信時刻と、UE における第 1 のメッセージの受信のローカル時刻とに基づいて、UE におけるローカルタイミングを基地局用のローカル送信時刻に関連付け得る。基地局用の第 1 のローカル送信時刻と、UE における第 1 のメッセージの受信のローカル時刻とに基づいて、UE におけるローカルタイミングを基地局用のローカル送信時刻に関連付けるための手段が、たとえば、図 6 に示すように、UE 600 内の、ワイヤレストランシーバ 610 と、専用のハードウェアを備えているか、またはメモリ 604 および／または媒体 620 内の、たとえば、伝搬遅延モジュール 626 内の実行可能コードまたはソフトウェア命令を実行する 1 つ以上のプロセッサ 602 とを含み得る。UE は、ランダムアクセスチャネル (RACH) 上で基地局に第 2 のメッセージを送信し得、第 2 のメッセージはランダム変数を含み、第 2 のメッセージは第 1 の時刻に送信され、第 1 の時刻は、たとえば、図 3B 中のメッセージ 356 および図 4B 中のメッセージ 456 によって示されるように、UE におけるローカル時刻または基地局用の関連付けられたローカル送信時刻のいずれか一方である。ランダムアクセスチャネル (RACH) 上で基地局に第 2 のメッセージを送信するための手段であって、第 2 のメッセージがランダム変数を含み、第 2 のメッセージが第 1 の時刻に送信され、第 1 の時刻が UE におけるローカル時刻または基地局用の関連付けられたローカル送信時刻のいずれか一方である、手段が、たとえば、図 6 に示すように、UE 600 内の、ワイヤレストランシーバ 610 と、専用のハードウェアを備えているか、またはメモリ 604 および／または媒体 620 内の、たとえば、伝搬遅延モジュール 626 内の実行可能コードまたはソフトウェア命令を実行する 1 つ以上のプロセッサ 602 とを含み得る。UE は、第 2 のメッセージに応答して基地局から第 3 のメッセージを受信し得、第 3 のメッセージは第 2 の時刻とランダム変数とを含み、第 2 の時刻は、たとえば、図 3B 中のメッセージ 358 および図 4B 中のメッセージ 459 によって示されるように、第 2 のメッセージが基地局において受信された基地局用のローカル送信時刻である。第 2 のメッセージに応答して基地局から第 3 のメッセージを受信するための手段であって、第 3 のメッセージが第 2 の時刻とランダム変数とを含み、第 2 の時刻が、第 2 のメッセージが基地局において受信された基地局用のローカル送信時刻である、手段が、たとえば、図 6 に示すように、UE 600 内の、ワイヤレストランシーバ 610 と、専用のハードウェアを備えているか、またはメモリ 604 および／または媒体 620 内の、たとえば、伝搬遅延モジュール 626 内

20

30

40

50

の実行可能コードまたはソフトウェア命令を実行する1つ以上のプロセッサ602とを含み得る。UEは、たとえば、図3Bおよび図4Bにおいて説明したように、第1の時刻と第2の時刻とに基づいてRTTを決定し得る。第1の時刻と第2の時刻とに基づいてRTTを決定するための手段が、たとえば、図6に示すように、UE600内の、ワイヤレストランシーバ610と、専用のハードウェアを備えているか、またはメモリ604および／または媒体620内の、たとえば、伝搬遅延モジュール626内の実行可能コードまたはソフトウェア命令を実行する1つ以上のプロセッサ602とを含み得る。

【0143】

【0156】いくつかの実装形態では、第3のメッセージは、たとえば、図3Bおよび図4Bで説明したように、暗号化され得る。第3のメッセージは、基地局用のデジタル署名をさらに含み得、UEは、たとえば、図3Bおよび図4Bにおいて説明したように、基地局用のデジタル署名に基づいて第3のメッセージを認証し得る。基地局用のデジタル署名に基づいて第3のメッセージを認証するための手段が、たとえば、図6に示すように、UE600内の、専用のハードウェアを備えているか、またはメモリ604および／または媒体620内の、たとえば、セキュリティモジュール624内の実行可能コードまたはソフトウェア命令を実行する1つ以上のプロセッサ602を含み得る。

【0144】

【0157】攻撃デバイスが、UEと基地局との間のワイヤレスネットワーク内に存在し得、メッセージが、たとえば、図4A、図4B、および図5に示すように、リプレイ攻撃中に攻撃デバイスを介して受信される。UEは、タイミングアドバンスから、または（前に説明したように）RTTを測定することによって伝搬遅延を決定し得、たとえば、図4Bおよび図5において説明したように、伝搬遅延が予想範囲外であることに基づいて攻撃デバイスの存在を検出し得る。タイミングアドバンスから、またはRTTを測定することによって伝搬遅延を決定するための手段が、たとえば、図6に示すように、UE600内の、専用のハードウェアを備えているか、またはメモリ604および／または媒体620内の、たとえば、伝搬遅延モジュール626内の実行可能コードまたはソフトウェア命令を実行する1つ以上のプロセッサ602を含み得る。伝搬遅延が予想範囲外であることに基づいて攻撃デバイスの存在を検出するための手段が、たとえば、図6に示すように、UE600内の、専用のハードウェアを備えているか、またはメモリ604および／または媒体620内の、たとえば、攻撃検出モジュール630内の実行可能コードまたはソフトウェア命令を実行する1つ以上のプロセッサ602を含み得る。予想範囲は、たとえば、基地局への最大予想距離に基づく最大伝搬遅延を含み得る。UEは、たとえば、図5の段階1において説明したように、UEの推定ロケーションおよび基地局のロケーションを取得し得る。UEは、たとえば、図5の段階1において説明したように、UEの推定ロケーションと基地局のロケーションとの間の距離推定値を決定し得る。UEは、たとえば、図5の段階1において説明したように、距離推定値に基づいて予想範囲を決定し得る。UEの推定ロケーションおよび基地局のロケーションを取得するための手段が、たとえば、図6に示すように、UE600内の、ワイヤレストランシーバ610と、専用のハードウェアを備えているか、またはメモリ604および／または媒体620内の、たとえば、測位セッションモジュール628内の実行可能コードまたはソフトウェア命令を実行する1つ以上のプロセッサ602とを含み得る。UEの推定ロケーションと基地局のロケーションとの間の距離推定値を決定するための手段が、たとえば、図6に示すように、UE600内の、ワイヤレストランシーバ610と、専用のハードウェアを備えているか、またはメモリ604および／または媒体620内の、たとえば、伝搬遅延モジュール626内の実行可能コードまたはソフトウェア命令を実行する1つ以上のプロセッサ602とを含み得る。距離推定値に基づいて予想範囲を決定するための手段が、たとえば、図6に示すように、UE600内の、ワイヤレストランシーバ610と、専用のハードウェアを備えているか、またはメモリ604および／または媒体620内の、たとえば、伝搬遅延モジュール626内の実行可能コードまたはソフトウェア命令を実行する1つ以上のプロセッサ602とを含み得る。

10

20

30

40

50

【0145】

【0158】 一実装形態では、メッセージは、たとえば、図3Aのメッセージ302、図3Bのメッセージ352、図4Aのメッセージ402、ならびに図4Bのメッセージ452および453に示すように、基地局用のデジタル署名をさらに含む。UEは、たとえば、図3Bにおいて説明したように、基地局用のデジタル署名に基づいてメッセージ中の現在時刻を認証し得る。基地局用のデジタル署名に基づいてメッセージ中の現在時刻を認証するための手段が、たとえば、図6に示すように、UE600内の、専用のハードウェアを備えているか、またはメモリ604および／または媒体620内の、たとえば、セキュリティモジュール624内の実行可能コードまたはソフトウェア命令を実行する1つ以上のプロセッサ602を含み得る。UEは、たとえば、ワイヤレスネットワークから基地局用の公開暗号化鍵を受信し得、デジタル署名は、公開暗号化鍵に対応する秘密暗号化鍵に基づくものであり、現在時刻を認証することは、たとえば、図3A、図3B、図4A、および図4Bにおいて説明したように、公開暗号化鍵を使用する。ワイヤレスネットワークから基地局用の公開暗号化鍵を受信するための手段であって、デジタル署名が公開暗号化鍵に対応する秘密暗号化鍵に基づくものであり、現在時刻を認証することが公開暗号化鍵を使用する、手段が、たとえば、図6に示すように、UE600内の、専用のハードウェアを備えているか、またはメモリ604および／または媒体620内の、たとえば、セキュリティモジュール624内の実行可能コードまたはソフトウェア命令を実行する1つ以上のプロセッサ602を含み得る。

10

【0146】

20

【0159】 図9は、開示されている実装形態に一致する方法を用いた、図1、図3A、図3B、図4A、図4B、図5、および図7に示されるgNB110などの基地局によって実行される、ワイヤレスネットワークにおけるユーザ機器（UE）による信頼できる時刻の取得をサポートするための例示的な方法900のフローチャートを示す。

【0147】

【0160】 ブロック902では、基地局は、たとえば、図1および図3Aに関連して説明したように、現在時刻を取得し得る。現在時刻は、たとえば、協定世界時（UTC）時刻、全地球測位システム（GPS）時刻、GLONASS時刻、Beidou時刻、Galileo時刻、全地球航法衛星システム（GNSS）時刻、またはローカル地域時刻を含み得る。現在時刻を取得するための手段が、たとえば、SPS受信機715もしくは外部トランシーバ716と、図7に示すように、基地局700内の、専用のハードウェアを備えているか、またはメモリ704および／または媒体720内の、たとえば、現在時刻モジュール722内の実行可能コードまたはソフトウェア命令を実行する1つ以上のプロセッサ702を含み得る。

30

【0148】

【0161】 ブロック904では、基地局は、たとえば、図3Aのメッセージ302および図3Bのメッセージ352について説明したように、現在時刻の少なくとも一部分を暗号化する。現在時刻の少なくとも一部分を暗号化するための手段が、たとえば、図7に示すように、基地局700内の、専用のハードウェアを備えているか、またはメモリ704および／または媒体720内の、たとえば、セキュリティモジュール724内の実行可能コードまたはソフトウェア命令を実行する1つ以上のプロセッサ702を含み得る。

40

【0149】

【0162】 ブロック906では、基地局は、現在時刻を含むメッセージをブロードキャストし、UEは、メッセージを受信し、現在時刻の少なくとも一部分を解読することによって平文の現在時刻を取得し、かつ基地局とUEとの間の伝搬遅延を決定し、UEは、たとえば、図3Aのメッセージ302、図3Bのメッセージ352、図4Aのメッセージ402、および図4Bのメッセージ452について説明したように、平文の現在時刻と伝搬遅延とに基づいて補正済み現在時刻を決定する。いくつかの実装形態では、基地局は、基地局用のサブフレームまたはスロット境界への現在時刻の暗黙的または明示的なアライメント、現在時刻の不確実性、現在時刻の取得元となるソース、またはそれらの組合せのう

