



(12) 发明专利申请



(10) 申请公布号 CN 117859381 A

(43) 申请公布日 2024. 04. 09

(21) 申请号 202280051103.3

(22) 申请日 2022.06.06

(30) 优先权数据

17/386,325 2021.07.27 US

(85) PCT国际申请进入国家阶段日

2024.01.19

(86) PCT国际申请的申请数据

PCT/US2022/032396 2022.06.06

(87) PCT国际申请的公布数据

W02023/009218 EN 2023.02.02

(71) 申请人 高通股份有限公司

地址 美国加利福尼亚州

(72) 发明人 S·W·埃奇

(74) 专利代理机构 北京市柳沈律师事务所

11105

专利代理师 安之斐

(51) Int.Cl.

H04W 56/00 (2006.01)

H04W 12/122 (2006.01)

H04L 69/28 (2006.01)

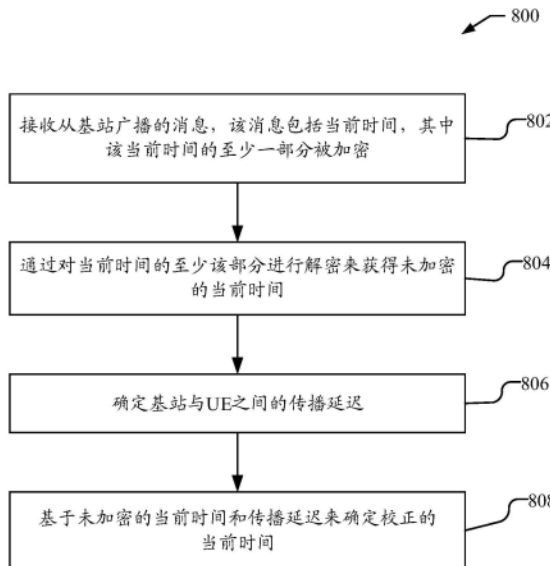
权利要求书4页 说明书44页 附图10页

(54) 发明名称

用于在无线网络中获取可靠时间的方法和装置

(57) 摘要

由用户装备 (UE) 在无线网络中从基站获取准确且可靠的时间。该基站可获得该时间,例如, UTC时间或GNSS时间,并且在广播该时间之前对该时间的至少一部分进行加密。UE基于定时提前、UE和基站的已知位置、或者UE与基站之间测得的往返传播时间 (RTT) 来确定UE与基站之间的传播延迟。可以基于从基站接收到的时间和传播延迟来确定校正时间。与由基站广播的时间包括在一起的数字签名提高了可靠性。UE可基于传播延迟超出预期范围来检测到攻击设备对广播时间的仿冒。



1. 一种由用户装备 (UE) 执行的用于支持在无线网络中获取时间的方法, 所述方法包括:

接收从基站广播的消息, 所述消息包括当前时间, 其中所述当前时间的至少一部分被加密;

通过对所述当前时间的至少所述部分进行解密来获得未加密的当前时间;

确定所述基站与所述UE之间的传播延迟; 以及

基于所述未加密的当前时间和所述传播延迟来确定校正的当前时间。

2. 根据权利要求1所述的方法, 其中所述当前时间包括协调世界时 (UTC) 时间、全球定位系统 (GPS) 时间、GLONASS时间、北斗时间、伽利略时间、全球导航卫星系统 (GNSS) 时间、或本地区域时间。

3. 根据权利要求1所述的方法, 其中确定所述传播延迟包括以下中的一者:

从所述基站获得定时提前, 其中所述传播延迟是根据所述定时提前来确定的;

获得所述UE的位置和所述基站的位置, 其中所述传播延迟是基于所述UE的所述位置与所述基站的所述位置之间的距离来确定的; 或者

测量所述UE与所述基站之间的往返传播时间 (RTT), 其中所述传播延迟等于所述RTT的一半。

4. 根据权利要求3所述的方法, 其中获得所述UE的位置和所述基站的位置包括以下中的至少一者:

在系统信息块 (SIB) 中接收来自所述基站的对所述基站的位置的广播;

接收包含所述基站的位置的长期演进 (LTE) 定位协议 (LPP) 辅助数据消息;

接收包含所述UE的所述位置的移动发起位置请求 (MO-LR) 响应消息; 或者

执行定位会话以确定所述UE的位置。

5. 根据权利要求3所述的方法, 其中测量所述RTT包括:

从所述基站接收指示针对所述基站的第一本地传输时间的第一消息;

基于针对所述基站的第一本地传输时间和在所述UE中接收到所述第一消息的本地时间来将所述UE中的本地定时与针对所述基站的本地传输时间相关联;

在随机接入信道 (RACH) 上向所述基站传送第二消息, 所述第二消息包括随机变量, 所述第二消息在第一时间被传送, 其中所述第一时间是所述UE中的本地时间或针对所述基站的相关联的本地传输时间;

响应于所述第二消息而从所述基站接收第三消息, 所述第三消息包括第二时间和所述随机变量, 其中所述第二时间是在所述基站处接收到所述第二消息的针对所述基站的本地传输时间; 以及

基于所述第一时间和所述第二时间来确定所述RTT。

6. 根据权利要求5所述的方法, 其中所述第三消息被加密。

7. 根据权利要求5所述的方法, 其中所述第三消息进一步包括针对所述基站的数字签名, 所述方法进一步包括:

基于针对所述基站的数字签名来认证所述第三消息。

8. 根据权利要求3所述的方法, 其中在所述无线网络中在所述UE与所述基站之间存在攻击设备, 其中所述消息是在重放攻击中经由所述攻击设备接收的, 所述方法进一步包括:

根据所述定时提前或通过测量所述RTT来确定所述传播延迟;以及
基于所述传播延迟超出预期范围来检测所述攻击设备的存在。

9.根据权利要求8所述的方法,其中所述预期范围包括基于到所述基站的最大预期距离的最大传播延迟。

10.根据权利要求8所述的方法,所述方法进一步包括:

获得所述UE的所估计位置和所述基站的位置;

确定所述UE的所估计位置与所述基站的所述位置之间的距离估计;以及

基于所述距离估计来确定所述预期范围。

11.根据权利要求1所述的方法,其中所述消息进一步包括以下中的至少一者:所述当前时间到基站子帧或时隙边界的隐式或显式对齐、所述当前时间的不确定性、所述当前时间的源、或它们的组合。

12.根据权利要求1所述的方法,其中所述消息进一步包括针对所述基站的数字签名,所述方法进一步包括:

基于针对所述基站的数字签名来认证该消息中的当前时间。

13.根据权利要求12所述的方法,所述方法进一步包括:

从所述无线网络接收针对所述基站的公共加密密钥,其中所述数字签名基于与所述公共加密密钥对应的私有加密密钥,其中认证所述当前时间使用所述公共加密密钥。

14.一种用户装备 (UE),所述UE被配置成用于支持在无线网络中获取时间,包括:

无线收发器,所述无线收发器被配置成与所述无线网络中的基站进行无线通信;

至少一个存储器;

耦合到所述无线收发器和所述至少一个存储器的至少一个处理器,其中所述至少一个处理器被配置成:

经由所述无线收发器接收从基站广播的消息,所述消息包括当前时间,其中所述当前时间的至少一部分被加密;

通过对所述当前时间的至少所述部分进行解密来获得未加密的当前时间;

确定所述基站与所述UE之间的传播延迟;以及

基于所述未加密的当前时间和所述传播延迟来确定校正的当前时间。

15.根据权利要求14所述的UE,其中所述当前时间包括协调世界时 (UTC) 时间、全球定位系统 (GPS) 时间、GLONASS时间、北斗时间、伽利略时间、全球导航卫星系统 (GNSS) 时间、或本地区域时间。

16.根据权利要求14所述的UE,其中所述至少一个处理器被配置成通过以下中的一者来确定所述传播延迟:

经由所述无线收发器从所述基站获得定时提前,其中所述传播延迟是根据所述定时提前来确定的;

获得所述UE的位置和所述基站的位置,其中所述传播延迟是基于所述UE的所述位置与所述基站的所述位置之间的距离来确定的;或者

测量所述UE与所述基站之间的往返传播时间 (RTT),其中所述传播延迟等于所述RTT的一半。

17.根据权利要求16所述的UE,其中所述至少一个处理器被配置成通过以下中的至少

一者来获得所述UE的位置和所述基站的位置：

经由所述无线收发器在系统信息块 (SIB) 中接收来自所述基站的对所述基站的位置的广播；

经由所述无线收发器接收包含所述基站的位置的长期演进 (LTE) 定位协议 (LPP) 辅助数据消息；

经由所述无线收发器接收包含所述UE的所述位置的移动发起位置请求 (MO-LR) 响应消息；或者

执行定位会话以确定所述UE的位置。

18. 根据权利要求16所述的UE, 其中所述至少一个处理器被配置成通过被配置成进行以下操作来测量所述RTT：

经由所述无线收发器从所述基站接收指示针对所述基站的第一本地传输时间的第一消息；

基于针对所述基站的第一本地传输时间和在所述UE中接收到所述第一消息的本地时间来将所述UE中的本地定时与针对所述基站的本地传输时间相关联；

经由所述无线收发器在随机接入信道 (RACH) 上向所述基站传送第二消息, 所述第二消息包括随机变量, 所述第二消息在第一时间被传送, 其中所述第一时间是所述UE中的本地时间或针对所述基站的相关联的本地传输时间；

经由所述无线收发器响应于所述第二消息而从所述基站接收第三消息, 所述第三消息包括第二时间和所述随机变量, 其中所述第二时间是在所述基站处接收到所述第二消息的针对所述基站的本地传输时间；以及

基于所述第一时间和所述第二时间来确定所述RTT。

19. 根据权利要求18所述的UE, 其中所述第三消息被加密。

20. 根据权利要求18所述的UE, 其中所述第三消息进一步包括针对所述基站的数字签名, 所述至少一个处理器被进一步配置成：

基于针对所述基站的所述数字签名来认证所述第三消息。

21. 根据权利要求16所述的UE, 其中在所述无线网络中在所述UE与所述基站之间存在攻击设备, 其中所述消息是在重放攻击中经由所述攻击设备接收的, 所述至少一个处理器被进一步配置成：

根据所述定时提前或通过测量所述RTT来确定所述传播延迟；以及

基于所述传播延迟超出预期范围来检测所述攻击设备的存在。

22. 根据权利要求21所述的UE, 其中所述预期范围包括基于到所述基站的预期距离的最大传播延迟。

23. 根据权利要求21所述的UE, 其中所述至少一个处理器被进一步配置成：

获得所述UE的所估计位置和所述基站的位置；

确定所述UE的所估计位置与所述基站的所述位置之间的距离估计；以及

基于所述距离估计来确定所述预期范围。

24. 根据权利要求14所述的UE, 其中所述消息进一步包括以下中的至少一者：所述当前时间到基站子帧或时隙边界的隐式或显式对齐、所述当前时间的不确定性、所述当前时间的源、或它们的组合。

25. 根据权利要求14所述的UE, 其中所述消息进一步包括针对所述基站的数字签名, 其中所述至少一个处理器被进一步配置成:

基于针对所述基站的所述数字签名来认证所述消息中的所述当前时间。

26. 根据权利要求25所述的UE, 其中所述至少一个处理器被进一步配置成:

从所述无线网络接收针对所述基站的公共加密密钥, 其中所述数字签名基于与所述公共加密密钥对应的私有加密密钥, 其中认证所述当前时间使用所述公共加密密钥。

27. 一种用户装备 (UE), 所述UE被配置成用于支持在无线网络中获取时间, 包括:

用于接收从基站广播的消息的部件, 所述消息包括当前时间, 其中所述当前时间的至少一部分被加密;

用于通过对所述当前时间的至少所述部分进行解密来获得未加密的当前时间的部件;

用于确定所述基站与所述UE之间的传播延迟的部件; 以及

用于基于所述未加密的当前时间和所述传播延迟来确定校正的当前时间的部件。

28. 根据权利要求27所述的UE, 其中用于确定所述传播延迟的所述部件包括以下中的一者:

用于从所述基站获得定时提前的部件, 其中所述传播延迟是根据所述定时提前来确定的;

用于获得所述UE的位置和所述基站的位置的部件, 其中所述传播延迟是基于所述UE的所述位置与所述基站的所述位置之间的距离来确定的; 或者

用于测量所述UE与所述基站之间的往返传播时间 (RTT) 的部件, 其中所述传播延迟等于所述RTT的一半。

29. 一种包括存储在其上的程序代码的非暂态计算机可读存储介质, 所述程序代码能够操作以配置用户装备 (UE) 中的至少一个处理器以用于支持在无线网络中获取时间, 所述程序代码包括用于进行以下操作的指令:

接收从基站广播的消息, 所述消息包括当前时间, 其中所述当前时间的至少一部分被加密;

通过对所述当前时间的至少所述部分进行解密来获得未加密的当前时间;

确定所述基站与所述UE之间的传播延迟; 以及

基于所述未加密的当前时间和所述传播延迟来确定校正的当前时间。

30. 根据权利要求29所述的非暂态计算机可读存储介质, 其中用于确定所述传播延迟的所述指令包括用于以下中的一者的指令:

从所述基站获得定时提前, 其中所述传播延迟是根据所述定时提前来确定的;

获得所述UE的位置和所述基站的位置, 其中所述传播延迟是基于所述UE的所述位置与所述基站的所述位置之间的距离来确定的; 或者

测量所述UE与所述基站之间的往返传播时间 (RTT), 其中所述传播延迟等于所述RTT的一半。

用于在无线网络中获取可靠时间的方法和装置

[0001] 相关申请的交叉引用

[0002] 本申请要求于2021年7月27日提交的名称为“METHOD AND APPARATUS FOR ACQUISITION OF RELIABLE TIME IN A WIRELESS NETWORK (用于在无线网络中获取可靠时间的方法和装置)”的美国非临时申请第17/386,325号的权益,该专利申请被转让给本申请受让人并通过援引全部明确纳入于此。

背景技术

技术领域

[0003] 本公开一般涉及网络中的无线通信领域,并且更具体地涉及通过无线网络对时间的广播和可靠获取。

[0004] 信息

[0005] 无线通信系统被广泛部署以提供各种类型的通信内容,诸如语音、视频、分组数据、消息接发、广播等等。这些系统可以能够通过共享可用系统资源(例如,时间、频率和功率)来支持与多个用户的通信。此类多址系统的示例包括码分多址(CDMA)系统、时分多址(TDMA)系统、频分多址(FDMA)系统、以及正交频分多址(OFDMA)系统。无线多址通信系统可以包括数个基站,每个基站同时支持多个通信设备的通信,这些通信设备可以各自被称为用户装备(UE)。

[0006] 已经在各种电信标准中采用了这些多址技术以提供公共协议,该协议使得不同的无线设备能够在城市、国家、地区、以及甚至全球层面上进行通信。新兴电信标准的示例是新空口(NR),例如,5G无线电接入。NR是由第三代伙伴项目(3GPP)颁布的LTE移动标准的增强集。它被设计成通过在下行链路(DL)和上行链路(UL)上使用具有循环前缀(CP)的OFDMA以及支持波束形成、多输入多输出(MIMO)天线技术和载波聚集以改善频谱效率、降低成本、改善服务、利用新频谱、以及更好地与其他开放标准进行整合,来更好地支持移动宽带互联网接入。

[0007] 作为向UE提供4G或5G无线接入的一部分,无线网络可向UE提供当前时间(例如,UTC或GPS时间),该当前时间可能非常准确(例如,准确到1微秒(μ s))或不太准确(例如,准确到1秒)。例如,当其他定时源(例如,来自GNSS星座的定时)不可用时(例如,在GNSS的情形中,由于GNSS系统故障、GNSS信号不可用、或干扰或仿冒),这可能很有用。然而,这种定时支持本身可能例如因仿冒而经受可靠性损失。

发明内容

[0008] 由用户装备(UE)在无线网络中从基站获取准确且可靠的时间。该基站可获得该时间,例如协调世界时(UTC)时间或全球导航卫星系统(GNSS)时间,并且在广播该时间之前对该时间的至少一部分进行加密。UE基于定时提前、UE和基站的已知位置、或者UE与基站之间测得的往返传播时间(RTT)来确定UE与基站之间的传播延迟。可以基于从基站接收到的时

间和传播延迟来确定校正时间。与由基站广播的时间包括在一起的数字签名提高了可靠性。UE可基于传播延迟超出预期范围来检测到攻击设备对广播时间的仿冒。

[0009] 在一个具体实施中,一种由用户装备 (UE) 执行的用于支持在无线网络中获取时间的方法包括:接收从基站广播的消息,该消息包括当前时间,其中该当前时间的至少一部分被加密;通过对所述当前时间的至少所述部分进行解密来获得未加密的当前时间;确定该基站与该UE之间的传播延迟;以及基于该未加密的当前时间和该传播延迟来确定校正的当前时间。

[0010] 在一个具体实施中,一种被配置用于支持在无线网络中获取时间的用户装备 (UE) 包括:无线收发器,该无线收发器被配置成与该无线网络中的基站进行无线通信;至少一个存储器;耦合到该无线收发器和该至少一个存储器的至少一个处理器,其中该至少一个处理器被配置成:经由该无线收发器接收从基站广播的消息,该消息包括当前时间,其中该当前时间的至少一部分被加密;通过对所述当前时间的至少所述部分进行解密来获得未加密的当前时间;确定该基站与该UE之间的传播延迟;以及基于该未加密的当前时间和该传播延迟来确定校正的当前时间。

[0011] 在一个具体实施中,一种被配置用于支持在无线网络中获取时间的用户装备 (UE) 包括:用于接收从基站广播的消息的部件,该消息包括当前时间,其中该当前时间的至少一部分被加密;用于通过对该当前时间的至少该部分进行解密来获得未加密的当前时间的部件;用于确定该基站与该UE之间的传播延迟的部件;以及用于基于该未加密的当前时间和该传播延迟来确定校正的当前时间的部件。

[0012] 在一个具体实施中,一种包括存储在其上的程序代码的非暂态计算机可读存储介质,该程序代码能够操作用于配置用户装备 (UE) 中的至少一个处理器以用于支持在无线网络中获取时间,该程序代码包括用于进行以下操作的指令:接收从基站广播的消息,该消息包括当前时间,其中该当前时间的至少一部分被加密;通过对当前时间的至少部分进行解密来获得未加密的当前时间;确定该基站与该UE之间的传播延迟;以及基于该未加密的当前时间和该传播延迟来确定校正的当前时间。

[0013] 在一个具体实施中,一种由基站执行的用于支持由用户装备 (UE) 在无线网络中获取时间的方法包括:获得当前时间;对该当前时间的至少一部分进行加密;以及广播消息,该消息包括该当前时间,其中该UE接收该消息,通过对该当前时间的至少该部分进行解密来获得未加密的当前时间,并且确定该基站与该UE之间的传播延迟,其中该UE基于该未加密的当前时间和该传播延迟来确定校正的当前时间。

[0014] 在一个具体实施中,一种被配置用于支持由用户装备 (UE) 在无线网络中获取时间的基站包括:外部接口,该外部接口被配置成与该无线网络中的实体进行无线通信;至少一个存储器;至少一个处理器,该至少一个处理器耦合到该外部接口和该至少一个存储器,其中该至少一个处理器被配置成:获得当前时间;对该当前时间的至少一部分进行加密;以及广播消息,该消息包括该当前时间,其中该UE接收该消息,通过对该当前时间的至少该部分进行解密来获得未加密的当前时间,并且确定该基站与该UE之间的传播延迟,其中该UE基于该未加密的当前时间和该传播延迟来确定校正的当前时间。

[0015] 在一个具体实施中,一种被配置用于支持由用户装备 (UE) 在无线网络中获取时间的基站包括:用于获得当前时间的部件;用于对该当前时间的至少一部分进行加密的部件;

以及用于广播消息的部件,该消息包括该当前时间,其中该UE接收该消息,通过该当前时间的至少该部分进行解密来获得未加密的当前时间,并且确定该基站与该UE之间的传播延迟,其中该UE基于该未加密的当前时间和该传播延迟来确定校正的当前时间。

[0016] 在一个具体实施中,一种包括存储在其上的程序代码的非暂态计算机可读存储介质,该程序代码能够操作以配置基站中的至少一个处理器用于支持由用户装备 (UE) 在无线网络中获取时间,该程序代码包括用于进行以下操作的指令:获得当前时间;对该当前时间的至少一部分进行加密;以及广播消息,该消息包括该当前时间,其中该UE接收该消息,通过该当前时间的至少该部分进行解密来获得未加密的当前时间,并且确定该基站与该UE之间的传播延迟,其中该UE基于该未加密的当前时间和该传播延迟来确定校正的当前时间。

附图说明

[0017] 呈现附图以帮助描述本公开的各个方面,且提供附图仅用于说明而非限制各方面。

[0018] 图1示出了根据本公开的一方面的无线通信系统的高级系统架构。

[0019] 图2A图示了可在来自基站的消息中广播的当前时间的格式。

[0020] 图2B、图2C和图2D图示了可从基站广播的当前时间的加密。

[0021] 图2E图示了关于可从基站广播的当前时间的附加信息。

[0022] 图3A图示了用于在无线网络中广播和获取时间的信令流。

[0023] 图3B图示了用于在无线网络中广播和获取时间以及确定基站与UE之间的传播延迟的信令流。

[0024] 图4A图示了用于在其中攻击设备存在并执行重放攻击的无线网络中广播和获取时间的信令流。

[0025] 图4B图示了在存在重放攻击的情况下具有增加的可靠性的用于在无线网络中广播和获取时间以及确定基站与UE之间的传播延迟的信令流。

[0026] 图5图示了用于在无线网络中广播和获取时间以及检测由攻击方设备进行的重放攻击的信令流。

[0027] 图6示出了图示被配置成用于支持从无线网络获取当前时间的UE的某些示例性特征的示意框图。

[0028] 图7示出了图示被配置成用于支持从无线网络获取当前时间的基站的某些示例性特征的示意框图。

[0029] 图8示出了由UE执行的用于支持由UE在无线网络中获取时间的示例性方法的流程图。

[0030] 图9示出了由基站执行的用于支持由UE在无线网络中获取时间的示例性方法的流程图。

[0031] 不同附图中具有相同附图标记的元素、阶段、步骤和/或动作可彼此对应(例如,可彼此相似或相同)。此外,各个附图中的一些元素使用数字前缀、继以字母或数字后缀进行标记。数字前缀相同但后缀不同的元素可以是相同类型的元素的不同实例。不带任何后缀的数字前缀在本文中被用于引述具有该数字前缀的任何元素。例如,图1中示出了基站的不

同实例110-1、110-2、110-3。那么,对基站110的引用是指基站110-1、110-2、110-3中的任一者。

具体实施方式

[0032] 本公开的各方面在以下针对出于图示目的提供的各种示例的描述和相关附图中提供。在不脱离本公开的范围的情况下,可以设计出替代方面。另外,将不详细描述或将省略本公开的众所周知的元件,以免使本公开的相关细节难以理解。

[0033] 词语“示例性”和/或“示例”在本文中用于表示“用作示例、示例或说明”。本文中描述为“示例性”和/或“示例”的任何方面不必被解释为优于或胜过其他方面。同样,术语“本公开的各方面”不要求本公开容的所有方面都包括所讨论的特征、优势或操作模式。

[0034] 本领域技术人员将理解,可以使用各种不同的技术和方法中的任何一种来表示下面描述的信息和信号。例如,在以下整个描述中可能提及的数据、指令、命令、信息、信号、比特、符号和码片可以由电压、电流、电磁波、磁场或磁性粒子、光场或光学粒子、或者它们的任何组合来表示,这部分地取决于特定应用、部分地取决于期望的设计、部分地取决于相应的技术,等等。

[0035] 此外,按照要由例如计算设备的元件执行的动作的序列描述了许多方面。将认识到的是,本文描述的各种动作可以由特定电路(例如,专用集成电路(ASIC))、由通过一个或多个处理器执行的程序指令、或者由两者的组合来执行。另外,本文描述的动作序列可被视为完全体现在任何形式的非暂态计算机可读存储介质内,该非暂态计算机可读存储介质中存储有对应计算机指令集,该对应计算机指令集在执行时将致使或指示设备的相关联处理器执行本文描述的功能。因此,本公开的各个方面可以以多种不同的形式来体现,所有这些形式已经被预期在所要求保护的主题的范围内。另外,对于本文描述的各方面中的每个方面,任何这样的方面的对应形式在本文中可以被描述为例如“被配置为执行所描述的动作的逻辑”。

[0036] 如本文所使用的,术语“用户装备”(UE)以及“基站”并非旨在专用于或以其他方式被限定于任何特定的无线电接入技术(RAT),除非另有说明。一般而言,UE可以是被用户用来通过无线通信网络进行通信的任何无线通信设备(例如,移动电话、路由器、平板计算机、膝上型计算机、用于跟踪消费项目、包裹、资产或实体(诸如个人和宠物)的消费者跟踪设备、可穿戴设备(例如,智能手表、眼镜、增强现实(AR)/虚拟现实(VR)头戴式设备等)、交通工具(例如,汽车、摩托车、自行车等)、物联网(IoT)设备等)。UE可以是移动的或者可以(例如,在某些时间)是驻定的,并且可以与无线电接入网(RAN)进行通信。如本文所使用的,术语“UE”可以互换地被称为“接入终端”或“AT”、“客户端设备”、“无线设备”、“订户设备”、“订户终端”、“订户站”、“用户终端”或UT、“移动终端”、“移动站”、“移动设备”、或其变体。总体而言,UE可以经由RAN与核心网通信,并且通过核心网,UE可以与诸如互联网的外部网络以及与其他UE连接。当然,连接到核心网络和/或互联网的其它机制对于UE也是可能的,比如通过有线接入网络、无线局域网(WLAN)网络(例如,基于IEEE 802.11等)等等。

[0037] 基站可取决于其被部署在其中的网络而在与UE处于通信时根据若干种RAT中的一种RAT进行操作,并且可替代地被称为接入点(AP)、网络节点、B节点、演进型B节点(eNB)、新空口(NR)B节点(也被称为gNB)等。此外,在一些系统中,基站可以纯粹提供边缘节点信令功

能,而在其他系统中,基站可以提供附加控制和/或网络管理功能。UE可以借以向基站发送信号的通信链路被称为上行链路(UL)信道(例如,反向业务信道、反向控制信道、接入信道等)。基站可以借以向UE发送信号的通信链路被称为下行链路(DL)或前向链路信道(例如,寻呼信道、控制信道、广播信道、前向业务信道等)。如本文中所使用的,术语业务信道(TCH)可以指代UL/反向或DL/前向业务信道。

[0038] 术语“基站”可以指单个物理传送点或者指可能或可能不共处一地的多个物理传送点。例如,在术语“基站”指单个物理传送点的情况下,该物理传送点可以是与基站的小区相对应的基站天线。在术语“基站”指多个共处一地的物理传送点的情况下,这些物理传送点可以是基站的天线阵列(例如,如在多输入多输出(MIMO)系统中或在基站采用波束形成的情况下)。在术语“基站”指多个非共处一地的物理传送点的情况下,这些物理传送点可以是分布式天线系统(DAS)(经由传输介质来连接到共用源的在空间上分离的天线的网络)或远程无线电头端(RRH)(连接到服务基站的远程基站)。替换地,非共处一地的物理传输点可以是UE接收测量报告的服务基站和该UE正在测量其参考RF信号的邻居基站。

[0039] 获取准确且可靠的时间(诸如协调世界时(UTC))对于现代经济的许多关键基础设施和部门(诸如发电和配电、电信、交通模式、对证券交易所交易加盖时间戳等)以及许多其他的关键和非关键使用情形是必需的。例如,通常从全球导航卫星系统(GNSS)信号获得高度准确的时间。然而,GNSS可能在一些位置(例如,室内)不可用,或者可能例如因仿冒或干扰而发生故障。

[0040] 作为对全球导航卫星系统(GNSS)的故障(例如,仿冒或干扰)的回退,无线网络对可靠定时提供的支持正在成为3GPP和其他标准开发组织(SDO)中的重要领域。除了克服GNSS定时失败之外,使用通过无线网络的定时获取还可在室内使用,其中GNSS有时不可用。用于经由无线网络的定时提供的关键组分是高准确度和高可靠性,例如,以避免定时仿冒并使得接收方能够知晓接收到的定时是否正确和精确。

[0041] 如本文所讨论的,可以通过无线网络获取准确且可靠的时间,基站在该无线网络中广播包括当前时间的消息,该当前时间的至少一部分被加密。当前时间例如可以是协调世界时(UTC)时间、全球定位系统(GPS)时间、GLONASS时间、北斗时间、伽利略时间、全球导航卫星系统(GNSS)时间、或本地区域时间(例如,美国东部标准时间(EST)或太平洋夏令时间(PDT))。接收实体(例如,UE)可对当前时间进行解密。然而,由于广播消息的传播时间,由UE获得的未加密的当前时间可能不准确。相应地,UE可例如基于从基站获得的定时提前、UE和基站的已知位置、或者UE与基站之间测得的往返传播时间(RTT)来确定基站与其自身之间的传播延迟。然后,可基于未加密的当前时间和传播延迟来确定校正的当前时间。可例如使用包括在广播消息中的基站的数字签名来认证当前时间的可靠性。另外,UE还可通过确定具有当前时间的消息是直接从基站而不是经由攻击设备(例如,在重放攻击中)接收的来验证当前时间的可靠性。例如,UE和基站可以执行RTT测量规程以确定传播延迟,并且UE可以通过将测得的RTT与预期的RTT范围(例如,基于到基站的预期距离)进行比较来验证使用重放攻击的攻击设备的不存在。