50

ちの少なくとも1つをメッセージ中に含め得る。現在時刻を含むメッセージをブロードキャストするための手段、および基地局用のサブフレームまたはスロット境界への現在時刻のアライメント、現在時刻の不確実性、現在時刻の取得元となるソース、またはそれらの組合せのうちの少なくとも1つをメッセージ中に含めるための手段が、たとえば、図7に示すように、基地局700内の、トランシーバ710と、専用のハードウェアを備えているか、またはメモリ704および／または媒体720内の、たとえば、現在時刻モジュール722内の実行可能コードまたはソフトウェア命令を実行する1つ以上のプロセッサ702とを含み得る。

【0150】

【0163】一実装形態では、基地局は、タイミングアドバンスをUEに送信することによって伝搬遅延の決定においてUEを支援し得、タイミングアドバンスは、たとえば、図3Aおよび図4Aで説明したように、UEによる伝搬遅延の決定を可能にする（たとえば、伝搬遅延がタイミングアドバンスの半分として取得される）。タイミングアドバンスをUEに送信するための手段であって、タイミングアドバンスがUEによる伝搬遅延の決定を可能にする、手段が、たとえば、図7に示すように、基地局700内の、トランシーバ710と、専用のハードウェアを備えているか、またはメモリ704および／または媒体720内の、たとえば、伝搬遅延モジュール726内の実行可能コードまたはソフトウェア命令を実行する1つ以上のプロセッサ702とを含み得る。

【0151】

【0164】一実装形態では、基地局は、UEのロケーションと基地局のロケーションとのうちの少なくとも一方を含むメッセージをUEに送信することによって、伝搬遅延の決定においてUEを支援し得、伝搬遅延は、たとえば、図3Aについて説明したように、UEのロケーションと基地局のロケーションとの間の距離に基づいてUEによって決定される。UEのロケーションと基地局のロケーションとのうちの少なくとも一方を含むメッセージをUEに送信するための手段であって、伝搬遅延が、UEのロケーションと基地局のロケーションとの間の距離に基づいてUEによって決定される、手段が、たとえば、図7に示すように、基地局700内の、トランシーバ710と、専用のハードウェアを備えているか、またはメモリ704および／または媒体720内の、たとえば、伝搬遅延モジュール726内の実行可能コードまたはソフトウェア命令を実行する1つ以上のプロセッサ702とを含み得る。図3Aについて説明したように、基地局は、たとえば、システム情報ブロック（SIB）中の基地局のロケーションをブロードキャストすること、基地局のロケーションを含むロングタームエボリューション（LTE）測位プロトコル（LPP）支援データメッセージをUEに転送すること、UEのロケーションを含むモバイル発信ロケーション情報要求（MO-LR）応答メッセージをUEに送信すること、または、UEとUE用のロケーションサーバ（たとえば、LMF152またはSLP162）との間でLPPメッセージを転達して、UEのロケーションを決定すること、あるいはそれらの任意の組合せによって、UEのロケーションと基地局のロケーションとのうちの少なくとも一方を含むメッセージをUEに送り得る。システム情報ブロック（SIB）中の基地局のロケーションをブロードキャストするための手段が、たとえば、図7に示すように、基地局700内の、トランシーバ710と、専用のハードウェアを備えているか、またはメモリ704および／または媒体720内の、たとえば、測位セッションモジュール728内の実行可能コードまたはソフトウェア命令を実行する1つ以上のプロセッサ702とを含み得る。基地局のロケーションを含むロングタームエボリューション（LTE）測位プロトコル（LPP）支援データメッセージをUEに転送するための手段が、たとえば、図7に示すように、基地局700内の、トランシーバ710と、専用のハードウェアを備えているか、

10

20

30

40

50

、またはメモリ 704 および／または媒体 720 内の、たとえば、測位セッションモジュール 728 内の実行可能コードまたはソフトウェア命令を実行する 1 つ以上のプロセッサ 702 とを含み得る。UE と UE 用のロケーションサーバとの間で LPP メッセージを転達して、UE のロケーションを決定するための手段が、たとえば、図 7 に示すように、基地局 700 内の、トランシーバ 710 と、専用のハードウェアを備えているか、またはメモリ 704 および／または媒体 720 内の、たとえば、測位セッションモジュール 728 内の実行可能コードまたはソフトウェア命令を実行する 1 つ以上のプロセッサ 702 とを含み得る。

【0152】

【0165】一実装形態では、基地局は、UE と基地局との間の往復伝搬時間 (RTT) の測定において UE を支援することによって、伝搬遅延の決定において UE を支援し得、伝搬遅延は、たとえば、図 3 B および図 4 B において説明したように、RTT の半分に等しい。UE と基地局との間の往復伝搬時間 (RTT) の測定において UE を支援するための手段であって、伝搬遅延が RTT の半分に等しい、手段が、たとえば、図 7 に示すように、基地局 700 内の、トランシーバ 710 と、専用のハードウェアを備えているか、またはメモリ 704 および／または媒体 720 内の、たとえば、伝搬遅延モジュール 726 内の実行可能コードまたはソフトウェア命令を実行する 1 つ以上のプロセッサ 702 とを含み得る。

【0153】

【0166】一実装形態では、基地局は、基地局用の第 1 のローカル送信時刻を示す第 1 のメッセージを UE に送信することによって、RTT の測定において UE を支援し得、UE は、たとえば、図 3 B 中のメッセージ 354 および図 4 B 中のメッセージ 454 によって示されるように、基地局用の第 1 のローカル送信時刻と UE における第 1 のメッセージの受信のローカル時刻とに基づいて、UE におけるローカルタイミングを基地局用のローカル送信時刻に関連付ける。基地局用の第 1 のローカル送信時刻を示す第 1 のメッセージを UE に送信するための手段であって、UE が、基地局用の第 1 のローカル送信時刻と UE における第 1 のメッセージの受信のローカル時刻とに基づいて、UE におけるローカルタイミングを基地局用のローカル送信時刻に関連付ける、手段が、たとえば、図 7 に示すように、基地局 700 内の、トランシーバ 710 と、専用のハードウェアを備えているか、またはメモリ 704 および／または媒体 720 内の、たとえば、伝搬遅延モジュール 726 内の実行可能コードまたはソフトウェア命令を実行する 1 つ以上のプロセッサ 702 とを含み得る。基地局は、ランダムアクセスチャネル (RACH) 上で UE から第 2 のメッセージを受信し得、第 2 のメッセージはランダム変数を含み、第 2 のメッセージは第 1 の時刻に送信され、第 1 の時刻は、たとえば、図 3 B 中のメッセージ 356 および図 4 B 中のメッセージ 457 によって示されるように、UE におけるローカル時刻または基地局用の関連付けられたローカル送信時刻のいずれか一方である。ランダムアクセスチャネル (RACH) 上で UE から第 2 のメッセージを受信するための手段であって、第 2 のメッセージがランダム変数を含み、第 2 のメッセージが第 1 の時刻に送信され、第 1 の時刻が UE 内のローカル時刻または基地局用の関連付けられたローカル送信時刻のいずれか一方である、手段が、たとえば、図 7 に示すように、基地局 700 内の、トランシーバ 710 と、専用のハードウェアを備えているか、またはメモリ 704 および／または媒体 720 内の、たとえば、伝搬遅延モジュール 726 内の実行可能コードまたはソフトウェア命令を実行する 1 つ以上のプロセッサ 702 とを含み得る。基地局は、第 2 の時刻を測定することができ、第 2 の時刻は、たとえば、図 3 B 中のメッセージ 356 および図 4 B 中のメッセージ 457 によって示されるように、第 2 のメッセージが基地局において受信された基地局用のローカル送信時刻である。第 2 の時刻を測定するための手段であって、第 2 の時刻が、基地局において第 2 のメッセージが受信された基地局用のローカル送信時刻である、手段が、たとえば、図 7 に示すように、基地局 700 内の、トランシーバ 710 と、専用のハードウェアを備えているか、またはメモリ 704 および／または媒体 720 内の、たとえば、伝搬遅延モジュール 726 内の実行可能コードまたはソフトウェア命令を実

10

20

30

40

50

行する1つ以上のプロセッサ702とを含み得る。基地局は、第2のメッセージに応答して第3のメッセージをUEに送り得、第3のメッセージは第2の時刻とランダム変数とを含み、UEは、たとえば、図3B中のメッセージ358ならびに図4B中のメッセージ458および459によって示されるように、第1の時刻と第2の時刻とに基づいてRTTを決定する。第2のメッセージに応答して第3のメッセージをUEに送信するための手段であって、第3のメッセージが第2の時刻とランダム変数とを含む、手段が、たとえば、図7に示すように、基地局700内の、トランシーバ710と、専用のハードウェアを備えているか、またはメモリ704および／または媒体720内の、たとえば、伝搬遅延モジュール726内の実行可能コードまたはソフトウェア命令を実行する1つ以上のプロセッサ702とを含み得る。

10

【0154】

【0167】 いくつかの実装形態では、基地局は、たとえば、図3Bおよび図4Bで説明したように、第3のメッセージを暗号化し得る。第3のメッセージを暗号化するための手段が、たとえば、図7に示すように、基地局700内の、トランシーバ710と、専用のハードウェアを備えているか、またはメモリ704および／または媒体720内の、たとえば、セキュリティモジュール724内の実行可能コードまたはソフトウェア命令を実行する1つ以上のプロセッサ702とを含み得る。基地局は、基地局用のデジタル署名を第3のメッセージ中に含め得、UEは、たとえば、図3Bおよび図4Bにおいて説明したように、基地局用のデジタル署名に基づいて第3のメッセージを認証する。基地局用のデジタル署名を第3のメッセージ中に含めるための手段であって、UEが基地局用のデジタル署名に基づいて第3のメッセージを認証する、手段が、たとえば、図7に示すように、基地局700内の、トランシーバ710と、専用のハードウェアを備えているか、またはメモリ704および／または媒体720内の、たとえば、セキュリティモジュール724内の実行可能コードまたはソフトウェア命令を実行する1つ以上のプロセッサ702とを含み得る。

20

【0155】

【0168】 いくつかの実装形態では、攻撃デバイスが、UEと基地局との間のワイヤレスネットワーク内に存在し得、メッセージが、たとえば、図4Aおよび図4Bに示すように、リプレイ攻撃中に攻撃デバイスを介してUEによって受信される。UEは、タイミグアドバンスから、または（上記のように）RTTを測定することによって伝搬遅延を決定し得、たとえば、図4Bおよび図5に示すように、伝搬遅延が予想範囲外であることに基づいて、攻撃デバイスの存在を検出し得る。予想範囲は、たとえば、UEと基地局との間の最大予想距離に基づく最大伝搬遅延であり得る。予想範囲は、たとえば、UEの推定ロケーションと、UEによって取得された基地局のロケーションとに基づき得る。