[0042] 需注意,无线网络可使用多种已知技术来获得准确当前时间,该当前时间可包括能够根据一个或多个GNSS群集、无线网络的一个或多个内部时钟源(例如,原子钟)或可提供时间的外部服务器时钟源(例如,使用网络时间协议(NTP))确定准确时间的参考设备或

参考网络。

[0043] 图1示出了基于非漫游5G NR网络的架构以支持如本文所讨论的由UE通过无线网络获取可靠时间。图1示出了通信系统100,该通信系统包括UE 102和第五代(5G)网络的各组件,该5G网络包括下一代无线电接入网(NG-RAN) 112(其包括基站(BS),该基站有时被称为新空口(NR) B节点或gNB 110-1、110-2和110-3)、下一代演进型B节点(ng-eNB) 114、以及5G核心网(5GCN) 150(其与外部客户端130进行通信)。gNB 110的架构可以被划分成功能部分,其例如包括gNB中央单元(gNB-CU)、一个或多个gNB分布式单元(gNB-DU)和一个或多个gNB远程单元(gNB-RU)中的一者或多者,这些功能部分中的任一者与gNB 110的其他部分可在物理上共处或可在物理上分开。5G网络也可以称为新空口(NR)网络;NG-RAN 112可称为NR RAN或5G RAN;并且5GCN 150可称为下一代(NG)核心网(NGC)。通信系统100可进一步利用来自全球导航卫星系统(GNSS)(如GPS、GLONASS、Galileo、或北斗)、或某个其他本地或区域性卫星定位系统(SPS)(诸如IRNSS、EGNOS或WAAS)的空间飞行器(SV) 190的信息。以下描述了通信系统100的附加组件。通信系统100可包括附加或替换组件。

[0044] 图1示出了UE 102的服务gNB 110-1以及邻居gNB 110-2、110-3和ng-eNB 114。相邻gNB可以是能够接收和测量由UE 102传输的上行链路(UL)信号和/或能够传输可由UE 102接收和测量以支持UE 102的定位的下行链路(DL)参考信号(RS)(例如,定位参考信号(PRS))的任何gNB。

[0045] 应当注意到,图1仅提供了各个组件的一般化图示,其中任何或全部组件可被恰适地利用,并且每个组件可按需重复或省略。具体而言,尽管仅示出了一个UE 102,但是应当理解,许多UE(例如,数百、数千、数百万等)可以利用通信系统100。类似地,通信系统100可包括更大或更小数目的SV 190、gNB 110-1、110-2、外部客户端130和/或其他组件。连接通信系统100中的各个组件的所图示的连接包括数据和信令连接,其可包括附加(中间)组件、直接或间接的物理和/或无线连接、和/或附加网络。此外,可取决于期望的功能性而重新布置、组合、分离、替换和/或省略各组件。

[0046] 虽然图1示出了基于5G的网络,但是类似的网络具体实施和配置可用于其他通信技术,诸如3G、长期演进(LTE)(也称为4G)、以及IEEE 802.11WiFi等。例如,在使用无线局域网(WLAN)(例如IEEE 802.11无线电接口)的情况下,UE 102可以与接入网(AN)(而不是NG-RAN)进行通信,并且相应地,组件112在本文中有时被称为AN或RAN,用术语“RAN”、“(R)AN”或“(R)AN 112”标示。在AN(例如,IEEE 802.11AN)的情形中,AN可以连接到非3GPP互通功能(N3IWF)(例如,在5GCN 150中)(图1中未示出),其中N3IWF连接到AMF 154。

[0047] UE 102可以是任何电子设备并且可被称为设备、移动设备、无线设备、移动终端、终端、移动站(MS)、启用安全用户面定位(SUPL)的终端(SET)或某个其他名称。UE 102可以是独立设备或可嵌入在要被监视或跟踪的另一个设备(例如,工厂工具)中。此外,UE 102可对应于智能手表、数字眼镜、健身监视器、智能汽车、智能家电、蜂窝电话、智能电话、膝上型计算机、平板设备、PDA、用于跟踪消费项目、包裹、资产或实体(诸如个人和宠物)的消费者跟踪设备、控制设备、或某个其他便携式或可移动设备。UE 102可以包括单个实体或者可以包括多个实体,诸如在其中用户可以采用音频、视频、和/或数据I/O设备、和/或身体传感器以及分开的有线或无线调制解调器的个域网中。通常,尽管不是必须的,UE 102可使用一种或多种无线电接入技术(RAT)(诸如GSM、码分多址(CDMA)、宽带CDMA(WCDMA)、LTE、高速率分

组数据 (HRPD)、IEEE 802.11WiFi (也称为Wi-Fi)、Bluetooth® (BT)、微波接入全球互通 (WiMAX)、5G新空口 (NR) (例如,使用NG-RAN 112和5GCN 150) 等) 来支持无线通信。UE 102还可使用无线局域网 (WLAN) 来支持无线通信,无线局域网可使用例如数字用户线 (DSL) 或分组电缆连接到其他网络 (例如,互联网)。使用这些RAT中的一者或多者可允许UE 102与外部客户端130通信 (例如,经由图1中未示出的5GCN 150的元件、或者可能经由网关移动位置中心 (GMLC) 160), 和/或允许外部客户端130 (例如,经由GMLC 160) 接收关于UE 102的位置信息。

[0048] UE 102可进入与可包括NG-RAN 112的无线通信网络的连通状态。在一个示例中, UE 102可以通过向NG-RAN 112中的蜂窝收发器 (诸如gNB 110-1) 传送无线信号或从该蜂窝收发器接收无线信号来与蜂窝通信网络通信。收发器提供朝向UE 102的用户面和控制面协议端接并可称为基站、基收发器站、无线电基站、无线电收发器、无线电网络控制器、收发器功能、基站子系统 (BSS)、扩展服务集 (ESS)、或其他某个合适术语。

[0049] 在特定具体实施中,UE 102可具有能够获得位置相关测量的电路系统和处理资源。由UE 102获得的位置相关测量可包括对于从属于卫星定位系统 (SPS) 或全球导航卫星系统 (GNSS) (诸如GPS、GLONASS、Galileo或北斗) 的卫星飞行器 (SV) 190接收到的信号的测量,和/或可包括对于从固定在已知位置处的地面发射机 (例如,诸如gNB) 接收到的信号的测量。随后,UE 102、或UE 102可以向其发送测量的gNB 110-1可以使用若干定位方法中的任一种基于这些位置相关测量来获得针对UE 102的位置估计,举例而言,这些定位方法诸如GNSS、辅助式GNSS (A-GNSS)、高级前向链路三边测量 (AFLT)、出发角 (AOD)、抵达时间差 (TDOA)、往返时间 (RTT)、WLAN (也称为WiFi) 定位、或增强型小区ID (ECID)、或它们的组合。在这些技术 (例如,A-GNSS、AFLT、AOD、RTT和TDOA) 中的一些技术中,可在UE 102处相对于固定在已知位置处的三个或更多个地面发射器 (例如,gNB) 或相对于具有准确已知轨道数据的四个或更多个SV 190、或它们的组合,至少部分地基于由这些发射器或卫星传输并在UE 102处接收到的导频、定位参考信号 (PRS) 或其他定位相关信号来测量伪距、或定时差。

[0050] 图1中的位置服务器可对应于例如位置管理功能 (LMF) 152或安全用户面定位 (SUPL) 位置平台 (SLP) 162,可以能够向UE 102提供定位辅助数据,包括例如关于要测量的信号的信息 (例如,预期信号定时、信号编码、信号频率、信号多普勒)、地面发射机 (例如,gNB) 的位置和身份、和/或关于GNSS SV的信号、定时和轨道信息,以促成诸如A-GNSS、AFLT、AOD、TDOA、RTT和ECID之类的定位技术。该促成可包括提高由UE 102进行的信号获取和测量准确度,并且在一些情形中,使UE 102能够基于位置测量来计算其估计位置。例如,位置服务器 (例如,LMF 152或SLP 162) 可包括历书 (也被称为基站历书 (BSA)), 该历书指示一个或多个特定区域 (诸如特定场所) 中蜂窝收发器和/或本地收发器的位置和身份,并且可提供描述由蜂窝基站或AP (例如,gNB) 传输的信号的信息,诸如传输功率和信号定时。UE 102可以针对从蜂窝收发器和/或本地收发器接收到的信号获得信号强度测量 (例如,收到信号强度指示 (RSSI)), 和/或可以获得信噪比 (S/N)、参考信号收到功率 (RSRP)、参考信号收到质量 (RSRQ)、抵达时间 (TOA)、抵达角 (AOA)、出发角 (AOD)、接收时间-传输时间差 (Rx-Tx)、或UE 102与蜂窝收发器 (例如,gNB) 或本地收发器 (例如,WiFi接入点 (AP)) 之间的往返信号传播时间 (RTT)。UE 102可使用这些测量连同从位置服务器 (例如,LMF 152或SLP 162) 接收的或在NG-RAN 112中由基站 (例如,gNB 110-1、110-2) 广播的辅助数据 (例如,地面历书数据

或GNSS卫星数据,诸如GNSS历书和/或GNSS星历信息)一起来确定UE 102的位置。

[0051] 在一些具体实施中,使用网络实体来辅助定位UE 102。例如,网络中的实体诸如gNB 110-1、110-2可测量由UE 102传输的UL信号。UL信号可包含或包括UL参考信号,诸如UL定位参考信号 (PRS) 或UL探测参考信号 (SRS)。然后,获得位置测量的实体 (例如,gNB 110-1、110-2) 可将位置测量传递给UE 102或LMF 152,该UE或LMF可使用这些测量来确定多个收发器对的实时差 (RTD)。可使用UL信号的位置测量的示例可包括RSSI、RSRP、RSRQ、TOA、Rx-Tx、AOA和RTT。

[0052] 对UE 102的位置的估计可以称为位置、位置估计、位置锁定、锁定、定位、定位估计或定位锁定,并且可以是地理的,从而提供关于UE 102的位置坐标 (例如,纬度和经度),该位置坐标可以包括或可以不包括海拔分量 (例如,海平面以上的高度;地平面、楼层平面或地下室平面以上的高度或以下的深度)。替代地,UE 102的位置可被表达为市政位置 (例如,表达为邮政地址或建筑物中某个点或较小区域的指定 (诸如特定房间或楼层))。

[0053] 如图1中所示,NG-RAN 112中的成对gNB可以相互连接,例如,如图1中所示的直接地或经由其他gNB 110-1、110-2间接地相互连接。经由UE 102与gNB 110-1、110-2中的一个或多个gNB之间的无线通信来向UE 102提供对5G网络的接入,该一个或多个gNB可使用5G (例如,NR) 代表UE 102来提供对5GCN 150的无线通信接入。在图1中,假定UE 102的服务gNB是gNB 110-1,尽管其他gNB (例如,gNB 110-2、110-3或ng-gNB 114) 在UE 102移到另一位置的情况下可充当服务gNB,或者可充当副gNB来向UE 102提供附加吞吐量和带宽。

[0054] 如所提及的,虽然图1描绘了被配置成根据5G通信协议来进行通信的节点,但是也可以使用被配置成根据其他通信协议 (诸如举例而言LTE协议) 来进行通信的节点。被配置成使用不同协议来进行通信的此类节点可至少部分地由5GCN 150控制。由此,NG-RAN 112可包括以下各项的任何组合:gNB、支持LTE的演进型B节点 (eNB)、或者其他类型的基站或接入点。作为示例,NG-RAN 112可包括一个或多个ng-eNB 114,其向UE 102提供LTE无线接入并且可以连接到5GCN 150中的实体 (诸如AMF 154)。

[0055] gNB 110-1、110-2、110-3和ng-eNB 114可以与接入和移动性管理功能 (AMF) 154通信,该AMF 154出于定位功能性可以与位置管理功能 (LMF) 152通信。AMF 154可支持UE 102的移动性 (包括小区改变和切换),并且可参与支持去往UE 102的信令连接并且可能帮助建立和释放UPF 158所支持的UE 102的协议数据单元 (PDU) 会话。AMF 154的其他功能可包括:端接来自NG-RAN 112的控制面 (CP) 接口;端接来自UE (诸如UE 102) 的非接入阶层 (NAS) 信令连接;NAS加密和完好性保护;注册管理;连接管理;可达性管理;移动性管理;接入认证和授权。

[0056] 当UE 102接入NG-RAN 112时,gNB 110-1可支持对UE 102的定位。gNB 110-1还可处理例如直接地或间接地从GMLC 160接收的对UE 102的位置服务请求。在一些实施方案中,实现gNB 110-1的节点/系统可附加地或替代地实现其他类型的位置支持模块,诸如增强型服务移动位置中心 (E-SMLC) 或安全用户面位置 (SUPL) 位置平台 (SLP) 162。将注意,在一些实施方案中,定位功能性 (包括推导UE 102的位置) 的至少一部分可以在UE 102处执行 (例如,使用针对由无线节点传送的信号的信号测量以及提供给UE 102的辅助数据)。

[0057] GMLC 160可以支持从外部客户端130接收到的针对UE 102的位置请求,并且可以将此类位置请求转发给UE 102的服务AMF 154。然后,AMF 154可将位置请求转发给gNB

110-1或LMF 152;该gNB或LMF可获得UE 102的一个或多个位置估计(例如根据来自外部客户端130的请求)并且可将该位置估计返回给AMF 154,该AMF可经由GMLC 160将该位置估计返回给外部客户端130。GMLC 160可包含针对外部客户端130的订阅信息,并且可认证和授权来自外部客户端130的针对UE 102的位置请求。GMLC 160可进一步通过向AMF 154发送针对UE 102的位置请求来发动针对UE 102的位置会话,并且可在该位置请求中包括UE 102的身份和所请求的位置(例如,诸如当前位置、或者一系列周期性或触发式位置)的类型。

[0058] 如所图示的,统一数据管理(UDM)161可连接到GMLC 160。UDM 161类似于用于LTE接入的归属订户服务器(HSS),并且如果需要,则UDM 161可与HSS组合。UDM 161是中央数据库,其包含用于UE 102的用户相关和订阅相关信息并可执行以下功能:UE认证、UE识别、接入授权、注册和移动性管理、订阅管理和短消息服务管理。

[0059] 如图1中进一步图示的,外部客户端130可经由GMLC 160和/或SLP 162连接到核心网150。外部客户端130可以可任选地连接到核心网150和/或经由互联网175连接到在5GCN 150外部的SLP 164。外部客户端130可以是服务器、web服务器、或用户装备,诸如个人计算机、UE等。

[0060] 网络开放功能(NEF)163可以连接到GMLC 160和AMF 154。在一些具体实施中,可连接到NEF 163以直接与外部客户端130或与应用功能的(AF)132进行通信。NEF 163可支持关于5GCN 150和UE 102的能力和事件对外部客户端130或AF 132的安全开放,并且可实现信息从外部客户端130或AF 132到5GCN 150的安全供应。NEF 163例如还可用于获得针对UE 102的当前或最后已知位置,可获得针对UE 102的位置变化的指示、或UE 102何时变得可用(或可达)的指示。外部客户端130或AF 132可访问NEF 163以便获得UE 102的位置信息。

[0061] LMF 152和gNB 110-1可使用新空口定位协议A(NRPPa)来进行通信。NRPPa可以在3GPP TS 38.455中定义,其中在gNB 110-1与LMF 152之间传递NRPPa消息。此外,LMF 152和UE 102可使用3GPP TS 37.355中所定义的LTE定位协议(LPP)来进行通信,其中经由服务AMF 154以及UE 102的服务gNB 110-1在UE 102与LMF 152之间传递LPP消息。LPP协议可用于支持使用UE辅助的定位方法和/或基于UE的定位方法(诸如辅助式GNSS(A-GNSS)、实时运动学(RTK)、无线局域网(WLAN)、出发角(AOD)、抵达时间差(TDOA)、往返时间(RTT)和/或增强型小区身份(ECID))来定位UE 102。NRPPa协议可用于支持使用基于网络的定位方法(诸如ECID)(当与由gNB 110-1、110-2、110-3或ng-eNB 114获得或从中获得的测量一起使用时)来定位UE 102和/或可由LMF 152用来获得来自gNB 110的位置相关信息,诸如定义来自gNB的定位参考信号(PRS)传输以支持TDOA的参数。

[0062] gNB 110-1、110-2、110-3或ng-eNB 114可使用下一代应用协议(NGAP)(例如,如3GPP技术规范(TS)38.413中所定义的)来与AMF 154通信。NGAP可使AMF 154能够向UE 102的gNB 110-1请求UE 102的位置,并且可使gNB 110-1能够向AMF 154返回UE 102的位置。

[0063] gNB 110-1、110-2、110-3或ng-eNB 114可使用Xn应用协议(XnAP)(例如,如3GPP TS 38.423中所定义的)相互通信。XnAP可允许一个gNB 110请求另一gNB 110获得针对UE 102的UL位置测量并返回这些UL位置测量。XnAP还可使gNB 110能够请求另一个gNB 110传输下行链路(DL)RS或PRS以使UE 102能够获得所传输的DL RS或PRS的DL位置测量。

[0064] gNB(例如,gNB 110-1)可以使用(例如,如在3GPP TS 38.331中定义的)无线电资源控制(RRC)协议与UE 102通信。RRC可允许gNB(例如,gNB 110-1)向UE 102请求对由gNB

110-1和/或由其他gNB 110-2、110-3或ng-eNB 114传送的DL RS或DL PRS的位置测量并返回这些位置测量中的一些或全部。RRC还可使得gNB (例如,gNB 110-1)能够请求UE 102传送UL RS或PRS,以使得gNB 110-1或者其他gNB 110-2、110-3或ng-eNB 114能够获得所传送的UL RS或PRS的UL位置测量。

[0065] 如所图示的,会话管理功能(SMF)156连接AMF 154和UPF 158。SMF 156可管理用于UE 102的PDU会话的建立、修改和释放,执行用于UE 102的IP地址分配和管理,充当UE 102的动态主机配置协议(DHCP)服务器,以及代表UE 102来选择和控制UPF 158。

[0066] 用户面功能(UPF)158可支持UE 102的语音和数据承载,并且可使UE 102能够对其他网络(诸如互联网175)进行语音和数据接入。UPF 158的功能可包括:至数据网络的外部PDU会话互连点、分组(例如,网际协议(IP))路由和转发、分组检视和策略规则实施的用户面部分、用户面的服务质量(QoS)处置、下行链路分组缓冲以及下行链路数据通知触发。UPF 158可被连接到SLP 162,以使用由开放移动联盟(OMA)所定义的SUPL定位解决方案来实现对UE 102的定位的支持。SLP 162可进一步连接到外部客户端130或从该外部客户端访问。

[0067] 为了支持UE 102获取可靠时间,gNB 110和/或ng-eNB 114中的一者或多者可包括能够接收、解码和处理来自属于一个或多个GNSS星座的太空交通工具(SV)的信号的GNSS接收机。例如,该信号可以是导航信号并可指示准确时间(例如,GPS时间或UTC时间)。在一些其他情况下,gNB 110可连接到能够向gNB 110提供准确GNSS时间的GNSS参考网络。另外,gNB 110(和/或ng-eNB 114)可能够交换定时信息以便:(i)向没有GNSS接收器并且未连接到GNSS参考网络或具有GNSS接收器但是当前不能从GNSS SV接收信号的gNB 110或ng-eNB 114提供准确时间;(ii)比较时间信息以便检测由一个或多个gNB 110(或ng-eNB 114)进行的时间确定是否可能出错(例如,由于外部干扰或仿冒);以及/或者(iii)通过组合(例如,平均)来自多个gNB 110的时间确定来提高定时准确度。附加地或替代地,一个或多个gNB 110和/或ng-eNB 114可从AMF 154或UPF 158接收准确定时信息(例如,使用NTP)。AMF 154和/或UPF 158又可从像UDM 161或NEF 163那样的某个其他实体接收准确定时,这些其他实体又可包含或连接到准确时间源(例如,原子钟)或可从某个外部时间源(例如,GNSS参考网络或由政府机构拥有和操作的的安全服务器)接收时间。由gNB 110或ng-eNB 114获得的定时信息(例如,其经由AMF 154或UPF 158从UDM 161或NEF 163接收到)可包括时间源的标识(例如,可以标识政府运行的原子钟源或GNSS参考网络),并且可以指示准确度水平(例如,可以指示时间精确到1 μ s、1毫秒(ms)或1秒)。由gNB 110或ng-eNB 114确定或向其提供准确当前时间可使gNB 110或ng-eNB 114能够向UE 102提供准确时间,如本文所述。

[0068] 应当理解,虽然图1示出了用于非漫游UE的网络架构,但通过适当的、众所周知的改变,可以提供用于漫游UE的相应网络架构。

[0069] 如以上所讨论的,获取准确且可靠的时间对于现代经济的许多关键基础设施和部门以及许多其他关键和非关键使用情形是必需的。例如,高度准确的时间可由UE(诸如UE 102)从来自SV 190的GNSS信号接收。然而,在一些场景中,来自SV 190的信号可能不可用,诸如在室内或在城市峡谷位置中。附加地,来自SV 190的信号可能因攻击诸如仿冒或干扰而不可用。

[0070] 可以由UE 102通过无线系统100获取当前时间。例如,gNB 110可广播消息,该消息可由UE 102接收并可包括当前时间。gNB 110例如可来自SV 190或来自实体(诸如核心网

150中的AMF 154或UPF 158)的信号获得当前时间,如先前所述。作为示例,当前时间可以是UTC时间、GPS时间、GLONASS时间、北斗时间、伽利略时间、GNSS时间或本地时间(例如,EST或PDT)。gNB 110可周期性地在一个或多个消息中(例如,在系统信息块(SIB)中)向UE 102提供当前时间。

[0071] 作为示例,图2A图示了可在来自gNB 110的消息中广播的当前时间200的格式。当前时间200可以是UTC时间、GPS时间、GLONASS时间、北斗时间、伽利略时间、GNSS时间或本地时间(例如,EST或PDT)等。当前时间200可根据ISO 8601或任何其他期望格式表达。如图2A中所图示的,在UTC时间的情形中,当前时间200可包括年(yyyy)、月(MM)、周(ww)、日(D)、小时(hh)、分钟(mm)、秒(ss)和秒的分数(f...)。秒的分数(f...)可以是十进制分数,并且可包括如所需的十进制位。众所周知,UTC时间可通过对于第二(ss)字段分别包括“60”值或省略“59”值来适应闰秒的增加或减少。当然,如果需要,可使用其他格式,例如,可不包括周,并且可使用两个数字(DD)来表达天等。在GPS时间、伽利略时间或北斗时间的情况下,时间可表达为自某个开始时间(例如,在GPS的情况下,1980年1月5日到6日00:00UTC(午夜))以来已经过去的秒数。此外,在一些情况下,当前时间200有时可被提供作为自先前提供的时间以来的时间间隔。

[0072] 由gNB 110广播的定时信息可以被完全加密,或者定时信息的一部分可以被加密。具有接收加密的时间的订阅的UE 102可从gNB 110或从5GCN 150中的实体(例如,AMF 154)接收加密密钥,该加密密钥例如可在UE 102执行向5GCN 150的注册时提供(例如,由AMF 154提供)。UE 102可使用加密密钥来对加密的定时信息或定时信息的被加密的部分进行解密。加密可使用任何加密算法,诸如由美国国家标准与技术协会(NIST)定义的高级加密标准(AES)算法中的一种AES算法。例如,在一个实施方案中,可使用AES计数器模式算法。在这种情况下,可在传达当前时间的每个广播消息(或SIB)中使用不同计数器。由于广播消息中的加密的比特的数目可以小于加密密钥中的比特的数目(例如,在下文关于图2C和图2D所述的变体的情况下),因此在一些情况下,使用公共密文流(例如,在AES计数器模式的情况下)对连续广播消息(或连续广播消息的部分)进行加密和指示用于每个广播消息的密文流的部分可更容易、更方便或更安全。

[0073] 例如,由gNB 110进行的加密将使基于订阅的服务能够获得高度准确的定时信息,并且可以辅助确保定时信息的可靠性。在一些具体实施中,可以仅加密低阶比特或字段,这将允许没有加密密钥的UE 102获得近似时间(例如,如果仅加密分数秒,则精确到1秒),而具有加密密钥的UE 102可以获得更准确的时间(例如,精确到1 μ s)。

[0074] 作为示例,图2B、图2C和图2D图示了在来自gNB 110的消息中广播的当前UTC时间200的格式,其中阴影表示当前时间200的加密的部分。如图2B所示,所有当前时间200可被加密。另一方面,如关于图2C中的阴影所图示的,可以加密仅秒的分数,这准许任何UE 102以1秒的准确度获得当前时间,而具有加密密钥的UE 102可以获得更准确的时间。图2D图示了当前时间200的扩展格式,其示出秒的分数(例如,十分之一、百分之一、千分之一、千分之十等)的单独单位,并且用阴影图示了一些分数(例如,十分之一和百分之一)可未加密,并且更低阶(例如,千分之一和以下)可被加密。

[0075] 图2E图示了可由gNB 110连同在向UE 102广播的消息(例如,SIB)中的当前时间一起包括的附加信息。该信息可包括当前时间(例如,UTC以及如图2A至图2D中的任一个图中

的那样)、gNB 110处的本地传输时间(其可用于更精确地指示当前时间,如下文所述,并且如果消息传输与gNB 110的本地传输时间帧和/或子帧结构相关联或是其一部分,则其包括内容或指示可以是隐式的)、当前时间的源(例如,GPS、伽利略、GLONASS、北斗、GNSS、本地原子钟、具有原子钟的外部服务器、GNSS参考网络、gNB 110的本地时钟)和/或当前时间的准确度或不确定性(例如,1秒、1ms或1 μ s)以及在一些情况下的数字签名(DigSig)。数字签名(DigSig)的目的可以是提高由UE 102接收的当前时间的可靠性,这可能是重要考虑因素,特别是对于关键使用情况。为了使当前时间信息更可靠,连接到无线网络(例如,5GCN 150)的UE 102可首先使用现有(例如,3GPP)安全机制来认证无线网络并建立到无线网络(例如,到服务gNB 110-1和/或服务AMF 154)的安全(例如,加密)连接。网络实体(例如,服务AMF 154或服务gNB 110-1)随后可以向UE 102提供适用于一个gNB 110(例如,服务gNB 110-1)或许多或所有gNB 110的公共加密密钥(也被称为公钥)。gNB 110可以随后广播当前时间(例如,在SIB消息中),并且包括数字签名(DigSig)以基于仅对该网络已知的对应的私有加密密钥(也被称为私钥)来认证当前时间。认证只能不频繁地执行(例如,通过每分钟或每五分钟包括一次DigSig)以减少额外的信令和处理。如果UE 102使用公钥来认证数字签名,则UE 102可信任所接收的当前时间。网络实体和UE可诸如基于RSA算法或数字签名算法(DSA)来使用任何标准类型的数字签名。

[0076] 需注意,使用如上文所述的数字签名的公钥-私钥形式的认证可以比基于对当前时间的所有或部分进行加密的认证(如图2B至图2D所示)更可靠。这是因为加密通常将基于gNB 110和UE 102两者已知的单个加密密钥,该加密密钥可由攻击设备容易地获得(例如,从无线网络或从UE 102)。然而,在公钥-私钥对的情况下,私钥不被公开给UE 102并仅在无线网络内已知。

[0077] 图3A图示了用于在包括gNB 110和UE 102的无线网络中广播和获取可靠时间的信令流300,其中纵轴表示时间(其中时间在向下方向上增加),并且横轴表示实体之间的距离。图3A作为非限制性示例提供。例如,图3A图示了5G网络实体(即,gNB 110或ng-eNB 114)的使用,但是如果需要,可以使用其他类型的网络,诸如其中可使用eNB来代替gNB 110的LTE网络。附加地,将理解,可存在附加信令和过程,并且由gNB 110发送的消息可包括附加组件。

[0078] 如所例示,在当前时间T处或接近该当前时间(例如,在1 μ s或1ms内),gNB 110广播消息302,该消息由UE 102在时间T+ Δ 处接收。消息302可被包括在系统信息块(SIB)中并包括当前时间T,并且可包括在gNB 110处的相关联的本地传输时间t的隐式或显式指示(例如,诸如下一子帧的开始或当前子帧的结束)。该关联可以是当本地时间正好是t时当前时间正好是T。隐式本地时间t可在(例如)3GPP TS中定义并可不被显式地包括在消息302中。本地时间t可实现当前时间T的更准确的传达,并且可不要求gNB 110在正好是时间T时广播消息302。在没有本地时间t的情况下,gNB 110可能需要在时间T上或尽可能接近时间T来广播消息302,并且UE 102可能需要对消息302的到达加时间戳。当前时间T例如可以是UTC时间、GPS时间、GLONASS时间、北斗时间、伽利略时间、GNSS时间、或本地区域时间(例如,EST或PDT)。例如,gNB 110可以获得当前时间T,如先前所描述的--例如,可以从SV 190或另一个网络实体(诸如图1中所示的AMF 154)周期性地获得T,并且可以在来自SV 190或其他网络实体的更新之间的短时段内使用本地时钟来维持时间T。本地时钟例如还可维持NG-RAN