30

【0156】

【0169】 一実装形態では、基地局は、基地局用のデジタル署名をメッセージ中に含め得、UEは、たとえば、図3Aのメッセージ302、図3Bのメッセージ352、図4Aのメッセージ402、ならびに図4Bのメッセージ452および453に示すように、基地局用のデジタル署名に基づいてメッセージ中の現在時刻を認証する。基地局用のデジタル署名をメッセージ中に含めるための手段であって、UEが基地局用のデジタル署名に基づいてメッセージ中の現在時刻を認証する、手段が、たとえば、図7に示すように、基地局700内の、トランシーバ710と、専用のハードウェアを備えているか、またはメモリ704および／または媒体720内の、たとえば、現在時刻モジュール722内の実行可能コードまたはソフトウェア命令を実行する1つ以上のプロセッサ702とを含み得る。基地局は、基地局用の公開暗号化鍵をUEに送り得、デジタル署名は、公開暗号化鍵に対応する秘密暗号化鍵に基づくものであり、UEは、たとえば、図3Aおよび図3Bで説明したように、公開暗号化鍵を使用して現在時刻を認証する。基地局用の公開暗号化鍵をUEに送信するための手段であって、デジタル署名が公開暗号化鍵に対応する秘密暗号化鍵に基づくものであり、UEが公開暗号化鍵を使用して現在時刻を認証する、手段が、たとえば、図7に示すように、基地局700内の、トランシーバ710と、専用のハードウ

40

50

エアを備えているか、またはメモリ 704 および／または媒体 720 内の、たとえば、セキュリティモジュール 724 内の実行可能コードまたはソフトウェア命令を実行する 1 つ以上のプロセッサ 702 とを含み得る。

【0157】

【0170】 本明細書全体にわたる「一例」、「ある例」、「特定の例」、または「例示的な実装形態」への言及は、特徴および／または例について説明した特定の特徴、構造、または特性が、特許請求される主題の少なくとも 1 つの特徴および／または例に含まれることを意味する。したがって、本明細書全体にわたる様々な場所における「一例では」、「ある例」、「特定の例では」、もしくは「特定の实装形態では」という句または他の同様の句の出現は、必ずしもすべてが同じ特徴、例、および／または限定に言及しているとは限らない。さらに、特定の特徴、構造、または特性が、1 つ以上の例および／または特徴において組み合わせられてもよい。

10

【0158】

【0171】 本明細書に含まれる詳細な説明のいくつかの部分は、特定の装置または専用コンピューティングデバイスもしくはプラットフォームのメモリに記憶されている 2 値デジタル信号に対する動作のアルゴリズムまたは記号表現に関して提示される。この特定の明細書の文脈では、特定の装置などという用語は、プログラムされるとプログラムソフトウェアからの命令に従って特定の動作を実行する、汎用コンピュータを含む。アルゴリズムによる説明または記号表現は、信号処理または関連技術の当業者が、自身の仕事の本質を他の当業者に伝えるために使用する技法の例である。ここでいうアルゴリズムとは、一般的には、所望の結果をもたらす自己矛盾のない一連の演算または同様の信号処理であると考えられる。この文脈では、演算または処理は物理数量の物理的操作を伴う。必ずしもそうとは限らないが、通常、このような数量は、記憶、転達、合成、比較、または別様に操作することが可能な電気信号または磁気信号の形態を取ることがある。主に一般的な用法上、このような信号をビット、データ、値、要素、シンボル、文字、用語、数字、数値などと呼ぶことが、時として好都合であることが分かっている。しかしながら、これらまたは類似の用語のすべてが便宜的なラベルにすぎず、適切な物理数量と関連付けなければならないことを理解されたい。別段に明記されていない限り、本明細書の議論から明らかなように、本明細書全体にわたって、「処理する」、「コンピューティングする」、「算出する」、「決定する」などの用語を利用する議論は、専用コンピュータ、専用コンピューティング装置または同様の専用電子コンピューティングデバイスなどの特定の装置のアクションまたはプロセスを指すことを理解されたい。したがって、本明細書の文脈では、専用コンピュータまたは同様の専用電子コンピューティングデバイスは通常、専用コンピュータまたは同様の専用電子コンピューティングデバイスのメモリ、レジスタ、もしくは他の情報記憶デバイス、送信デバイス、またはディスプレイデバイス内の物理的な電子量または磁気量として表される信号を操作または変換することが可能である。

20

30

【0159】

【0172】 上述の詳細な説明では、特許請求される主題の完全な理解を与えるために多数の具体的な詳細が記載されている。しかしながら、特許請求される主題がこれらの具体的な詳細なしに実践され得ることが、当業者によって理解されよう。他の場合には、特許請求される主題を不明瞭にしないように、当業者によって知られているであろう方法および装置は、詳細には説明されていない。

40

【0160】

【0173】 本明細書で使用される「および」、「または」、および「および／または」という用語は、このような用語が使用される文脈に少なくとも部分的に依存することも想定される、様々な意味を含み得る。通常、「または」が、A、B または C などの列挙を関連付けるために使用される場合、ここでは、A、B、および C という包括的な意味で使われる、ならびに、ここでは、A、B、または C という排他的な意味で使われることが意図されている。加えて、本明細書で使用される「1 つ以上の」という用語は、単数の任意の特徴、構造、もしくは特性を説明するために使用されることがあり、あるいは、複数

50

の特徴、構造、もしくは特性、または特徴、構造、もしくは特性の何らかの他の組合せを説明するために使用されることがある。とはいえ、これは例示にすぎず、特許請求される主題がこの例に限定されないことに留意されたい。

【0161】

【0174】 現時点で例示的な特徴であると見なされているものが例示および説明されているが、特許請求される主題から逸脱することなく、様々な他の修正を加えるのも、等価物で置き換えるのも可能であることは、当業者によって理解されよう。加えて、本明細書で説明される中心概念から逸脱することなく、特許請求される主題の教示に特定の状況を適合させるために、多くの修正を加え得る。

【0162】

【0175】 本明細書に鑑みて、実施形態は特徴の様々な組合せを含んでもよい。以下の番号付きの条項において、実装例について説明する。

【0163】

【0176】 条項1。ワイヤレスネットワークにおける時刻の取得をサポートするためにユーザ機器（UE）によって実行される方法であって、基地局からブロードキャストされたメッセージを受信することであって、メッセージが現在時刻を含み、現在時刻の少なくとも一部分が暗号化される、受信することと、現在時刻の少なくとも一部分を解読することによって、平文の現在時刻を取得することと、基地局とUEとの間の伝搬遅延を決定することと、平文の現在時刻と伝搬遅延とに基づいて、補正済み現在時刻を決定することとを含む、方法。

【0164】

【0177】 条項2。現在時刻が、協定世界時（UTC）時刻、全地球測位システム（GPS）時刻、GLONASS時刻、Beidou時刻、Galileo時刻、全地球航行衛星システム（GNSS）時刻、またはローカル地域時刻を含む、条項1に記載の方法。

【0165】

【0178】 条項3。伝搬遅延を決定することが、基地局からタイミングアドバンスを取得することであって、伝搬遅延がタイミングアドバンスから決定される、取得すること、UEのロケーションおよび基地局のロケーションを取得することであって、伝搬遅延が、UEのロケーションと基地局のロケーションとの間の距離に基づいて決定される、取得すること、または、UEと基地局との間の往復伝搬時間（RTT）を測定することであって、伝搬遅延がRTTの半分に等しい、測定すること、のうちの1つを含む、条項1または2のいずれか一項に記載の方法。

【0166】

【0179】 条項4。UEのロケーションおよび基地局のロケーションを取得することが、システム情報ブロック（SIB）中の基地局のロケーションのブロードキャストを基地局から受信すること、基地局のロケーションを含むロングタームエボリューション（LTE）測位プロトコル（LPP）支援データメッセージを受信すること、UEのロケーションを含むモバイル発信ロケーション情報要求（MO-LR）応答メッセージを受信すること、または、測位セッションを実行してUEのロケーションを決定すること、のうちの少なくとも1つを含む、条項3に記載の方法。

【0167】

【0180】 条項5。RTTを測定することが、基地局用の第1のローカル送信時刻を示す第1のメッセージを基地局から受信することと、基地局用の第1のローカル送信時刻とUEにおける第1のメッセージの受信のローカル時刻とに基づいて、UEにおけるローカルタイミングを基地局用のローカル送信時刻に関連付けることと、ランダムアクセスチャネル（RACH）上で基地局に第2のメッセージを送信することであって、第2のメッセージがランダム変数を含み、第2のメッセージが第1の時刻に送信され、第1の時刻がUEにおけるローカル時刻または基地局用の関連付けられたローカル送信時刻のいずれか一方である、送信することと、第2のメッセージに応答して基地局から第3のメッセージを受信することであって、第3のメッセージが第2の時刻とランダム変数とを含み、第2の

時刻が、第 2 のメッセージが基地局において受信された基地局用のローカル送信時刻である、受信することと、第 1 の時刻と第 2 の時刻とに基づいて R T T を決定することと、を含む、条項 3 または 4 のいずれか一項に記載の方法。

【0168】

【0181】 条項 6。第 3 のメッセージが暗号化される、条項 5 に記載の方法。

【0169】

【0182】 条項 7。第 3 のメッセージが、基地局用のデジタル署名をさらに含み、方法が、基地局用のデジタル署名に基づいて第 3 のメッセージを認証することをさらに含む、条項 5 または 6 のいずれか一項に記載の方法。

【0170】

【0183】 条項 8。攻撃デバイスが、U E と基地局との間のワイヤレスネットワーク内に存在し、メッセージが、リプレイ攻撃中に攻撃デバイスを介して受信され、方法が、タイミングアドバンスから、または R T T を測定することによって伝搬遅延を決定することと、伝搬遅延が予想範囲外であることに基づいて攻撃デバイスの存在を検出することと、をさらに含む、条項 3 ～ 7 のいずれか一項に記載の方法。

【0171】

【0184】 条項 9。予想範囲が、基地局への最大予想距離に基づく最大伝搬遅延を含む、条項 8 に記載の方法。

【0172】

【0185】 条項 10。U E の推定ロケーションおよび基地局のロケーションを取得することと、U E の推定ロケーションと基地局のロケーションとの間の距離推定値を決定することと、距離推定値に基づいて予想範囲を決定することと、をさらに含む、条項 8 または 9 のいずれか一項に記載の方法。

【0173】

【0186】 条項 11。メッセージが、基地局サブフレームまたはスロット境界への現在時刻の暗黙的または明示的なアライメント、現在時刻の不確実性、現在時刻のソース、またはそれらの組合せのうちの少なくとも 1 つをさらに含む、条項 1 ～ 10 のいずれか一項に記載の方法。

【0174】

【0187】 条項 12。メッセージが、基地局用のデジタル署名をさらに含み、方法が、基地局用のデジタル署名に基づいて、メッセージ中の現在時刻を認証することをさらに含む、条項 1 ～ 11 のいずれか一項に記載の方法。

【0175】

【0188】 条項 13。ワイヤレスネットワークから基地局用の公開暗号化鍵を受信することであって、デジタル署名が、公開暗号化鍵に対応する秘密暗号化鍵に基づくものであり、現在時刻を認証することが、公開暗号化鍵を使用する、受信することをさらに含む、条項 12 に記載の方法。