112中的gNB 110的本地传输时间 t 。如上文所讨论,当前时间 T 的至少一部分可由gNB 110加密,如关于图2B至图2D所述。

[0079] 在一些具体实施中,消息302可包括附加信息,例如,如针对图2E所描述的。在一个示例中,消息302可包括或引用本地时间 t (例如,如上文所述),该本地时间 t 可指示当前时间 T 与由gNB 110传输的子帧边界或时隙边界的对齐(或关联)。在一个示例中,消息302可包括当前时间 T 的不确定性。在一个示例中,消息302可包括当前时间 T 的源,例如,当前时间 T 是否从SV或网络实体获得,以及当前时间是UTC时间、GPS时间、GLONASS时间、北斗时间、伽利略时间、GNSS时间等。消息302可包括另外的附加信息(例如,如针对图2E所描述的的数字签名)和/或前述的任何组合。

[0080] 由于具有当前时间 T 的广播消息302将从gNB 110在信号传播延迟 Δ 之后抵达UE 102,则由UE 102在时间 $T+\Delta$ 处获得的消息302中的当前时间 T 对于一些使用情形可能不够准确。无论消息302是否包括隐式或显式本地时间 t ,这都可适用。当不包括(隐式地或显式地)本地时间 t 时,UE 102可仅假定当前时间 T 适用于在 $T+\Delta$ 上接收到消息302的时间(例如,接收到消息302的开始或消息302的结束的时间)并因此可能具有等于 Δ 的误差。当包括或指示(隐式地或显式地)本地时间 t 时,UE 102可将当前时间 T 与从gNB 110接收的特定传输时间 t (诸如当前或下一子帧或时隙的开始或结束)相关联。这种关联通常将对于gNB 110处的传输是正确的,但是当本地传输时间 t 指示(例如,子帧或时隙的开始或结束)已经抵达UE 102时将延迟时间 Δ ,这将再次导致误差 Δ 。

[0081] 因此,提供高度准确的当前时间 T 可能需要UE 102确定其自身与gNB 110之间的传播延迟 Δ 的能力。在具有传播延迟 Δ 的知识的情况下,UE 102可以向所接收的当前时间 T 添加传播延迟 Δ ,以在由UE 102接收到广播消息302的时间处或在由UE 102接收到隐式或显式本地时间 t 的时间处获得正确的当前时间 $T+\Delta$ 。

[0082] UE 102可以各种方式确定广播gNB 110与其自身之间的传播延迟 Δ 。例如,UE 102可在另一个消息(图3A未示出)诸如用于NR无线电接口的无线电资源控制(RRC)协议或介质访问控制(MAC)协议的消息中从gNB 110获得定时提前(TA)。TA可指示UE 102到gNB 110的传输将在从gNB 110接收到的传输定时之前的时间间隔。例如,如果UE 102在本地UE时间 $T1$ 从gNB 110接收到新子帧的开始,则UE 102可支持向gNB 110的传输定时,使得UE 102在本地UE时间 $T1$ 至TA向gNB 110传输新子帧的开始。TA值对于每个UE 102可以是单独的,并且可由gNB 110使用以确保来自所有支持的UE 102的传输由gNB 110以同步方式接收(例如,其中gNB 110同时从所有支持的UE 102接收新子帧的开始)。在一些情况下,可由所有UE 102将定时提前偏移添加到TA值,而不影响用于在gNB 110处同步来自不同UE 102的传输的到达时间的使用。通常(并且众所周知),TA值等于UE 102与gNB 110之间的往返信号传播时间(RTT)。因此,单向传播延迟可作为TA值的一半获得(并因此 $\Delta = TA/2$)。使用定时提前的限制是UE 102通常是需要处于RRC CONNECTED状态并具有到gNB 110的RRC信令连接。因此,定时提前的使用可能不适用于从gNB 110接收当前时间 T 的处于RRC IDLE状态或RRC INACTIVE状态的UE 102。

[0083] 在另一个具体实施中,UE 102可使用已知定位技术来确定到gNB 110的范围(例如,距离),并且可基于无线信号的速度来将该范围转换成传播延迟 Δ ($\Delta = \text{范围}/c$,其中 c 是光速)。

[0084] 例如,在一些具体实施中,UE 102可以使用例如在基于UE的定位技术中的已知定位技术(诸如A-GNSS、WiFi、DL-TDOA、DL-AOD、多小区RTT、ECID等)在与位置服务器(例如,LMF 152或SLP 162)的定位会话中获得其位置,并且可以获得广播方gNB 110的位置。UE 102可基于UE 102和gNB 110的位置之间的距离来确定到gNB 110的范围。在一些具体实施中,gNB 110的位置可由UE 102从来自gNB 110的包括gNB 110的位置的所广播的SIB消息或从包括在定位会话期间经由gNB 110从位置服务器(例如,LMF 152或SLP 162)接收到的gNB 110的位置的LPP辅助数据消息获得。UE 102的位置可由位置服务器(例如,LMF 152或SLP 162)响应于移动发起位置请求(MO-LR)而使用例如UE辅助定位技术中的已知定位技术(诸如A-GNSS、WiFi、DL-TDOA、DL-AOD、多小区RTT、ECID等)来确定,并且位置服务器随后可在MO-LR响应消息中向UE 102发送该位置。UE 102的位置还可由UE 102在不使用例如基于UE的定位技术或独立定位技术中的已知定位技术(诸如GNSS、A-GNSS、WiFi、DL-TDOA、DL-AOD、多小区RTT、ECID等)与位置服务器交互的情况下确定。

[0085] 在另一个示例中,UE 102可基于UE 102与gNB 110之间的往返传播时间(RTT)(例如,传播延迟 Δ 是RTT的一半)来确定到gNB 110的距离。RTT以及因此传播延迟 Δ 例如可使用随机接入信道(RACH)来测量。为了将RACH规程限制到仅那些订阅高准确度当前时间T的UE,可以使用仅那些订阅高准确度当前时间的UE知晓的加密密钥来执行gNB RACH响应消息的加密。例如,相同加密密钥可用于对如图2B至图2D中的当前时间的部分或全部进行加密和对gNB RACH响应消息的部分或全部进行加密。这可以限制gNB 110上支持RTT确定的负载。

[0086] 图3B类似于图3A并图示了用于在无线网络中广播和获取可靠时间的信令流350,包括用于确定gNB 110与UE 102之间的传播延迟 Δ 的RTT规程。图3B作为非限制性示例提供。例如,将理解,可存在附加信令和过程,并且在gNB 110与UE 102之间发送的消息可包括附加组件。图3B中所示的规程的益处在于,其可由处于RRC IDLE或RRC INACTIVE状态并且其中定时提前可能不可用的UE 102使用。

[0087] 如所例示,类似于图3A所示的消息302,在当前时间T处或接近该当前时间,gNB 110广播消息352,该消息由UE 102在时间 $T + \Delta$ 上接收。消息352可与图3A中的消息302相同或类似。因此,消息352可被包括在SIB中,当前时间T的至少一部分可被加密,并且消息352可包括附加信息,诸如在gNB 110处的隐式或显式本地NR传输时间 t 、当前时间T到基站子帧或时隙边界的对齐的隐式或显式指示、当前时间T的不确定性、当前时间T的源或它们的组合。UE 102可基于先前获得的加密密钥来对当前时间T以及(如果也被加密的话)附加信息进行解密以获得未加密的当前时间T(以及未加密的附加信息)。

[0088] gNB 110可以在gNB 110的本地时间 t 处向UE 102传送消息或信号354。消息或信号354例如可以是同步信号块(SSB)或信道状态信息参考信号(CSI-RS)。消息或信号354可包括或可指示传输的本地时间 t 。UE 102可基于所接收的本地传输时间 t 和在UE 102中接收到消息或信号354的本地时间来将UE中的本地定时(例如,UE 102的内部定时源或内部时钟)与gNB 110的本地传输时间相关联。

[0089] 响应于消息或信号354,UE 102可以向gNB 110发送消息356,其可以是例如作为RACH请求消息的RRC消息。消息356可以由UE 102在针对gNB 110的RACH上传送。UE 102可以在消息356中包括随机变量(RV)(例如,包括8到16比特的随机比特串)。在第一时间(例如,

其可以对应于消息356的开始或结束的传输时间)处传送消息356,该第一时间可以是UE的本地时间或针对gNB 110的相关本地传输时间。消息356由gNB 110在第二时间(例如,本地时间 $t+2\Delta$)接收。注意,图3B图示了如在UE 102处接收到消息或信号354时发生的第一时间,并且因此其中第一时间对应于在消息或信号354中包括的或由该消息或信号354指示的本地时间 t 。然而,第一时间也可以在消息或信号354抵达UE 102之后不久(例如,1到100ms之后)发生,在该情形中,第一时间可以对应于UE 102已知并且超过 t 的针对gNB 110的某个本地传输时间。

[0090] gNB 110获得(例如,测量)消息356的抵达时间(例如,消息356的开始或结束的抵达时间)并且响应于消息356而向UE 102返回响应消息358。响应消息358例如可以是在gNB 110的公共控制信道(CCCH)上传输的RRC消息。如以上所讨论的,为了将RACH规程限制到仅那些订阅高准确度当前时间 T 的UE,可以使用仅那些订阅高准确度当前时间的UE知晓的加密密钥来加密响应消息358。因此,如果被加密的话,则UE 102可对响应消息358的部分或全部进行解密。响应消息358可包括来自消息356的随机变量(RV)并包括第二时间,例如,在gNB 110处接收到消息356的本地时间(在该示例中, $t+2\Delta$)。需注意,在本文所述的所有规程中将需要一致地测量传输和接收时间,使得用于相同消息的时间应用于该消息的相同部分,例如该消息的开始或结束。因此,本文所描述的第一和第二时间可都适用于消息356的开始,或者可都适用于消息356的结束。

[0091] UE 102接收响应消息358并识别随机变量(RV)。UE 102随后可基于从响应消息358获得的第一时间(例如, t 的已知值)和第二时间(例如,在该示例中的 $t+2\Delta$ 的值)来获得传播延迟 Δ 。在了解传播延迟 Δ 的情况下,UE 102可向在消息352中所接收的当前时间 T 添加传播延迟 Δ ,以在广播消息352的接收时间处或在相关联的本地时间 t (如果其针对消息352被隐式地或显式地包括或指示)处获得正确的当前时间 $T+\Delta$ 。应当理解,由消息354、356和358例示的RTT规程(以及用于确定UE 102的位置的任何定位规程)可能不一定在接收到消息352之后发生。例如,RTT规程(或定位规程)被执行以获得传播延迟 Δ 并可在接收到当前时间 T 之前或之后发生。此外,如果UE 102不移动或缓慢地移动,则RTT规程(或定位规程)不一定需要在时间上接近到当前时间 T 来执行。

[0092] 如果UE 102未接收到响应消息358(例如,在传送消息356之后的某个最大预期响应时间之后),则UE 102可以在稍后的时间 t' 处重传消息356(图3B中未示出)并且等待接收与响应消息358类似的响应消息(图3B中未示出)。例如,如果gNB 110未正确地接收到消息356(例如,由于干扰或由于来自UE 102的用于消息356的传输的过低传输功率),则可能发生这种情况。对于消息356的重传并假设gNB 110为此与响应消息358类似地发送响应消息,UE 102可使用时间 t' 而不是时间 t 来获得如上所述的传播延迟 Δ 。

[0093] 由UE 102接收到的当前时间 T 的可靠性可以是尤其是对于关键使用情形的重要考虑因素。为了使当前时间信息可靠,连接到无线网络的UE 102可首先使用现有安全机制来认证无线网络。网络实体(例如,AMF 154或gNB 110)随后可以向UE 102提供适用于一个gNB 110(例如,服务gNB 110-1)或者适用于许多或所有gNB 110的公共加密密钥。然后,gNB 110可例如在SIB消息302或352中广播当前时间 T ,并且包括数字签名(DigSig)以基于仅对网络已知的对应私钥来认证当前时间 T 。认证可能仅不频繁地执行(例如,每分钟一次或每5分钟一次)以减少额外的信令和处理。如果使用公钥来认证数字签名,则UE 102可信任所接收的

当前时间T。

[0094] 使用与当前时间T一起被包括的数字签名可提高当前时间T的可靠性。例如,除了重放攻击之外,数字签名可防止某个攻击实体对当前时间T的仿冒,因为在所包括的当前T是尚未由gNB 110传输的未来时间的情况下,攻击实体将无法在由该攻击实体朝向UE 102传输的与消息302或消息352类似的消息中包括正确数字签名。然而,在重放攻击中,攻击实体可获得从gNB 110广播的当前时间T并在稍后(延迟)时间向UE 102重新发送当前时间T和数字签名,由此在UE 102中引起早于正确当前时间的不正确时间。作为示例,在图1中,攻击设备108可从gNB 110-1接收包含当前时间T的所广播的消息(与数字签名等一起)并可以在重放攻击中向UE 102发送该消息。仅经由数字签名不能检测重放攻击,因为数字签名被包括在所重放的消息中。因此,当UE 102接收到来自攻击设备108的所重放的消息时,UE 102可认为当前时间是 $T + \Delta$,而实际上此时当前时间可能因延迟而晚得多。

[0095] 图4A类似于图3A,并且图示了用于在其中攻击设备108存在并正在执行重放攻击的包括gNB 110和UE 102的无线网络中广播和获取可靠时间的信令流400。

[0096] 如所例示,在当前时间T处或接近该当前时间(例如,在当前时间T的 $1\mu\text{s}$ 或 1ms 内),gNB 110广播消息402,该消息由UE 102在时间 $T + \Delta$ 处或接近该时间接收。消息402可与关于图3A和图3B所述的消息302和352相同或类似。因此,消息402可以是SIB消息,并且可包括当前时间T、可任选的隐式或显式本地时间 t 和数字签名(DigSig)。消息402可另外包括或指示当前时间T到基站子帧或时隙边界的对齐、当前时间的不确定性、当前时间的源、或它们的组合。攻击设备108可接收消息402,并且在延迟 $\Delta 1$ 之后,可在重放攻击中发送消息403,该消息由UE 102在时间 $T + \Delta + \Delta 1$ 处接收。延迟 Δ 可包括从gNB 110到攻击设备108的传播时间加上从攻击设备108到UE 102的传播时间。延迟 $\Delta 1$ 可包括在攻击设备108处接收消息402(例如,该消息的开始)与传输消息403(例如,该消息的开始)之间的延迟。消息403可以是消息402的副本,并且因此,可包括当前时间T(其可至少部分地由gNB 110加密)、以及针对gNB 110的数字签名(DigSig)。UE 102可对当前时间的至少该部分进行解密以获得未加密的当前时间。

[0097] 在UE 102未检测到攻击设备108的情况下,UE 102可能不当地依赖于消息403中的所接收的当前时间T,其可具有至少 $\Delta 1$ 的误差。因此,可能期望UE 102通过确定具有当前时间T的消息是直接从gNB 110而不是经由攻击设备108(例如,在重放攻击中)接收来验证当前时间T的可靠性。