【0176】

【0189】 条項 14。ワイヤレスネットワークにおける時刻の取得をサポートするように構成されたユーザ機器（U E）であって、ワイヤレスネットワーク内の基地局とワイヤレス通信するように構成されたワイヤレストランシーバと、少なくとも 1 つのメモリと、ワイヤレストランシーバおよび少なくとも 1 つのメモリに結合された少なくとも 1 つのプロセッサと、を備え、少なくとも 1 つのプロセッサが、ワイヤレストランシーバを介して、基地局からブロードキャストされたメッセージを受信し、メッセージが現在時刻を含み、現在時刻の少なくとも一部分が暗号化され、現在時刻の少なくとも一部分を解読することによって、平文の現在時刻を取得し、基地局と U E との間の伝搬遅延を決定し、平文の現在時刻と伝搬遅延とに基づいて、補正済み現在時刻を決定する、ように構成される、ユーザ機器（U E）。

【0177】

【0190】 条項 15。現在時刻が、協定世界時（U T C）時刻、全地球測位システム（

10

20

30

40

50

G P S) 時刻、G L O N A S S 時刻、B e i d o u 時刻、G a l i l e o 時刻、全地球航法衛星システム (G N S S) 時刻、またはローカル地域時刻を含む、条項 1 4 に記載の U E 。

【 0 1 7 8 】

【 0 1 9 1 】 条項 1 6 。少なくとも 1 つのプロセッサが、ワイヤレスランシーバを介して、基地局からタイミングアドバンスを取得することであって、伝搬遅延がタイミングアドバンスから決定される、取得すること、U E のロケーションおよび基地局のロケーションを取得することであって、伝搬遅延が、U E のロケーションと基地局のロケーションとの間の距離に基づいて決定される、取得すること、または、U E と基地局との間の往復伝搬時間 (R T T) を測定することであって、伝搬遅延が R T T の半分に等しい、測定すること、のうちの 1 つによって、伝搬遅延を決定するように構成される、条項 1 4 または 1 5 のいずれか一項に記載の U E 。

10

【 0 1 7 9 】

【 0 1 9 2 】 条項 1 7 。少なくとも 1 つのプロセッサが、ワイヤレスランシーバを介して、システム情報ブロック (S I B) 中の基地局のロケーションのブロードキャストを基地局から受信すること、ワイヤレスランシーバを介して、基地局のロケーションを含むロングタームエボリューション (L T E) 測位プロトコル (L P P) 支援データメッセージを受信すること、ワイヤレスランシーバを介して、U E のロケーションを含むモバイル発信ロケーション情報要求 (M O - L R) 応答メッセージを受信すること、または、測位セッションを実行して U E のロケーションを決定すること、のうちの少なくとも 1 つによって、U E のロケーションおよび基地局のロケーションを取得するように構成される、条項 1 6 に記載の U E 。

20

【 0 1 8 0 】

【 0 1 9 3 】 条項 1 8 。少なくとも 1 つのプロセッサが、ワイヤレスランシーバを介して、基地局用の第 1 のローカル送信時刻を示す第 1 のメッセージを基地局から受信し、基地局用の第 1 のローカル送信時刻と U E における第 1 のメッセージの受信のローカル時刻とに基づいて、U E におけるローカルタイミングを基地局用のローカル送信時刻に関連付け、ワイヤレスランシーバを介して、ランダムアクセスチャネル (R A C H) 上で基地局に第 2 のメッセージを送信し、第 2 のメッセージがランダム変数を含み、第 2 のメッセージが第 1 の時刻に送信され、第 1 の時刻が、U E におけるローカル時刻または基地局用の関連付けられたローカル送信時刻のいずれか一方であり、ワイヤレスランシーバを介して、第 2 のメッセージに応答して基地局から第 3 のメッセージを受信し、第 3 のメッセージが第 2 の時刻とランダム変数とを含み、第 2 の時刻が、第 2 のメッセージが基地局において受信された基地局用のローカル送信時刻であり、第 1 の時刻と第 2 の時刻とに基づいて R T T を決定する、ように構成されることによって R T T を測定するように構成される、条項 1 6 または 1 7 のいずれか一項に記載の U E 。

30

【 0 1 8 1 】

【 0 1 9 4 】 条項 1 9 。第 3 のメッセージが暗号化される、条項 1 8 に記載の U E 。

【 0 1 8 2 】

【 0 1 9 5 】 条項 2 0 。第 3 のメッセージが、基地局用のデジタル署名をさらに含み、少なくとも 1 つのプロセッサが、基地局用のデジタル署名に基づいて第 3 のメッセージを認証するようにさらに構成される、条項 1 8 または 1 9 のいずれか一項に記載の U E 。

40

【 0 1 8 3 】

【 0 1 9 6 】 条項 2 1 。攻撃デバイスが、U E と基地局との間のワイヤレスネットワーク内に存在し、メッセージが、リプレイ攻撃中に攻撃デバイスを介して受信され、少なくとも 1 つのプロセッサが、タイミングアドバンスから、または R T T を測定することによって伝搬遅延を決定し、伝搬遅延が予想範囲外であることに基づいて、攻撃デバイスの存在を検出する、ようにさらに構成される、条項 1 6 ~ 2 0 のいずれか一項に記載の U E 。

【 0 1 8 4 】

【 0 1 9 7 】 条項 2 2 。予想範囲が、基地局への最大予想距離に基づく最大伝搬遅延を含

50

む、条項 2 1 に記載の U E。

【 0 1 8 5 】

【 0 1 9 8 】 条項 2 3。少なくとも 1 つのプロセッサが、U E の推定ロケーションおよび基地局のロケーションを取得し、U E の推定ロケーションと基地局のロケーションとの間の距離推定値を決定し、距離推定値に基づいて予想範囲を決定する、ようにさらに構成される、条項 2 1 または 2 2 のいずれか一項に記載の U E。

【 0 1 8 6 】

【 0 1 9 9 】 条項 2 4。メッセージが、基地局サブフレームまたはスロット境界への現在時刻の暗黙的または明示的なアライメント、現在時刻の不確実性、現在時刻のソース、またはそれらの組合せのうちの少なくとも 1 つをさらに含む、条項 1 4 ~ 2 3 のいずれか一項に記載の U E。

【 0 1 8 7 】

【 0 2 0 0 】 条項 2 5。メッセージが、基地局用のデジタル署名をさらに含み、少なくとも 1 つのプロセッサが、基地局用のデジタル署名に基づいてメッセージ中の現在時刻を認証する、ようにさらに構成される、条項 1 4 ~ 2 4 のいずれか一項に記載の U E。

【 0 1 8 8 】

【 0 2 0 1 】 条項 2 6。少なくとも 1 つのプロセッサが、ワイヤレスネットワークから基地局用の公開暗号化鍵を受信し、デジタル署名が、公開暗号化鍵に対応する秘密暗号化鍵に基づくものであり、現在時刻を認証することが、公開暗号化鍵を使用する、ようにさらに構成される、条項 2 5 に記載の U E。

【 0 1 8 9 】

【 0 2 0 2 】 条項 2 7。ワイヤレスネットワークにおける時刻の取得をサポートするように構成されたユーザ機器 (U E) であって、基地局からブロードキャストされたメッセージを受信するための手段であって、メッセージが現在時刻を含み、現在時刻の少なくとも一部分が暗号化される、受信するための手段と、現在時刻の少なくとも一部分を解読することによって、平文の現在時刻を取得するための手段と、基地局と U E との間の伝搬遅延を決定するための手段と、平文の現在時刻と伝搬遅延とに基づいて、補正済み現在時刻を決定するための手段と、を備える、ユーザ機器 (U E) 。

【 0 1 9 0 】

【 0 2 0 3 】 条項 2 8。現在時刻が、協定世界時 (U T C) 時刻、全地球測位システム (G P S) 時刻、G L O N A S S 時刻、B e i d o u 時刻、G a l i l e o 時刻、全地球航法衛星システム (G N S S) 時刻、またはローカル地域時刻を含む、条項 2 7 に記載の U E。

【 0 1 9 1 】

【 0 2 0 4 】 条項 2 9。伝搬遅延を決定するための手段が、基地局からタイミングアドバンスを取得するための手段であって、伝搬遅延がタイミングアドバンスから決定される、取得するための手段、U E のロケーションおよび基地局のロケーションを取得するための手段であって、伝搬遅延が、U E のロケーションと基地局のロケーションとの間の距離に基づいて決定される、取得するための手段、または、U E と基地局との間の往復伝搬時間 (R T T) を測定するための手段であって、伝搬遅延が R T T の半分に等しい、測定するための手段、のうちの 1 つを含む、条項 2 7 または 2 8 のいずれか一項に記載の U E。

【 0 1 9 2 】

【 0 2 0 5 】 条項 3 0。U E のロケーションおよび基地局のロケーションを取得するための手段が、システム情報ブロック (S I B) 中の基地局のロケーションのブロードキャストを基地局から受信するための手段、基地局のロケーションを含むロングタームエボリューション (L T E) 測位プロトコル (L P P) 支援データメッセージを受信するための手段、U E のロケーションを含むモバイル発信ロケーション情報要求 (M O - L R) 応答メッセージを受信するための手段、または、測位セッションを実行して U E のロケーションを決定するための手段、のうちの少なくとも 1 つを含む、条項 2 9 に記載の U E。

【 0 1 9 3 】

【0206】 条項 3 1。R T Tを測定するための手段が、基地局用の第 1 のローカル送信時刻を示す第 1 のメッセージを基地局から受信するための手段と、基地局用の第 1 のローカル送信時刻と U E における第 1 のメッセージの受信のローカル時刻とに基づいて、U E におけるローカルタイミングを基地局用のローカル送信時刻に関連付けるための手段と、ランダムアクセスチャネル (R A C H) 上で基地局に第 2 のメッセージを送信するための手段であって、第 2 のメッセージがランダム変数を含み、第 2 のメッセージが第 1 の時刻に送信され、第 1 の時刻が U E におけるローカル時刻または基地局用の関連付けられたローカル送信時刻のいずれか一方である、送信するための手段と、第 2 のメッセージに応答して基地局から第 3 のメッセージを受信するための手段であって、第 3 のメッセージが第 2 の時刻とランダム変数とを含み、第 2 の時刻が、第 2 のメッセージが基地局において受信された基地局用のローカル送信時刻である、受信するための手段と、第 1 の時刻と第 2 の時刻とに基づいて R T T を決定するための手段と、を含む、条項 2 9 または 3 0 のいずれか一項に記載の U E。

10

【0194】

【0207】 条項 3 2。第 3 のメッセージが暗号化される、条項 3 1 に記載の U E。

【0195】

【0208】 条項 3 3。第 3 のメッセージが、基地局用のデジタル署名をさらに含み、U E が、基地局用のデジタル署名に基づいて第 3 のメッセージを認証するための手段をさらに備える、条項 3 1 または 3 2 のいずれか一項に記載の U E。

【0196】

20

【0209】 条項 3 4。攻撃デバイスが、U E と基地局との間のワイヤレスネットワーク内に存在し、メッセージが、リプレイ攻撃中に攻撃デバイスを介して受信され、U E が、タイミングアドバンスから、または R T T を測定することによって伝搬遅延を決定するための手段と、伝搬遅延が予想範囲外であることに基づいて、攻撃デバイスの存在を検出するための手段とをさらに備える、条項 2 9 ～ 3 3 のいずれか一項に記載の U E。

【0197】

【0210】 条項 3 5。予想範囲が、基地局への最大予想距離に基づく最大伝搬遅延を含む、条項 3 4 に記載の U E。

【0198】

【0211】 条項 3 6。U E の推定ロケーションおよび基地局のロケーションを取得するための手段と、U E の推定ロケーションと基地局のロケーションとの間の距離推定値を決定するための手段と、距離推定値に基づいて予想範囲を決定するための手段と、をさらに備える、条項 3 4 または 3 5 のいずれか一項に記載の U E。

30

【0199】

【0212】 条項 3 7。メッセージが、基地局サブフレームまたはスロット境界への現在時刻の暗黙的または明示的なアライメント、現在時刻の不確実性、現在時刻のソース、またはそれらの組合せのうちの少なくとも 1 つをさらに含む、条項 2 7 ～ 3 6 のいずれか一項に記載の U E。

【0200】

【0213】 条項 3 8。メッセージが、基地局用のデジタル署名をさらに含み、U E が、基地局用のデジタル署名に基づいて、メッセージ中の現在時刻を認証するための手段をさらに備える、条項 2 7 ～ 3 7 のいずれか一項に記載の U E。

40

【0201】

【0214】 条項 3 9。ワイヤレスネットワークから基地局用の公開暗号化鍵を受信するための手段であって、デジタル署名が、公開暗号化鍵に対応する秘密暗号化鍵に基づくものであり、現在時刻を認証することが、公開暗号化鍵を使用する、受信するための手段、をさらに備える、条項 3 8 に記載の U E。

【0202】

【0215】 条項 4 0。それに記憶されているプログラムコードを含む非一時的コンピュータ可読記憶媒体であって、プログラムコードが、ワイヤレスネットワークにおける時刻

50

の取得をサポートするためにユーザ機器（UE）内の少なくとも1つのプロセッサを構成するように動作可能であり、プログラムコードが、基地局からブロードキャストされたメッセージを受信し、メッセージが現在時刻を含み、現在時刻の少なくとも一部分が暗号化され、現在時刻の少なくとも一部分を解読することによって、平文の現在時刻を取得し、基地局とUEとの間の伝搬遅延を決定し、平文の現在時刻と伝搬遅延とに基づいて、補正済み現在時刻を決定する、ための命令を含む、非一時的コンピュータ可読記憶媒体。

【0203】

【0216】 条項41。現在時刻が、協定世界時（UTC）時刻、全地球測位システム（GPS）時刻、GLONASS時刻、Beidou時刻、Galileo時刻、全地球航法衛星システム（GNSS）時刻、またはローカル地域時刻を含む、条項40に記載の非一時的コンピュータ可読記憶媒体。

10

【0204】

【0217】 条項42。伝搬遅延を決定するための命令が、基地局からタイミングアドバンスを取得することであって、伝搬遅延がタイミングアドバンスから決定される、取得すること、UEのロケーションおよび基地局のロケーションを取得することであって、伝搬遅延が、UEのロケーションと基地局のロケーションとの間の距離に基づいて決定される、取得すること、または、UEと基地局との間の往復伝搬時間（RTT）を測定することであって、伝搬遅延がRTTの半分に等しい、測定すること、のうちの1つを行うための命令を含む、条項40または41のいずれか一項に記載の非一時的コンピュータ可読記憶媒体。

20

【0205】

【0218】 条項43。UEのロケーションおよび基地局のロケーションを取得するための命令が、システム情報ブロック（SIB）中の基地局のロケーションのブロードキャストを基地局から受信すること、基地局のロケーションを含むロングタームエポリーション（LTE）測位プロトコル（LPP）支援データメッセージを受信すること、UEのロケーションを含むモバイル発信ロケーション情報要求（MO-LR）応答メッセージを受信すること、または、測位セッションを実行してUEのロケーションを決定すること、のうちの少なくとも1つを行うための命令を含む、条項42に記載の非一時的コンピュータ可読記憶媒体。

【0206】

【0219】 条項44。RTTを測定するための命令が、基地局用の第1のローカル送信時刻を示す第1のメッセージを基地局から受信し、基地局用の第1のローカル送信時刻とUEにおける第1のメッセージの受信のローカル時刻とに基づいて、UEにおけるローカルタイミングを基地局用のローカル送信時刻に関連付け、ランダムアクセスチャネル（RACH）上で基地局に第2のメッセージを送信し、第2のメッセージがランダム変数を含み、第2のメッセージが第1の時刻に送信され、第1の時刻がUEにおけるローカル時刻または基地局用の関連付けられたローカル送信時刻のいずれか一方であり、第2のメッセージに応答して基地局から第3のメッセージを受信し、第3のメッセージが第2の時刻とランダム変数とを含み、第2の時刻が、第2のメッセージが基地局において受信された基地局用のローカル送信時刻であり、第1の時刻と第2の時刻とに基づいてRTTを決定するための命令を含む、条項42または43のいずれか一項に記載の非一時的コンピュータ可読記憶媒体。

30

40

【0207】

【0220】 条項45。第3のメッセージが暗号化される、条項44に記載の非一時的コンピュータ可読記憶媒体。

【0208】

【0221】 条項46。第3のメッセージが、基地局用のデジタル署名をさらに含み、プログラムコードが、基地局用のデジタル署名に基づいて第3のメッセージを認証する、ための命令をさらに含む、条項44または45のいずれか一項に記載の非一時的コンピュータ可読記憶媒体。

50

【0209】

【0222】 条項47。攻撃デバイスが、UEと基地局との間のワイヤレスネットワーク内に存在し、メッセージが、リプレイ攻撃中に攻撃デバイスを介して受信され、プログラムコードが、タイミングアドバンスから、またはRTTを測定することによって伝搬遅延を決定し、伝搬遅延が予想範囲外であることに基づいて攻撃デバイスの存在を検出する、ための命令をさらに含む、条項42～46のいずれか一項に記載の非一時的コンピュータ可読記憶媒体。

【0210】

【0223】 条項48。予想範囲が、基地局への最大予想距離に基づく最大伝搬遅延を含む、条項47に記載の非一時的コンピュータ可読記憶媒体。

10

【0211】

【0224】 条項49。プログラムコードが、UEの推定ロケーションおよび基地局のロケーションを取得し、UEの推定ロケーションと基地局のロケーションとの間の距離推定値を決定し、距離推定値に基づいて予想範囲を決定する、ための命令をさらに含む、条項47または48のいずれか一項に記載の非一時的コンピュータ可読記憶媒体。

【0212】

【0225】 条項50。メッセージが、基地局サブフレームまたはスロット境界への現在時刻の暗黙的または明示的なアライメント、現在時刻の不確実性、現在時刻のソース、またはそれらの組合せのうちの少なくとも1つをさらに含む、条項40～49のいずれか一項に記載の非一時的コンピュータ可読記憶媒体。

20

【0213】

【0226】 条項51。メッセージが、基地局用のデジタル署名をさらに含み、プログラムコードが、基地局用のデジタル署名に基づいてメッセージ中の現在時刻を認証する、ための命令をさらに含む、条項40～50のいずれか一項に記載の非一時的コンピュータ可読記憶媒体。

【0214】

【0227】 条項52。プログラムコードが、ワイヤレスネットワークから基地局用の公開暗号化鍵を受信し、デジタル署名が、公開暗号化鍵に対応する秘密暗号化鍵に基づくものであり、現在時刻を認証することが、公開暗号化鍵を使用する、ための命令をさらに含む、条項51に記載の非一時的コンピュータ可読記憶媒体。

30

【0215】

【0228】 条項53。ワイヤレスネットワークにおける、ユーザ機器(UE)による時刻の取得をサポートするために基地局によって実行される方法であって、現在時刻を取得することと、現在時刻の少なくとも一部分を暗号化することと、現在時刻を含むメッセージをブロードキャストすることと、を含み、UEが、メッセージを受信し、現在時刻の少なくとも一部分を解読することによって平文の現在時刻を取得し、かつ基地局とUEとの間の伝搬遅延を決定し、UEが、平文の現在時刻と伝搬遅延とに基づいて、補正済み現在時刻を決定する、方法。

【0216】

【0229】 条項54。現在時刻が、協定世界時(UTC)時刻、全地球測位システム(GPS)時刻、GLONASS時刻、Beidou時刻、Galileo時刻、全地球航行衛星システム(GNSS)時刻、またはローカル地域時刻を含む、条項53に記載の方法。

40

【0217】

【0230】 条項55。タイミングアドバンスをUEに送信することであって、タイミングアドバンスが、UEによる伝搬遅延の決定を可能にする、送信すること、UEのロケーションと基地局のロケーションとのうちの少なくとも一方を含むメッセージをUEに送信することであって、伝搬遅延が、UEのロケーションと基地局のロケーションとの間の距離に基づいてUEによって決定される、送信すること、または、UEと基地局との間の往復伝搬時間(RTT)の測定においてUEを支援することであって、伝搬遅延がRTTの

50

半分に等しい、支援することと、のうちの1つを実行することによって、伝搬遅延の決定においてUEを支援することをさらに含む、条項53または54のいずれか一項に記載の方法。

【0218】

【0231】 条項56。UEのロケーションと基地局のロケーションとのうちの少なくとも一方を含むメッセージをUEに送信することが、システム情報ブロック(SIB)中の基地局のロケーションをブロードキャストすること、基地局のロケーションを含むロングタームエボリューション(LTE)測位プロトコル(LPP)支援データメッセージをUEに転送すること、UEのロケーションを含むモバイル発信ロケーション情報要求(MO-LR)応答メッセージをUEに送信すること、または、UEとUE用のロケーションサーバとの間でLPPメッセージを転達して、UEのロケーションを決定すること、のうちの少なくとも1つを含む、条項55に記載の方法。

10

【0219】

【0232】 条項57。RTTの測定においてUEを支援することが、基地局用の第1のローカル送信時刻を示す第1のメッセージをUEに送信することであって、UEが、基地局用の第1のローカル送信時刻とUEにおける第1のメッセージの受信のローカル時刻とに基づいて、UEにおけるローカルタイミングを基地局用のローカル送信時刻に関連付ける、送信することと、ランダムアクセスチャネル(RACH)上でUEから第2のメッセージを受信することであって、第2のメッセージがランダム変数を含み、第2のメッセージが第1の時刻に送信され、第1の時刻がUEにおけるローカル時刻または基地局用の関連付けられたローカル送信時刻のいずれか一方である、受信することと、第2の時刻を測定することであって、第2の時刻が、第2のメッセージが基地局において受信された基地局用のローカル送信時刻である、測定することと、第2のメッセージに応答してUEに第3のメッセージを送信することであって、第3のメッセージが、第2の時刻とランダム変数とを含み、UEが、第1の時刻と第2の時刻とに基づいてRTTを決定する、送信することと、を含む、条項55または56のいずれか一項に記載の方法。