[0098] 当前时间T的可靠性的验证可由UE 102通过周期性地验证UE 102与gNB 110之间的传播延迟在预期范围内或等于预期值来执行。如果UE 102处于RRC CONNECTED状态,则UE 102可周期性地从gNB 110接收定时提前(TA),如前所述,该定时提前可用于确定传播延迟(作为TA的一半)。由于gNB 110与处于RRC CONNECTED中的UE 102之间的通信可以攻击设备108无法(或非常难以)解密或修改的方式加密,因此攻击设备108可能无法伪造或仿冒定时提前,并且因此,如果执行重放攻击,则UE 102可接收定时提前,UE 102然后可如下文进一步所述的那样处置该定时提前以确定是否可存在攻击设备108。

[0099] 然而,如果UE 102处于RRC IDLE或RRC INACTIVE状态,则UE 102可能未接收到来自gNB 110的定时提前,并且可能需要使用与针对图3B描述的规程类似的规程来测量与gNB 110的传播延迟,但利用一些附加功能来实现对攻击设备108的检测(在攻击设备108存在

时)。然后,UE 102可使用类似于图3B所示的RACH规程的RACH规程来周期性地获得gNB 110到UE 102的传播延迟 Δ 。如果攻击设备108要阻止RACH规程或要返回错误RACH响应,则UE 102可检测到这种情况(例如,使用数字签名或缺少RACH响应)并确定攻击设备108的存在。例如,gNB 110可在RACH响应消息中以及在具有当前时间的广播消息中进行数字签名,即包括数字签名(DigSig)。因此,为了有效攻击,攻击设备108将必须通过充当中间人来实现RACH规程。如果攻击设备108可成功地执行中间人重放攻击,则由攻击设备108插入传播延迟中的任何误差将必然地小,例如小于100 μ s或小于10 μ s,例如受从UE 102到gNB 110的最大可能范围限制。此外,即使当当前时间误差非常小时,UE 102也可通过将预期传播延迟与所测量的传播延迟进行比较来检测仿冒,这可进一步减小任何可能误差,例如减小到小于1 μ s。该技术在下文进一步详述。

[0100] 图4B类似于图4A,并且图示了用于在其中攻击设备108存在并执行重放攻击的无线网络中广播和获取可靠时间、以及使用RTT规程来检测重放攻击的信令流450。图4B作为非限制性示例提供。例如,将理解,可存在附加信令和过程,并且在gNB 110与UE 102之间发送的消息可包括附加组件。从UE 102和gNB 110的角度来看,图4B中用于确定RTT和传播延迟的规程可以与针对图3B描述的规程相同,不同之处在于在图4B中存在攻击设备108,其将通常影响由UE 102获得的时间和定时测量。图4B中所示的规程的益处在于,其可由处于RRC IDLE或RRC INACTIVE状态并且其中定时提前可能不可用的UE 102使用。

[0101] 如图4B中所例示的,类似于图4A中所示的消息402和403,在当前时间T处或接近当前时间T,gNB 110广播消息452,该消息由攻击设备108接收,并且被复制,并且在重放攻击中在延迟 $\Delta 1$ 之后作为消息453发送到UE 102,以使得UE 102在时间T+ Δ + $\Delta 1$ 处在经复制消息453中接收到当前时间T。消息452(以及因此消息453)包括当前时间T(其一部分可被加密)、以及在gNB 110处的任选的显式或隐式本地NR传输时间t、以及数字签名(DigSig)。消息452(以及因此消息453)可另外包括当前时间T到基站子帧或时隙边界的隐式或显式对齐、当前时间T的不确定性、当前时间T的源、或它们的组合。UE 102可对当前时间T的至少该部分进行解密以获得未加密的当前时间T。

[0102] 类似于图3B中讨论的RTT规程,gNB 110可以在gNB 110处的本地时间t处向UE 102传送消息或信号454(例如,SSB消息或CSI-RS信号)。消息或信号454由攻击设备108接收、被复制并在延迟 $\Delta 1$ 之后作为消息或信号455发送到UE 102。消息或信号454、以及因此消息或信号455可包括或指示由gNB 110进行的传输的本地时间t,并且UE 102可将其内部定时设定为与来自gNB 110的时间t匹配。需注意,攻击设备108不能相比于消息453的传输和消息459的传输中的延迟 $\Delta 1$ (稍后描述)来改变消息或信号455的传输中的延迟 $\Delta 1$ 而不被UE 102检测到,该UE然后可推断攻击设备108的存在或来自gNB 110的传输的至少某种严重误差。如果攻击设备108将改变延迟 $\Delta 1$,则UE 102可检测到在gNB 110处的本地传输时间t(其通常在消息或信号455以及消息453和459中隐式地或显式地传达)相比于UE 102中的本地时间源的对应变化。尽管UE 102中的本地时间源可能不如gNB 110中的本地时间t精确,但是其可足够精确以检测到gNB 110的本地时间t的显著变化(例如,10 μ s或更多),这在攻击设备108将改变延迟 $\Delta 1$ 的情况下从UE 102的角度来看可能发生。

[0103] 响应于消息或信号455,UE 102可以向gNB 110发送消息456,其可以是例如作为RACH请求消息的RRC消息。消息456可由UE 102在针对gNB 110的RACH上传输。UE 102可在消

息456中包括随机变量(RV)(例如,包括8到16比特的随机比特串)。消息456在第一时间被传输,该第一时间可以是UE的本地时间或gNB 110的相关联的本地传输时间。攻击设备108可接收消息456,并且在延迟 $\Delta 2$ 之后向gNB 110发送经复制消息457。因此,gNB 110在本地时间 $t+2\Delta+\Delta 1+\Delta 2$ (这里称为第二时间)接收经复制消息457。应当注意,如果延迟 $\Delta 2$ 等于延迟 $\Delta 1$,则信号453的接收的总传播延迟 $\Delta+\Delta 1$ 可由UE 102基于UE 102与gNB 110之间的往返时间(RTT)来确定,包括由攻击设备108插入的延迟 $2\times\Delta 1$ 。因此,可假定延迟 $\Delta 2$ 不同于 $\Delta 1$ 。需注意,图4B(像图3B)图示了如在UE 102处接收到消息或信号455时发生的第一时间,并且因此,其中第一时间对应于在消息或信号455中包括的或由该消息或信号指示的时间 t 。然而,第一时间也可在消息或信号455抵达UE 102之后不久(例如,1ms至100ms之后)发生,在该情况,第一时间可对应于UE 102已知并超过 t 的针对gNB 110的某个本地传输时间。

[0104] gNB 110获得(例如,测量)经复制消息457的抵达时间(即,测量第二时间),并且向UE 102返回响应消息458(例如,在针对gNB 110的CCCH上传送的RRC消息)。响应消息458包括随机变量(RV)、数字签名(DigSig)和第二时间,该第二时间在图4B中是在gNB 110处接收到经复制消息457的本地时间 $t+2\Delta+\Delta 1+\Delta 2$ 。响应消息458可由gNB 110加密。攻击设备108接收响应消息458,并且例如在延迟 $\Delta 1$ 之后向UE 102发送作为响应消息458的副本的消息459。在响应消息458中包括数字签名(DigSig)验证了gNB 110发起响应消息458。因此,当数字签名验证失败时,攻击设备108不能改变响应消息458,或者UE 102将检测到消息459的变化。此外,攻击设备108不能阻止响应消息458,或者UE 102将因缺少任何响应消息而检测到攻击。相应地,UE 102接收具有随机变量(RV)和第二时间(在图4B中对应于在gNB 110处接收到经复制消息457的本地时间 $t+2\Delta+\Delta 1+\Delta 2$)的经复制响应消息459。UE 102可获得传播延迟 $\Delta+(\Delta 1+\Delta 2)/2$ 。

[0105] 类似于图3B中的信令流350,如果UE 102未接收到经复制响应消息459(例如,在传送消息456之后的某个最大预期响应时间之后),则UE 102可以在稍后的时间 t' 处重传消息456(图4B中未示出)并且等待接收与经复制响应消息459类似的响应消息(图4B中未示出)。例如,如果gNB 110例如因UE 102发送消息456或攻击设备108发送经复制消息457的干扰或低传输功率而没有正确地接收到经复制消息457,则可能发生这种情况。对于消息456的重传并假设gNB 110为此与响应消息458类似地发送响应消息,UE 102可使用时间 t' 而不是时间 t 来获得如上所述的传播延迟 $\Delta+(\Delta 1+\Delta 2)/2$ 。

[0106] 如果攻击设备108将过大的延迟 $\Delta 1$ 和/或 $\Delta 2$ 插入传播延迟中,则UE 102可检测到攻击。例如,无线小区具有有限大小,这限制了可能的传播时间量。在没有中继的情况下,UE 102与gNB 110之间的最大可能范围可以是例如基于大小区大小的30km,其转换成大约100 μ s的传播延迟。当中继存在时(其通常将仅发生在农村地区),最大可能范围可能增加(例如,到100km),在该情形中,UE 102可基于已知环境(例如,城市、郊区或农村)或网络运营商或UE供应商可以在UE 102中为其配置环境的UE 102的近似已知位置来调整对最大可能范围的预期。因此,如果UE 102检测到超过100 μ s的总传播延迟并且不存在中继,则UE 102可以推断出攻击设备很有可能已将附加延迟插入到传播延迟中,并且因此,在消息453处接收到的当前时间 T 不可靠并且应该被丢弃。UE 102还可使用更小或更大阈值来检测攻击,例如在城市或郊区环境中的10 μ s或可能存在中继的农村环境中的1ms。因此,为了避免检测到,攻击设备108不能阻止图4B中所示的规程,它也不能仿冒响应消息458,并且攻击设备108随后

被限制在其可插入到传播延迟中的误差量小于由UE 102用来验证传播延迟的阈值,其在大多数环境中可以是 $10\mu\text{s}$ - $100\mu\text{s}$ 。

[0107] 附加地,如果UE 102例如从先前定位估计知道其自己的位置,并且知道gNB 110的位置,则UE 102可基于这两个位置之间的距离来独立地确定预期传播延迟 Δ 。然后,UE 102可基于传播延迟 Δ 的预期值与传播延迟 Δ 的测量值之间的失配来检测攻击设备108的仿冒(例如,如根据图4B中的规程或使用定时提前获得的)。如果失配大于阈值,例如 $1\mu\text{s}$,则UE 102可确定攻击设备很可能已经将附加延迟插入传播延迟中,并且因此,在消息453处接收到的当前时间T不可靠并应当被丢弃。通过这种附加的基于位置的验证,UE 102可以以较高概率验证攻击设备108的存在或不存在,因为由攻击设备108添加的延迟(对于重放或中间人攻击)通常将是远大于由UE 102用来验证测得的传播延迟的阈值(例如, $1\mu\text{s}$)。

[0108] 当由UE 102使用在UE 102如先前所描述的处于RRC连通状态时由gNB 110提供给UE 102的定时提前值获得传播延迟时,如以上所描述的测得传播延迟与预期传播延迟的比较也可以由UE 102来执行。如果攻击设备正在对UE 102执行中间人攻击,则由gNB 110提供给UE 102的定时提前然后也将包括延迟 $\Delta 1$ 和 $\Delta 2$,因为UE 102与gNB 110之间的所有信令将随后被攻击设备108接收、复制和转发(例如,如图4B所示),并且因此由gNB 110进行的定时提前确定将包括由攻击设备108添加的延迟。然后,UE 102可获得作为定时提前的一半的传播延迟并将其与基于UE 102和gNB 110之间的最大可能距离的期望值或基于UE 102和gNB 110的已知位置的UE 102和gNB 110之间的计算范围进行比较。随后,攻击设备108存在的推断可以与先前针对图4B中的RTT规程描述的推断正好相同。

[0109] 注意,UE 102可以使用UE 102与gNB 110之间的RTT而不是传播延迟(例如,对于图4B中的规程)作为确定攻击设备108存在或不存在的手段。RTT是传播延迟的两倍,并且因此,可由UE 102以与传播延迟类似的方式测量或获得。同样地,RTT的预期范围将是传播延迟的预期范围的两倍。因此,本文关于使用传播延迟来检测攻击设备108的存在的各种陈述也可适用于RTT的使用。

[0110] 图5图示了用于在包括UE 102、gNB 110和LMF 152的无线网络中广播和获取可靠时间、以及检测由攻击设备108进行的重放攻击的信令流500。

[0111] 在阶段1处,UE 102确定UE 102与gNB 110之间的预期范围。预期范围的确定可基于例如UE 102和gNB 110的已知位置。UE 102的位置可由UE 102或由LMF 152(其然后可向UE 102提供该位置)使用UE 102与LMF 152(或SLP 162,图5中未示出)之间的使用已知定位技术(诸如DL-TDOA、DL-AOD、多小区RTT、A-GNSS、WiFi、ECID等)的定位会话来确定。UE 102可从LMF 152(或从SLP 162)、从gNB 110(例如,如果由gNB 110包括在包含当前时间T的消息中或其他广播消息中)或从可从其gNB位置已被大致确定的PLMN的互联网web服务器获得的信息获得gNB 110的位置。在一些具体实施中,UE 102可以由此确定UE 102和gNB 110之间的预期范围。在其他具体实施中,LMF 152可确定预期范围并可向UE 102提供预期范围。

[0112] 在阶段2处,gNB 110例如在SIB消息中广播当前时间T连同对在gNB 110处的本地传输时间t的隐式或显式指示以及数字签名(DigSig),该SIB消息可以由攻击设备108接收和存储。

[0113] 在阶段3处,攻击设备108在延迟 $\Delta 1$ 之后向UE 102发送具有当前时间T连同本地传输时间t的隐式或显式指示以及数字签名(DigSig)的SIB消息的副本。

[0114] 在阶段4处,UE 102获得UE 102与gNB 110之间的总传播延迟,包括由攻击设备插入的延迟(例如, $\Delta + (\Delta 1 + \Delta 2) / 2$)。总传播延迟例如可如图4B所讨论的那样测量(例如,如果UE 102处于RRC IDLE或RRC INACTIVE状态)或可由UE 102根据由gNB 110提供的定时提前确定(例如,如果UE 102处于RRC CONNECTED状态)。

[0115] 在阶段5处,UE 102可基于在阶段1获得的预期范围和在阶段4测得的总传播延迟(例如, $\Delta + (\Delta 1 + \Delta 2) / 2$)来检测攻击设备108的存在。例如,可基于UE 102与gNB 110之间的预期范围来确定预期传播延迟,并且可将预期传播延迟与来自阶段4的测量传播延迟进行比较。大于阈值(例如,100 μ s、10 μ s或1 μ s)的失配可以指示攻击设备的存在以及在阶段2处接收到的当前时间的不可靠性。在另一个示例中,可基于在阶段4中测量的总传播延迟来确定测量范围并将其与UE 102与gNB 110之间的预期范围进行比较。大于阈值距离(例如,30km、3km或300米)的失配可以指示攻击设备的存在以及在阶段2处接收到的当前时间的不可靠性。

[0116] 相应地,UE 102可以在无线网络中接收准确的当前时间并且可以验证当前时间是可靠的。如果发生仿冒,则UE 102可检测到仿冒并因此知道所接收的当前时间不可靠,或者通过仿冒成功插入的误差量可最小(例如,小于100 μ s、10 μ s或1 μ s)并且不显著损害由UE 102获得的当前时间。