20

【0220】

【0233】 条項58。第3のメッセージを暗号化することをさらに含む、条項57に記載の方法。

【0221】

30

【0234】 条項59。基地局用のデジタル署名を第3のメッセージ中に含めることであって、UEが、基地局用のデジタル署名に基づいて第3のメッセージを認証する、含めること、をさらに含む、条項57または58のいずれか一項に記載の方法。

【0222】

【0235】 条項60。攻撃デバイスが、UEと基地局との間のワイヤレスネットワーク内に存在し、メッセージが、リプレイ攻撃中に攻撃デバイスを介してUEによって受信され、UEが、タイミングアドバンスから、またはRTTを測定することによって伝搬遅延を決定し、UEが、伝搬遅延が予想範囲外であることに基づいて攻撃デバイスの存在を検出する、条項55～59のいずれか一項に記載の方法。

【0223】

40

【0236】 条項61。予想範囲が、UEと基地局との間の最大予想距離に基づく最大伝搬遅延を含む、条項60に記載の方法。

【0224】

【0237】 条項62。予想範囲が、UEの推定ロケーションと、UEによって取得された基地局のロケーションとに基づくものである、条項60または61のいずれか一項に記載の方法。

【0225】

【0238】 条項63。基地局用のサブフレームまたはスロット境界への現在時刻の暗黙的または明示的なアライメント、現在時刻の不確実性、現在時刻の取得元となるソース、またはそれらの組合せのうちの少なくとも1つを、メッセージ中に含めることをさらに含

50

む、条項 5 3 ～ 6 2 のいずれか一項に記載の方法。

【 0 2 2 6 】

【 0 2 3 9 】 条項 6 4。基地局用のデジタル署名をメッセージ中に含めることであって、UE が、基地局用のデジタル署名に基づいてメッセージ中の現在時刻を認証する、含めること、をさらに含む、条項 5 3 ～ 6 3 のいずれか一項に記載の方法。

【 0 2 2 7 】

【 0 2 4 0 】 条項 6 5。基地局用の公開暗号化鍵を UE に送信することであって、デジタル署名が、公開暗号化鍵に対応する秘密暗号化鍵に基づくものであり、UE が、公開暗号化鍵を使用して現在時刻を認証する、送信すること、をさらに含む、条項 6 4 に記載の方法。

【 0 2 2 8 】

【 0 2 4 1 】 条項 6 6。ワイヤレスネットワークにおけるユーザ機器（UE）による時刻の取得をサポートするように構成された基地局であって、ワイヤレスネットワーク内のエンティティとワイヤレス通信するように構成された外部インターフェースと、少なくとも 1 つのメモリと、外部インターフェースおよび少なくとも 1 つのメモリに結合された少なくとも 1 つのプロセッサと、を備え、少なくとも 1 つのプロセッサが、現在時刻を取得し、現在時刻の少なくとも一部分を暗号化し、現在時刻を含むメッセージをブロードキャストする、ように構成され、UE が、メッセージを受信し、現在時刻の少なくとも一部分を解読することによって平文の現在時刻を取得し、かつ基地局と UE との間の伝搬遅延を決定し、UE が、平文の現在時刻と伝搬遅延とに基づいて、補正済み現在時刻を決定する、基地局。

【 0 2 2 9 】

【 0 2 4 2 】 条項 6 7。現在時刻が、協定世界時（UTC）時刻、全地球測位システム（GPS）時刻、GLONASS 時刻、Beidou 時刻、Galileo 時刻、全地球航法衛星システム（GNSS）時刻、またはローカル地域時刻を含む、条項 6 6 に記載の基地局。

【 0 2 3 0 】

【 0 2 4 3 】 条項 6 8。少なくとも 1 つのプロセッサが、UE にタイミングアドバンスを送信することであって、タイミングアドバンスが、UE による伝搬遅延の決定を可能にする、送信すること、UE のロケーションと基地局のロケーションとのうちの少なくとも一方を含むメッセージを UE に送信することであって、伝搬遅延が、UE のロケーションと基地局のロケーションとの間の距離に基づいて UE によって決定される、送信すること、または、UE と基地局との間の往復伝搬時間（RTT）の測定において UE を支援することであって、伝搬遅延が RTT の半分に等しい、支援すること、のうちの 1 つを行うように構成されることによって、伝搬遅延の決定において UE を支援するようにさらに構成される、条項 6 6 または 6 7 のいずれか一項に記載の基地局。

【 0 2 3 1 】

【 0 2 4 4 】 条項 6 9。少なくとも 1 つのプロセッサが、システム情報ブロック（SIB）中の基地局のロケーションをブロードキャストすること、基地局のロケーションを含むロングタームエボリューション（LTE）測位プロトコル（LPP）支援データメッセージを UE に転送すること、UE のロケーションを含むモバイル発信ロケーション情報要求（MO-LR）応答メッセージを UE に送信すること、または、UE と UE 用のロケーションサーバとの間で LPP メッセージを転達して、UE のロケーションを決定すること、のうちの少なくとも 1 つを行うように構成されることによって、UE のロケーションと基地局のロケーションとのうちの少なくとも一方を含むメッセージを UE に送信するようにさらに構成される、条項 6 8 に記載の基地局。

【 0 2 3 2 】

【 0 2 4 5 】 条項 7 0。少なくとも 1 つのプロセッサが、基地局用の第 1 のローカル送信時刻を示す第 1 のメッセージを UE に送信し、UE が、基地局用の第 1 のローカル送信時刻と UE における第 1 のメッセージの受信のローカル時刻とに基づいて、UE におけるロ

10

20

30

40

50

ーカルタイミングを基地局用のローカル送信時刻に関連付け、ランダムアクセスチャネル（RACH）上でUEから第2のメッセージを受信し、第2のメッセージがランダム変数を含み、第2のメッセージが第1の時刻に送信され、第1の時刻が、UEにおけるローカル時刻または基地局用の関連付けられたローカル送信時刻のいずれか一方であり、第2の時刻を測定し、第2の時刻が、第2のメッセージが基地局において受信された基地局用のローカル送信時刻であり、第2のメッセージに応答してUEに第3のメッセージを送信し、第3のメッセージが、第2の時刻とランダム変数とを含み、UEが、第1の時刻と第2の時刻とに基づいてRTTを決定する、ように構成されることによって、RTTの測定においてUEを支援するようにさらに構成される、条項68または69のいずれか一項に記載の基地局。

10

【0233】

【0246】 条項71。少なくとも1つのプロセッサが、第3のメッセージを暗号化するようにさらに構成される、条項70に記載の基地局。

【0234】

【0247】 条項72。少なくとも1つのプロセッサが、基地局用のデジタル署名を第3のメッセージ中に含め、UEが、基地局用のデジタル署名に基づいて第3のメッセージを認証する、ようにさらに構成される、条項70または71のいずれか一項に記載の基地局。

【0235】

【0248】 条項73。攻撃デバイスが、UEと基地局との間のワイヤレスネットワーク内に存在し、メッセージが、リプレイ攻撃中に攻撃デバイスを介してUEによって受信され、UEが、タイミングアドバンスから、またはRTTを測定することによって伝搬遅延を決定し、UEが、伝搬遅延が予想範囲外であることに基づいて攻撃デバイスの存在を検出する、条項68～72のいずれか一項に記載の基地局。

20

【0236】

【0249】 条項74。予想範囲が、UEと基地局との間の最大予想距離に基づく最大伝搬遅延を含む、条項73に記載の基地局。

【0237】

【0250】 条項75。予想範囲が、UEの推定ロケーションとUEによって取得された基地局のロケーションとに基づくものである、条項73または74のいずれか一項に記載の基地局。

30

【0238】

【0251】 条項76。少なくとも1つのプロセッサが、基地局用のサブフレームまたはスロット境界への現在時刻の暗黙的または明示的なアライメント、現在時刻の不確実性、現在時刻の取得元となるソース、またはそれらの組合せのうちの少なくとも1つを、メッセージ中に含めるようにさらに構成される、条項66～75のいずれか一項に記載の基地局。

【0239】

【0252】 条項77。少なくとも1つのプロセッサが、基地局用のデジタル署名をメッセージ中に含め、UEが、基地局用のデジタル署名に基づいてメッセージ中の現在時刻を認証する、ようにさらに構成される、条項66～76のいずれか一項に記載の基地局。

40

【0240】

【0253】 条項78。少なくとも1つのプロセッサが、基地局用の公開暗号化鍵をUEに送信し、デジタル署名が、公開暗号化鍵に対応する秘密暗号化鍵に基づくものであり、UEが、公開暗号化鍵を使用して現在時刻を認証する、ようにさらに構成される、条項77に記載の基地局。

【0241】

【0254】 条項79。ワイヤレスネットワークにおけるユーザ機器（UE）による時刻の取得をサポートするように構成された基地局であって、現在時刻を取得するための手段と、現在時刻の少なくとも一部分を暗号化するための手段と、現在時刻を含むメッセージ

50

をブロードキャストするための手段と、を備え、UEが、メッセージを受信し、現在時刻の少なくとも一部分を解読することによって平文の現在時刻を取得し、かつ基地局とUEとの間の伝搬遅延を決定し、UEが、平文の現在時刻と伝搬遅延とに基づいて、補正済み現在時刻を決定する、基地局。

【0242】

【0255】 条項80。現在時刻が、協定世界時(UTC)時刻、全地球測位システム(GPS)時刻、GLONASS時刻、Beidou時刻、Galileo時刻、全地球航行衛星システム(GNSS)時刻、またはローカル地域時刻を含む、条項79に記載の基地局。

【0243】

【0256】 条項81。タイミングアドバンスをUEに送信するための手段であって、タイミングアドバンスが、UEによる伝搬遅延の決定を可能にする、送信するための手段、UEのロケーションと基地局のロケーションとのうちの少なくとも一方を含むメッセージをUEに送信するための手段であって、伝搬遅延が、UEのロケーションと基地局のロケーションとの間の距離に基づいてUEによって決定される、送信するための手段、または、UEと基地局との間の往復伝搬時間(RTT)の測定においてUEを支援するための手段であって、伝搬遅延がRTTの半分に等しい、支援するための手段、のうちの1つを含む、伝搬遅延の決定においてUEを支援するための手段をさらに備える、条項79または80のいずれか一項に記載の基地局。

【0244】

【0257】 条項82。UEのロケーションと基地局のロケーションとのうちの少なくとも一方を含むメッセージをUEに送信するための手段が、システム情報ブロック(SIB)中の基地局のロケーションをブロードキャストするための手段、基地局のロケーションを含むロングタームエボリューション(LTE)測位プロトコル(LPP)支援データメッセージをUEに転送するための手段、UEのロケーションを含むモバイル発信ロケーション情報要求(MO-LR)応答メッセージをUEに送信するための手段、または、UEとUE用のロケーションサーバとの間でLPPメッセージを転達して、UEのロケーションを決定するための手段、のうちの少なくとも1つを含む、条項81に記載の基地局。

【0245】

【0258】 条項83。RTTの測定においてUEを支援するための手段が、基地局用の第1のローカル送信時刻を示す第1のメッセージをUEに送信するための手段であって、UEが、基地局用の第1のローカル送信時刻とUEにおける第1のメッセージの受信のローカル時刻とに基づいて、UEにおけるローカルタイミングを基地局用のローカル送信時刻に関連付ける、送信するための手段と、ランダムアクセスチャネル(RACH)上でUEから第2のメッセージを受信するための手段であって、第2のメッセージがランダム変数を含み、第2のメッセージが第1の時刻に送信され、第1の時刻がUEにおけるローカル時刻または基地局用の関連付けられたローカル送信時刻のいずれか一方である、受信するための手段と、第2の時刻を測定するための手段であって、第2の時刻が、第2のメッセージが基地局において受信された基地局用のローカル送信時刻である、測定するための手段と、第2のメッセージに応答してUEに第3のメッセージを送信するための手段であって、第3のメッセージが第2の時刻とランダム変数とを含み、UEが、第1の時刻と第2の時刻とに基づいてRTTを決定する、送信するための手段と、を含む、条項81または82のいずれか一項に記載の基地局。

【0246】

【0259】 条項84。第3のメッセージを暗号化するための手段をさらに備える、条項83に記載の基地局。

【0247】

【0260】 条項85。基地局用のデジタル署名を第3のメッセージ中に含めるための手段であって、UEが、基地局用のデジタル署名に基づいて第3のメッセージを認証する、含めるための手段をさらに備える、条項83または84のいずれか一項に記載の基地局。

【0248】

【0261】 条項86。攻撃デバイスが、UEと基地局との間のワイヤレスネットワーク内に存在し、メッセージが、リプレイ攻撃中に攻撃デバイスを介してUEによって受信され、UEが、タイミングアドバンスから、またはRTTを測定することによって伝搬遅延を決定し、UEが、伝搬遅延が予想範囲外であることに基づいて攻撃デバイスの存在を検出する、条項81～85のいずれか一項に記載の基地局。

【0249】

【0262】 条項87。予想範囲が、UEと基地局との間の最大予想距離に基づく最大伝搬遅延を含む、条項86に記載の基地局。

【0250】

【0263】 条項88。予想範囲が、UEの推定ロケーションと、UEによって取得された基地局のロケーションとに基づくものである、条項86または87のいずれか一項に記載の基地局。

【0251】

【0264】 条項89。基地局用のサブフレームまたはスロット境界への現在時刻の暗黙的または明示的なアライメント、現在時刻の不確実性、現在時刻の取得元となるソース、またはそれらの組合せのうちの少なくとも1つを、メッセージ中に含めるための手段をさらに備える、条項79～88のいずれか一項に記載の基地局。

【0252】

【0265】 条項90。基地局用のデジタル署名をメッセージ中に含めるための手段であって、UEが、基地局用のデジタル署名に基づいてメッセージ中の現在時刻を認証する、含めるための手段をさらに備える、条項79～89のいずれか一項に記載の基地局。

【0253】

【0266】 条項91。基地局用の公開暗号化鍵をUEに送信するための手段であって、デジタル署名が、公開暗号化鍵に対応する秘密暗号化鍵に基づくものであり、UEが、公開暗号化鍵を使用して現在時刻を認証する、送信するための手段をさらに備える、条項90に記載の基地局。

【0254】

【0267】 条項92。それに記憶されているプログラムコードを含む非一時的コンピュータ可読記憶媒体であって、プログラムコードが、ワイヤレスネットワークにおける、ユーザ機器（UE）による時刻の取得をサポートするために基地局内の少なくとも1つのプロセッサを構成するように動作可能であり、プログラムコードが、現在時刻を取得し、現在時刻の少なくとも一部分を暗号化し、現在時刻を含むメッセージをブロードキャストする、ための命令を含み、UEが、メッセージを受信し、現在時刻の少なくとも一部分を解読することによって平文の現在時刻を取得し、かつ基地局とUEとの間の伝搬遅延を決定し、UEが、平文の現在時刻と伝搬遅延とに基づいて、補正済み現在時刻を決定する、非一時的コンピュータ可読記憶媒体。

【0255】

【0268】 条項93。現在時刻が、協定世界時（UTC）時刻、全地球測位システム（GPS）時刻、GLONASS時刻、Beidou時刻、Galileo時刻、全地球航行衛星システム（GNSS）時刻、またはローカル地域時刻を含む、条項92に記載の非一時的コンピュータ可読記憶媒体。

【0256】

【0269】 条項94。UEにタイミングアドバンスを送信することであって、タイミングアドバンスが、UEによる伝搬遅延の決定を可能にする、送信すること、UEのロケーションと基地局のロケーションとのうちの少なくとも一方を含むメッセージをUEに送信することであって、伝搬遅延が、UEのロケーションと基地局のロケーションとの間の距離に基づいてUEによって決定される、送信すること、または、UEと基地局との間の往復伝搬時間（RTT）の測定においてUEを支援することであって、伝搬遅延がRTTの半分に等しい、支援すること、のうちの1つを行うための命令を含む、伝搬遅延の決定に

10

20

30

40

50

においてUEを支援するための命令をさらに含む、条項92または93のいずれか一項に記載の非一時的コンピュータ可読記憶媒体。

【0257】

【0270】 条項95。UEのロケーションと基地局のロケーションとのうちの少なくとも一方を含むメッセージをUEに送信するための命令が、システム情報ブロック(SIB)中の基地局のロケーションをブロードキャストすること、基地局のロケーションを含むロングタームエボリューション(LTE)測位プロトコル(LPP)支援データメッセージをUEに転送すること、UEのロケーションを含むモバイル発信ロケーション情報要求(MO-LR)応答メッセージをUEに送信すること、または、UEとUE用のロケーションサーバとの間でLPPメッセージを転達して、UEのロケーションを決定すること、
10
のうちの少なくとも1つを行うための命令を含む、条項94に記載の非一時的コンピュータ可読記憶媒体。

【0258】

【0271】 条項96。RTTの測定においてUEを支援するための命令が、基地局用の第1のローカル送信時刻を示す第1のメッセージをUEに送信し、UEが、基地局用の第1のローカル送信時刻とUEにおける第1のメッセージの受信のローカル時刻とに基づいて、UEにおけるローカルタイミングを基地局用のローカル送信時刻に関連付け、ランダムアクセスチャネル(RACH)上でUEから第2のメッセージを受信し、第2のメッセージがランダム変数を含み、第2のメッセージが第1の時刻に送信され、第1の時刻が、UEにおけるローカル時刻または基地局用の関連付けられたローカル送信時刻のいずれか
20
一方であり、第2の時刻を測定し、第2の時刻が、第2のメッセージが基地局において受信された基地局用のローカル送信時刻であり、第2のメッセージに応答してUEに第3のメッセージを送信し、第3のメッセージが、第2の時刻とランダム変数とを含み、UEが、第1の時刻と第2の時刻とに基づいてRTTを決定する、ための命令を含む、条項94または95のいずれか一項に記載の非一時的コンピュータ可読記憶媒体。

【0259】

【0272】 条項97。プログラムコードが、第3のメッセージを暗号化するための命令をさらに含む、条項96に記載の非一時的コンピュータ可読記憶媒体。

【0260】

【0273】 条項98。プログラムコードが、基地局用のデジタル署名を第3のメッセージ中に含め、UEが、基地局用のデジタル署名に基づいて第3のメッセージを認証する、ための命令をさらに含む、条項96または97のいずれか一項に記載の非一時的コンピュータ可読記憶媒体。
30

【0261】

【0274】 条項99。攻撃デバイスが、UEと基地局との間のワイヤレスネットワーク内に存在し、メッセージが、リプレイ攻撃中に攻撃デバイスを介してUEによって受信され、UEが、タイミングアドバンスから、またはRTTを測定することによって伝搬遅延を決定し、UEが、伝搬遅延が予想範囲外であることに基づいて攻撃デバイスの存在を検出する、条項94～98のいずれか一項に記載の非一時的コンピュータ可読記憶媒体。
40

【0262】

【0275】 条項100。予想範囲が、UEと基地局との間の最大予想距離に基づく最大伝搬遅延を含む、条項99に記載の非一時的コンピュータ可読記憶媒体。

【0263】

【0276】 条項101。予想範囲が、UEの推定ロケーションと、UEによって取得された基地局のロケーションとに基づくものである、条項99または100のいずれか一項に記載の非一時的コンピュータ可読記憶媒体。

【0264】

【0277】 条項102。プログラムコードが、基地局用のサブフレームまたはスロット境界への現在時刻の暗黙的または明示的なアライメント、現在時刻の不確実性、現在時刻の取得元となるソース、またはそれらの組合せのうちの少なくとも1つを、メッセージ中
50

に含めるための命令をさらに含む、条項 9 2 ～ 1 0 1 のいずれか一項に記載の非一時的コンピュータ可読記憶媒体。

【 0 2 6 5 】

【 0 2 7 8 】 条項 1 0 3 。プログラムコードが、基地局用のデジタル署名をメッセージ中に含め、U E が、基地局用のデジタル署名に基づいてメッセージ中の現在時刻を認証する、ための命令をさらに含む、条項 9 2 ～ 1 0 2 のいずれか一項に記載の非一時的コンピュータ可読記憶媒体。

【 0 2 6 6 】

【 0 2 7 9 】 条項 1 0 4 。プログラムコードが、基地局用の公開暗号化鍵をU E に送信し、デジタル署名が、公開暗号化鍵に対応する秘密暗号化鍵に基づくものであり、U E が、公開暗号化鍵を使用して現在時刻を認証する、ための命令をさらに含む、条項 1 0 3 に記載の非一時的コンピュータ可読記憶媒体。

【 0 2 6 7 】

【 0 2 8 0 】 したがって、特許請求される主題は開示されている特定の例に限定されず、このような特許請求される主題が、添付の特許請求の範囲内に入るすべての態様およびその等価物も含み得ることが意図される。