[0117] 图6示出了示例被配置成用于支持从无线网络获取当前时间的UE 600(例如,其可以是图1、图3A、图3B、图4A、图4B和图5所示的UE 102)的某些示例性特征的示意框图,例如,如本文中所讨论的。UE 600例如可执行图3A、图3B、图4A、图4B和图5所示的信号流和图8所示的过程流,以及本文公开的算法。UE 600可以例如包括一个或多个处理器602、存储器604、示出为WWAN收发器610和WLAN收发器612的外部接口(诸如至少一个无线收发器(例如,无线网络接口))、SPS接收器615和一个或多个传感器613,它们可以与到非暂态计算机可读介质620和存储器604的一个或多个连接件606(例如,总线、线路、光纤、链路等)操作地耦合。例如,SPS接收器615可接收和处理来自图1所示的SV 190的SPS信号。一个或多个传感器613例如可以是可包括一个或多个加速度计、一个或多个陀螺仪、磁力计等的惯性测量单元(IMU)。UE 600还可包括未示出的附加项,诸如可包括例如显示器、按键板或其他输入设备(诸如显示器上的虚拟按键板)的用户接口,用户可以通过该用户接口与UE交接。在某些示例性具体实施中,UE 600的全部或一部分可采取芯片组等的形式。

[0118] 该至少一个无线收发器可以是用于WWAN通信系统的收发器610和用于WLAN通信系统的收发器612,或者可以是用于WWAN和WLAN两者的组合收发器。WWAN收发器610可包括耦合到一个或多个天线611的发射器610t和接收器610r以用于(例如,在一个或多个上行链路信道和/或一个或多个侧链路信道上)传输和/或(例如,在一个或多个下行链路信道和/或一个或多个侧链路信道上)接收无线信号,并将信号从无线信号转换成有线(例如,电和/或光)信号以及从有线(例如,电和/或光)信号转换成无线信号。WLAN收发器612可包括耦合到一个或多个天线611或耦合到分开的天线的发射器612t和接收器612r以用于(例如,在一个或多个上行链路信道和/或一个或多个侧链路信道上)传输和/或(例如,在一个或多个下行链路信道和/或一个或多个侧链路信道上)接收无线信号,并将信号从无线信号转换成有线(例如,电和/或光)信号以及从有线(例如,电和/或光)信号转换成无线信号。发射器610t和612t可包括可以是分立组件或组合/集成组件的多个发射器,和/或接收器610r和612r可包

括可以是分立组件或组合/集成组件的多个接收器。WWAN收发器610可被配置成根据各种无线电接入技术(RAT)来(例如,与基站和/或一个或多个其他设备)传达信号,这些RAT诸如6G新空口(NR)、GSM(全球移动系统)、UMTS(通用移动通信系统)、AMPS(高级移动电话系统)、CDMA(码分多址)、WCDMA(宽带CDMA)、LTE(长期演进)、LTE直连(LTE-D)、3GPP LTE-V2X(PC5)等。新无线电可以使用毫米波频率和/或6GHz以下频率。WLAN收发器612可被配置成根据各种无线电接入技术(RAT)来(例如,与接入点和/或一个或多个其他设备)传达信号,这些RAT诸如3GPP LTE-V2X(PC5)、IEEE 802.11(包括IEEE 802.11p)、WiFi、WiFi直连(WiFi-D)、Bluetooth[®]、Zigbee等。收发器610和612可例如通过光连接和/或电连接通信地耦合到收发器接口,该收发器接口可至少部分地与收发器610和612集成。

[0119] 在一些实施方案中,UE 600可包括天线611,该天线可在内部或在外。UE天线611可被用于传输和/或接收由无线收发器610和612处理的信号。在一些实施方案中,UE天线611可被耦合到无线收发器610和612。在一些实施方案中,可在UE天线611与无线收发器610和612的连接点处执行对由UE 600接收(传输)的信号的测量。例如,用于所接收(所传输)的RF信号测量的测量参考点可以是接收器610r(发射器610t)的输入(输出)端子以及UE天线611的输出(输入)端子。在具有多个UE天线611或天线阵列的UE 600中,天线连接器可被视为表示多个UE天线的聚集输出(输入)的虚拟点。在一些实施方案中,UE 600可测量接收信号(包括信号强度和TOA测量),并且原始测量可由一个或多个处理器602处理。

[0120] 可使用硬件、固件和软件的组合来实现一个或多个处理器602。例如,一个或多个处理器602可被配置成通过实现非暂态计算机可读介质(诸如介质620和/或存储器604)上的一个或多个指令或程序代码608来执行本文中所讨论的功能。在一些实施方案中,一个或多个处理器602可表示可被配置成执行与UE 600的操作相关的数据信号计算程序或过程的至少一部分的一个或多个电路。

[0121] 介质620和/或存储器604可存储包含可执行代码或软件指令的指令或程序代码608,这些可执行代码或软件指令在由一个或多个处理器602执行时使得一个或多个处理器602作为被编程为执行本文公开的技术的专用计算机来操作。如在UE 600中所例示,介质620和/或存储器604可包括一个或多个组件或模块,该一个或多个组件或模块可由一个或多个处理器602实现以执行本文所述的方法体系。虽然各组件或模块被例示为介质620中能够由一个或多个处理器602执行的软件,但是应当理解,各组件或模块可被存储在存储器604中或者可以是在一个或多个处理器602中或在处理器之外的专用硬件。

[0122] 数个软件模块和数据表可驻留在介质620和/或存储器604中,并且由一个或多个处理器602利用,以便管理本文所述的通信和功能性两者。应当理解,如在UE 600中所示的介质620和/或存储器604的内容的组织仅是示例性的,并且如此,各模块和/或数据结构的功能性可取决于UE 600的具体实施而按不同的方式来组合、分离和/或构造。

[0123] 介质620和/或存储器604可包括当前时间模块622,其在由一个或多个处理器602实现时将该一个或多个处理器602配置成例如经由无线收发器610在由基站广播的消息(诸如SIB消息)中接收当前时间。一个或多个处理器602可被进一步配置成基于所接收的当前时间和所确定的传播延迟来确定校正的当前时间。当前时间的至少一部分可以被加密。当前时间可以是例如UTC时间、GPS时间、GLONASS时间、北斗时间、伽利略时间、GNSS时间。该消息还可包括针对基站的本地传输时间。该一个或多个处理器602可以进一步被配置成在消

息中接收附加信息,诸如以下中的至少一者:当前时间到基站子帧或时隙边界的对齐、当前时间的不确定性、当前时间的源、或它们的组合。一个或多个处理器602可被进一步配置成在消息中接收基站的数字签名。

[0124] 介质620和/或存储器604可包括安全模块624,其在由一个或多个处理器602实现时将该一个或多个处理器602配置成解密来自基站的包括当前时间的至少一部分的消息以获得未加密的当前时间、和/或从基站接收的消息以用于确定UE与基站之间的传播延迟。一个或多个处理器602可被进一步配置成基于从基站发送的消息中包括的针对该基站的数字签名来认证这些消息。一个或多个处理器602例如可被配置成例如在连接到无线网络并认证该无线网络之后例如经由无线收发器610从无线网络接收用于该基站的公共加密密钥,并且该公共加密密钥可用来对消息和数字签名进行解密。

[0125] 介质620和/或存储器604可包括传播延迟模块626,其在由一个或多个处理器602实现时将该一个或多个处理器602配置成确定基站与UE之间的传播延迟。例如,一个或多个处理器602可被配置成经由无线从基站接收定时提前和将该定时提前用作传播延迟,即传播延迟等于该定时提前。在另一示例中,该一个或多个处理器602可以例如从定位会话中获得UE的位置和基站的位置,并且基于UE的位置与基站的位置之间的距离来确定传播延迟。该一个或多个处理器602可以被配置成通过被配置成进行以下操作来获得UE的位置和基站的位置:在SIB中接收来自基站的具有该基站的位置的广播,接收包含基站的位置的LPP辅助数据消息,接收包含UE的位置的MO-LR响应消息,执行定位会话以确定UE的位置,或它们的组合。在另一个示例中,一个或多个处理器602可被配置成测量UE与基站之间的RTT,并且基于该RTT的一半来确定传播延迟。例如,该一个或多个处理器602可以被配置成执行图3B和图4B中所图示的RTT规程。一个或多个处理器602可被配置成经由收发器610从基站接收包括针对该基站的本地传输时间的第一消息,并且可例如基于针对该基站的所接收的本地传输时间和在UE中接收到消息的本地时间来将该UE中的本地定时与该基站的本地传输时间相关联。一个或多个处理器602可被配置成经由收发器610向基站传输包括随机变量的第二消息(诸如RACH请求消息),并且作为响应,经由收发器610从基站接收第三消息(例如,RACH响应消息),该第三消息包括该随机变量以及在该基站处接收到该请求消息的针对该基站的本地传输时间。第三消息可以被加密并且可包括基站的数字签名。一个或多个处理器602可被配置成基于由基站在第一时间和第三消息中提供的时间来确定RTT。

[0126] 介质620和/或存储器604可包括定位会话模块628,其在由一个或多个处理器602实现时将该一个或多个处理器602配置成通过服务基站例如经由无线收发器610来参与同位置服务器的定位会话,包括接收定位能力请求消息、从基站接收定位辅助数据和/或广播位置信息、接收对位置信息的请求、执行从一个或多个基站接收到的PRS信号的定位测量(诸如TDOA、AOD、多RTT、ECID等);以及报告例如用于UE辅助式定位过程的位置信息(诸如定位测量),或确定用于基于UE的定位过程的定位估计。

[0127] 介质620和/或存储器604可包括攻击检测模块630,其在由一个或多个处理器602实现时将该一个或多个处理器602配置成检测无线网络中攻击设备的存在。可基于针对超出预期范围的传播延迟确定的所测量的RTT来检测攻击设备的存在。预期范围例如可以是基于到基站的预期最大距离的RTT值。预期范围例如可基于例如在定位会话中确定的UE的所估计位置与基站的位置之间的所确定的距离来确定。

[0128] 本文中所描述的方法体系取决于应用可通过各种手段来实现。例如,这些方法体系可在硬件、固件、软件或它们的任何组合中实现。对于硬件具体实施,一个或多个处理器602可在一个或多个专用集成电路(ASIC)、数字信号处理器(DSP)、数字信号处理设备(DSPD)、可编程逻辑设备(PLD)、现场可编程门阵列(FPGA)、处理器、控制器、微控制器、微处理器、电子设备、设计成执行本文所述功能的其他电子单元,或它们的组合内实现。

[0129] 对于固件和/或软件具体实施,这些方法体系可使用执行本文中所描述的功能的模块(例如,程序、函数、等等)来实现。有形地体现指令的任何机器可读介质可被用来实现本文中所描述的方法体系。例如,软件代码可被存储在连接到一个或多个处理器602并由该一个或多个处理器执行的非暂态计算机可读介质620或存储器604中。存储器可被实现在该一个或多个处理器内或该一个或多个处理器的外部。如本文中所使用的,术语“存储器”是指任何类型的长期、短期、易失性、非易失性或其他存储器,而并不限于任何特定类型的存储器或存储器数目、或记忆存储在其上的介质的类型。

[0130] 如果以固件和/或软件实现,则功能可作为一个或多个指令或程序代码608存储在非暂态计算机可读介质(诸如介质620和/或存储器604)上。示例包括编码有数据结构的计算机可读介质和编码有计算机程序代码608的计算机可读介质。例如,包括存储在其上的程序代码608的非暂态计算机可读介质可包括用于支持以与所公开的实施方案一致的方式由UE从无线网络获取当前时间的程序代码608。非暂态计算机可读介质620包括物理计算机存储介质。存储介质可以是计算机能够存取的任何可用介质。以示例的方式而不是限制方式,这种非暂态计算机可读介质可包括RAM、ROM、EEPROM、CD-ROM或其他光盘存储器、磁盘存储器或其他磁存储设备,或者能够用于存储具有指令或数据结构形式的期望的程序代码608并能够由计算机存取的任何其他介质。如本文所使用的,磁盘和光盘包括压缩光盘(CD)、激光光盘、光盘、数字多功能光盘(DVD)、软盘和蓝光光盘,其中磁盘通常磁性地复制数据,而光盘则利用激光来光学地复制数据。上述的组合应当也被包括在计算机可读介质的范围内。

[0131] 除了存储在计算机可读介质620上,指令和/或数据还可作为包括在通信装置中的传输介质上的信号来提供。例如,通信装置可包括具有指示指令和数据的信号的无线收发器610。这些指令和数据被配置成使一个或多个处理器实现权利要求中所概述的功能。也就是说,通信装置包括具有指示用于执行所公开的功能的信息的信号的传输介质。

[0132] 存储器604可表示任何数据存储机构。存储器604可包括例如主存储器和/或辅存储器。主存储器可包括例如随机存取存储器、只读存储器等。虽然在该示例中被例示为与一个或多个处理器602分开,但是应当理解,主存储器的全部或部分可设置在一个或多个处理器602内或以其他方式与该一个或多个处理器共处/耦合。辅存储器可包括例如与主存储器相同或相似类型的存储器和/或一个或多个数据存储设备或系统(诸如举例而言磁盘驱动器、光碟驱动器、磁带驱动器、固态存储器驱动器等)。

[0133] 在某些具体实施中,辅存储器可以可操作地容纳或以其他方式可配置成耦合到非暂态计算机可读介质620。如此,在某些示例性具体实施中,本文所呈现的方法和/或装置可以采取可包括存储在其上的计算机可实现程序代码608的计算机可读介质620的全部或部分的形式,该计算机可实现程序代码608在由一个或多个处理器602执行时可以可操作地被实现为能够执行如本文中所描述的示例操作的全部或部分。计算机可读介质620可以是存

储器604的一部分。

[0134] 图7示出了例示基站700 (例如,其可以是gNB、ng-eNB (例如,ng-eNB 114) 或eNB并可以是例如图1、图3A、图3B、图4A、图4B和图5所示的gNB 110) 的某些示例性特征的示意框图。基站700被配置用于支持UE对当前时间的广播和对当前时间的获取,例如,如本文所讨论。基站700可被配置成执行图3A、图3B、图4A、图4B和图5所示的信号流和图9所示的过程流,以及本文公开的算法。基站700可以例如包括一个或多个处理器702、存储器704、可包括收发器710 (例如,无线网络接口) 和通信接口716 (例如,至其他基站和/或核心网的有线或无线网络接口) 的外部接口和SPS接收器715,其可以可操作地用一个或多个连接件706 (例如,总线、线路、光纤、链路等) 耦合到非暂态计算机可读介质720和存储器704。基站700可进一步包括未被示出的附加项,诸如用户可籍以与UE对接的用户接口,该用户接口可包括例如显示器、按键板或其他输入设备 (诸如显示器上的虚拟按键板)。在某些示例性具体实施中,基站700的全部或部分可以采取芯片组等的形式。收发器710可例如包括被实现为能够在一种或多种类型的无线通信网络上传输一个或多个信号的发射器712、以及接收在该一种或多种类型的无线通信网络上传输的一个或多个信号的接收器714。外部接口716可以是能够连接到RAN中的其他基站或网络实体 (诸如位置服务器,例如,图1所示的AMF 154和LMF 152) 的有线或无线接口。SPS接收器715例如可接收并处理来自图1所示的SV 190的SPS信号以获得当前时间,例如UTC时间、GPS时间、GLONASS时间、北斗时间、伽利略时间、以及GNSS时间。