【 図 面 】

【 図 1 】

【 図 2 A 】

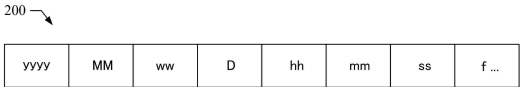
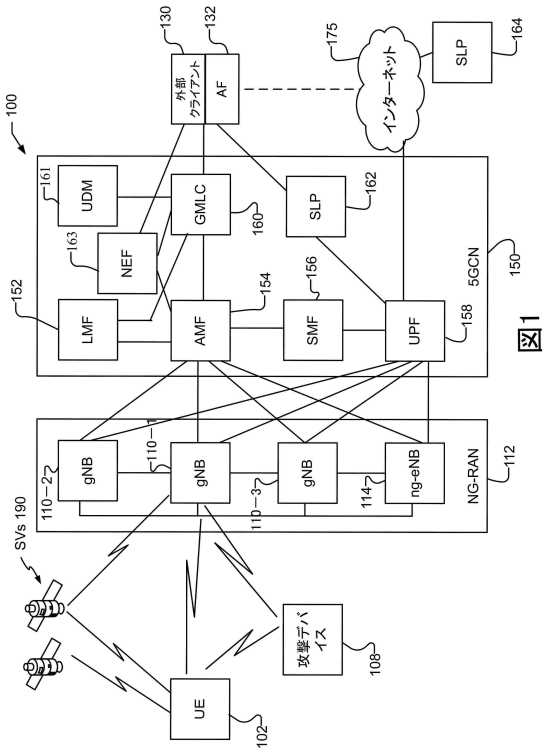


図2A

【図 2 B】



図2B

【図 2 C】

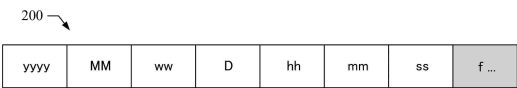


図2C

【図 2 D】

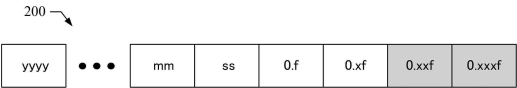


図2D

【図 2 E】

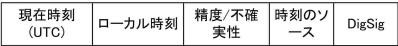


図2E

10

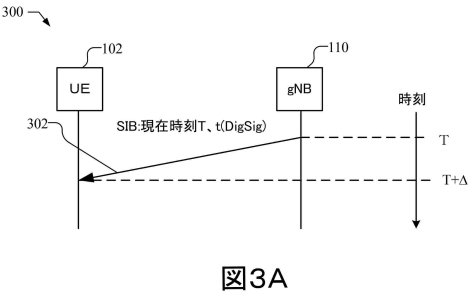
20

30

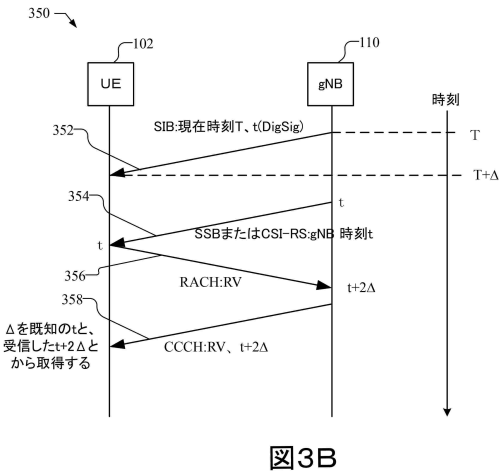
40

50

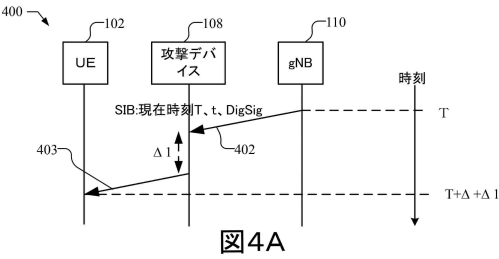
【図 3 A】



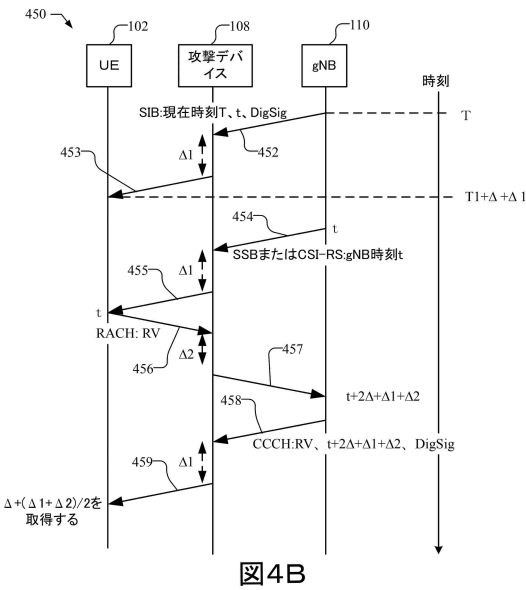
【図 3 B】



【図 4 A】



【図 4 B】



10

20

30

40

50

【図 5】

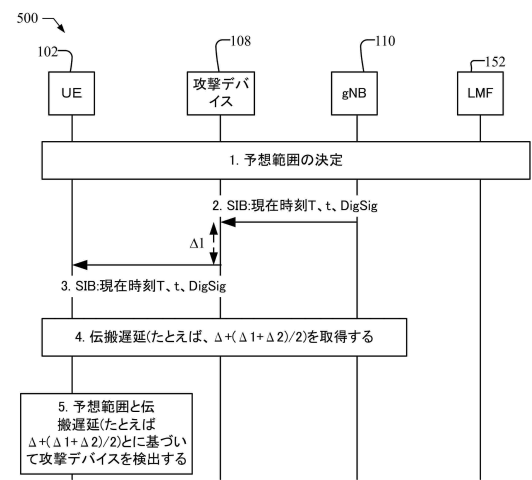


図5

【図 6】

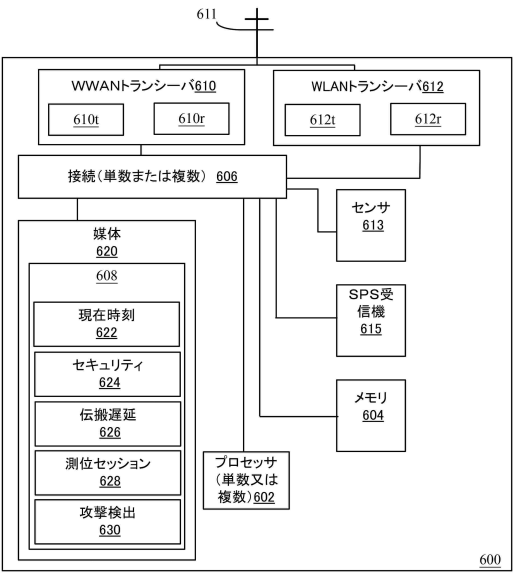


図6

【図 7】

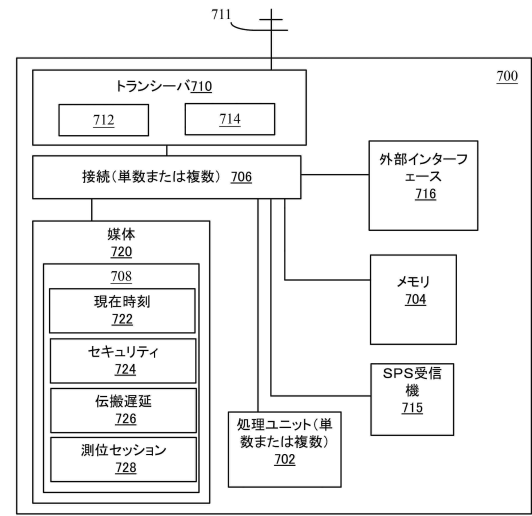


図7

【図 8】

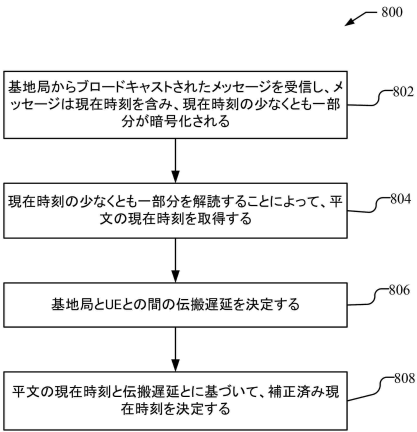


図8

10

20

30

40

50

【図 9】

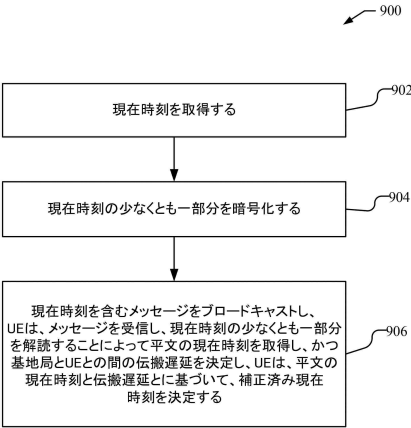


図9

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2022/032396

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W56/00 H04L69/28 H04W12/122
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04W H04L G01S

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2018/324740 A1 (EDGE STEPHEN WILLIAM [US] ET AL) 8 November 2018 (2018-11-08)	1, 2, 11-15, 24-27, 29
Y	figures 1b, 2, 4-5, 7, 8, 11 paragraph [0053] - paragraph [0058] paragraph [0071] - paragraph [0083] paragraph [0102] paragraph [0119] - paragraph [0142] paragraph [0165] - paragraph [0166] paragraph [0179] - paragraph [0188] ----- -/--	3-10, 16-23, 28, 30

☒ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

12 September 2022

Date of mailing of the international search report

19/09/2022

Name and mailing address of the ISA/
European Patent Office, P.B. 5618 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Riegler, Jörg

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2022/032396

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	QUALCOMM INCORPORATED: "DL and UL NR Positioning Procedures", 3GPP DRAFT; R2-1913395_(POSITIONING PROCEDURES+DRAFT LPP CR), 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE , vol. RAN WG2, no. Chongqing, China; 20191014 - 20191018 4 October 2019 (2019-10-04), XP051804974, Retrieved from the Internet: URL:https://ftp.3gpp.org/tsg_ran/WG2_RL2/TSGR2_107bis/Docs/R2-1913395.zip R2-1913395_(Positioning Procedures+Draft LPP CR).docx [retrieved on 2019-10-04] page 2 - page 5 -----	3-7, 16-20, 28, 30
Y	US 2021/103058 A1 (DRIES RONALD FRANKLIN [US] ET AL) 8 April 2021 (2021-04-08) figures 3,4 paragraph [0027] - paragraph [0046] -----	8-10, 21-23

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2022/032396

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2018324740 A1	08-11-2018	CN 110622587 A	27-12-2019
		EP 3619984 A1	11-03-2020
		TW 201844040 A	16-12-2018
		US 2018324740 A1	08-11-2018
		WO 2018204554 A1	08-11-2018

US 2021103058 A1	08-04-2021	EP 4038503 A1	10-08-2022
		US 2021103058 A1	08-04-2021
		WO 2021067790 A1	08-04-2021

フロントページの続き

(51)国際特許分類

H O 4 W

74/0833(2024.01)

F I

H O 4 W

74/0833

テーマコード (参考)

MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,N
E,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,
CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IQ,IR,IS,IT,JM,J
O,JP,KE,KG,KH,KN,KP,KR,KW,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,M
Z,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,ST,SV,SY,TH,
TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,WS,ZA,ZM,ZW

(特許庁注：以下のものは登録商標)

1. B L U — R A Y D I S C