[0135] 在一些实施方案中,基站700可包括天线711,其可以在内部或在外。天线711可用于传输和/或接收由收发器710处理的信号。在一些实施方案中,天线711可耦合到收发器710。在一些实施方案中,可以在天线711和收发器710的连接点处执行对由基站700接收 (传输) 的信号的测量。例如,用于所接收 (所传输) 的RF信号测量的测量参考点可以是接收器714 (发射器712) 的输入 (输出) 端子以及天线711的输出 (输入) 端子。在具有多个天线711或天线阵列的基站700中,天线连接器可被视为表示多个天线的聚集输出 (输入) 的虚拟点。在一些实施方案中,基站700可测量接收信号 (包括信号强度和TOA测量), 并且原始测量可由一个或多个处理器702处理。

[0136] 可使用硬件、固件和软件的组合来实现一个或多个处理器702。例如,一个或多个处理器702可被配置成通过实现非暂态计算机可读介质 (诸如介质720和/或存储器704) 上的一个或多个指令或程序代码708来执行本文中所讨论的功能。在一些实施方案中,一个或多个处理器702可表示可被配置成执行与基站700的操作相关的数据信号计算规程或过程的至少一部分的一个或多个电路。

[0137] 介质720和/或存储器704可存储包含可执行代码或软件指令的指令或程序代码708,这些可执行代码或软件指令在由一个或多个处理器702执行时使得一个或多个处理器702作为被编程为执行本文公开的技术的专用计算机来操作。如在基站700中所例示,介质720和/或存储器704可包括一个或多个组件或模块,这一个或多个组件或模块可由一个或多个处理器702实现以执行本文所述的方法体系。虽然各组件或模块被例示为介质720中能够由一个或多个处理器702执行的软件,但是应当理解,各组件或模块可被存储在存储器704中或者可以是在一个或多个处理器702中或在处理器之外的专用硬件。

[0138] 数个软件模块和数据表可驻留在介质720和/或存储器704中,并且由一个或多个

处理器702利用,以便管理本文所述的通信和功能性两者。应当理解,如基站700中示出的介质720和/或存储器704的内容的组织仅是示例性的,并且如此,各模块和/或数据结构的功能性可取决于基站700的具体实施而按不同的方式来组合、分离和/或构造。

[0139] 介质720和/或存储器704可包括当前时间模块722,其在由一个或多个处理器702实现时将该一个或多个处理器702配置成例如经由SPS接收机715从SV 190或经由外部接口716从网络实体(诸如AMF 154)获得当前时间。当前时间可以是例如UTC时间、GPS时间、GLONASS时间、北斗时间、伽利略时间、GNSS时间。一个或多个处理器702可被进一步配置成例如经由无线收发器710在消息诸如SIB消息中广播当前时间。当前时间的至少一部分可以被加密。所广播的消息还可包括针对基站的本地传输时间。该一个或多个处理器702可以进一步被配置成在消息中广播附加信息,诸如以下中的至少一者:当前时间到子帧或时隙边界的对齐、当前时间的不确定性、当前时间的源、或它们的组合。一个或多个处理器702可被进一步配置成广播具有该基站的数字签名的消息。

[0140] 介质720和/或存储器704可包括安全模块724,其在由一个或多个处理器702实现时将该一个或多个处理器702配置成加密来自基站的包括当前时间的至少一部分的消息、和/或传送至UE的消息以用于确定UE与基站之间的传播延迟。该一个或多个处理器702可以进一步被配置成在给UE的一个或多个消息中包括针对基站的数字签名。一个或多个处理器702可被进一步配置成经由收发器710将用于基站的公共加密密钥发送到UE,其中数字签名是基于与公共加密密钥对应的私有加密密钥。

[0141] 介质720和/或存储器704可包括传播延迟模块726,其在由一个或多个处理器702实现时将该一个或多个处理器702配置成辅助UE确定传播延迟。例如,一个或多个处理器702可被配置成获得定时提前并经由无线向UE发送该定时提前,其中传播延迟等于该定时提前。在另一个示例中,一个或多个处理器702可向UE发送包括UE的位置和基站的位置中的至少一者的消息,其中传播延迟可基于UE的位置与基站的位置之间的距离来确定。该一个或多个处理器702可以被配置成例如在SIB中广播基站的位置,转发包含基站的位置的LPP辅助数据消息,向UE发送包含UE的位置的MO-LR响应消息,在UE和针对该UE执行的位置之间传递LPP消息以确定该UE的位置,或它们的组合。在另一个示例中,一个或多个处理器702可被配置成辅助UE测量UE与基站之间的RTT,其中传播延迟等于RTT的一半。例如,一个或多个处理器702可被配置成执行图3B和图4B例示的RTT规程。该一个或多个处理器702可以被配置成经由收发器710向UE发送具有针对基站的本地传输时间的第一消息。一个或多个处理器702可被配置成经由收发器710从UE接收包括随机变量的第二消息(诸如RACH请求消息),并且作为响应,经由收发器710向UE发送第三消息(例如,RACH响应消息),该第三消息包括该随机变量以及在基站处接收到该请求消息的本地传输时间。第三消息可以被加密并且可包括基站的数字签名。

[0142] 介质720和/或存储器704可包括定位会话模块728,其在由一个或多个处理器702实现时将该一个或多个处理器702配置成例如经由无线收发器710和外部接口716来参与与UE和位置服务器的定位会话。例如,定位会话可包括LPP定位消息的传递、以及PRS信号到UE的传输以用于测量、和/或接收和测量来自UE的上行链路PRS信号并将这些UL测量经由外部接口716转发到位置服务器或经由收发器710转发到UE。

[0143] 本文中所描述的方法体系取决于应用可通过各种手段来实现。例如,这些方法体

系可在硬件、固件、软件或它们的任何组合中实现。对于硬件具体实施,一个或多个处理器702可在一个或多个专用集成电路(ASIC)、数字信号处理器(DSP)、数字信号处理设备(DSPD)、可编程逻辑设备(PLD)、现场可编程门阵列(FPGA)、处理器、控制器、微控制器、微处理器、电子设备、设计成执行本文所述功能的其他电子单元,或它们的组合内实现。

[0144] 对于固件和/或软件具体实施,这些方法体系可使用执行本文中所描述的功能的模块(例如,程序、函数、等等)来实现。有形地体现指令的任何机器可读介质可被用来实现本文中所描述的方法体系。例如,软件代码可被存储在连接到一个或多个处理器702并由该一个或多个处理器执行的非暂态计算机可读介质720或存储器704中。存储器可被实现在该一个或多个处理器内或该一个或多个处理器的外部。如本文中所使用的,术语“存储器”是指任何类型的长期、短期、易失性、非易失性或其他存储器,而并不限于任何特定类型的存储器或存储器数目、或记忆存储在其上的介质的类型。

[0145] 如果以固件和/或软件实现,则功能可作为一个或多个指令或程序代码708存储在非暂态计算机可读介质(诸如介质720和/或存储器704)上。示例包括编码有数据结构的计算机可读介质和编码有计算机程序代码708的计算机可读介质。例如,包括存储在其上的程序代码708的非暂态计算机可读介质可包括以与所公开的实施方案一致的方式来支持当前时间的广播和UE对当前时间的获取的程序代码708。非暂态计算机可读介质720包括物理计算机存储介质。存储介质可以是计算机能够存取的任何可用介质。以示例方式而不是限制方式,这种非暂态计算机可读介质可包括RAM、ROM、EEPROM、CD-ROM或其他光盘存储器、磁盘存储器或其他磁存储设备,或者能够用于存储具有指令或数据结构形式的期望的程序代码708并能够由计算机存取的任何其他介质。如本文所使用的,磁盘和光盘包括压缩光盘(CD)、激光光盘、光盘、数字多功能光盘(DVD)、软盘和蓝光光盘,其中磁盘通常磁性地复制数据,而光盘则利用激光来光学地复制数据。上述的组合应当也被包括在计算机可读介质的范围内。

[0146] 除了存储在计算机可读介质720上,指令和/或数据还可作为包括在通信装置中的传输介质上的信号来提供。例如,通信装置可包括具有指示指令和数据的信号的收发器710。这些指令和数据被配置成使一个或多个处理器实现权利要求中所概述的功能。也就是说,通信装置包括具有指示用于执行所公开的功能的信息的信号的传输介质。

[0147] 存储器704可表示任何数据存储机构。存储器704可包括例如主存储器和/或辅存储器。主存储器可包括例如随机存取存储器、只读存储器等。虽然在该示例中被例示为与一个或多个处理器702分开,但是应当理解,主存储器的全部或部分可设置在一个或多个处理器702内或以其他方式与该一个或多个处理器共处/耦合。辅存储器可包括例如与主存储器相同或相似类型的存储器和/或一个或多个数据存储设备或系统(诸如举例而言磁盘驱动器、光碟驱动器、磁带驱动器、固态存储器驱动器等)。

[0148] 在某些具体实施中,辅存储器可以可操作地容纳或以其他方式可配置成耦合到非暂态计算机可读介质720。如此,在某些示例性具体实施中,本文所呈现的方法和/或装置可采取可包括存储在其上的计算机可实现程序代码708的计算机可读介质720的全部或部分的形式,该计算机可实现程序代码在由一个或多个处理器702执行时可以可操作地被实现为能够执行如本文所述的示例操作的全部或部分。计算机可读介质720可以是存储器704的一部分。

[0149] 图8示出了以与所公开的具体实施一致的方式由用户装备 (UE) (诸如图1、图3A、图3B、图4A、图4B、图5和图6所示的UE 102) 执行的用于支持由UE在无线网络中获取可靠时间的示例性方法800的流程图。

[0150] 在框802处,UE接收从基站(例如,gNB 110或ng-eNB 114)广播的消息,该消息包括当前时间,其中该当前时间的至少一部分被加密,例如,如图3A中的消息302、图3B中的消息352、图4A中的消息402和403、以及图4B中的消息452和453中所图示的。当前时间例如可包括协调世界时 (UTC) 时间、全球定位系统 (GPS) 时间、GLONASS时间、北斗时间、伽利略时间、全球导航卫星系统 (GNSS) 时间、或本地区域时间。该消息可以进一步包括以下中的至少一者:当前时间到基站子帧或时隙边界的隐式或显式对齐、当前时间的不确定性、当前时间的源、或它们的组合,例如,如针对图2E所描述的。用于接收从基站广播的消息的部件可包括例如无线收发器610和具有专用硬件或实现图6所示的UE 600中的存储器604和/或介质620中的可执行代码或软件指令(诸如当前时间模块622)的一个或多个处理器602,该消息包括当前时间,其中该当前时间的至少一部分被加密。

[0151] 在框804处,UE通过该当前时间的至少该部分进行解密来获得未加密的当前时间,例如,如图2B-2E、3A、3B、4A和4B中所讨论的。用于通过对当前时间的至少该部分进行解密来获得未加密的当前时间的部件可包括例如具有专用硬件或实现图6所示的UE 600中的存储器604和/或介质620中可执行代码或软件指令(诸如安全模块624)的一个或多个处理器602。

[0152] 在框806处,UE确定该基站与该UE之间的传播延迟,例如,如图3A、3B、4A和4B中所讨论的。用于确定基站与UE之间的传播延迟的部件可包括例如无线收发器610和具有专用硬件或实现图6所示的UE 600中的存储器604和/或介质620中的可执行代码或软件指令(诸如传播延迟模块626)的一个或多个处理器602。

[0153] 在框808处,UE基于未加密的当前时间和该传播延迟来确定校正的当前时间,例如,如图3A、3B、4A和4B中所讨论的。用于基于未加密的当前时间和传播延迟来确定校正的当前时间的部件可包括例如具有专用硬件或实现图6所示的UE 600中的存储器604和/或介质620中的可执行代码或软件指令(诸如安全模块624)的一个或多个处理器602。

[0154] 在一个具体实施中,UE可以通过从基站获得定时提前来确定传播延迟,其中该传播延迟是根据定时提前来确定的(例如,确定为定时提前值的一半),例如,如在图3A和3B中所讨论的。用于从基站获得定时提前的部件可包括例如无线收发器610和具有专用硬件或实现图6所示的UE 600中的存储器604和/或介质620中的可执行代码或软件指令(诸如传播延迟模块626)的一个或多个处理器602,其中传播延迟是根据定时提前来确定的。

[0155] 在一个具体实施中,UE可以通过获得UE的位置和基站的位置来确定传播延迟,其中该传播延迟是基于UE的位置与基站的位置之间的距离来确定的,例如,如在图3A、3B、4A和4B中所讨论的。用于获得UE的位置和基站的位置的部件可包括例如无线收发器610和具有专用硬件或实现图6中所示的UE 600中的存储器604和/或介质620中的可执行代码或软件指令(诸如传播延迟模块626)的一个或多个处理器602,其中该传播延迟是基于UE的位置与基站的位置之间的距离来确定的。如关于图3A所讨论,UE可通过以下中的至少一者来获得UE的位置和基站的位置:在系统信息块 (SIB) 中接收来自该基站的对该基站的该位置的广播;接收包含所述基站的位置的长期演进 (LTE) 定位协议 (LPP) 辅助数据消息;接收包含

该UE的该位置的移动发起位置请求(MO-LR)响应消息;或者执行定位会话以确定该UE的该位置。用于在系统信息块(SIB)中接收来自基站的对基站的位置的广播的部件可包括例如无线收发器610和具有专用硬件或实现图6所示的UE 600中的存储器604和/或介质620中的可执行代码或软件指令(诸如传播延迟模块628)的一个或多个处理器602。用于接收包含基站的位置的长期演进(LTE)定位协议(LPP)辅助数据消息的部件可包括例如无线收发器610和具有专用硬件或实现图6所示的UE 600中的存储器604和/或介质620中的可执行代码或软件指令(诸如定位会话模块628)的一个或多个处理器602。用于接收包含UE的位置的移动发起位置请求(MO-LR)响应消息的部件可包括例如无线收发器610和具有专用硬件或实现图6所示的UE 600中的存储器604和/或介质620中的可执行代码或软件指令(诸如定位会话模块628)的一个或多个处理器602。用于执行定位会话以确定UE的位置的装置可包括例如无线收发器610和具有专用硬件或实现图6所示的UE 600中的存储器604和/或介质620中的可执行代码或软件指令(诸如定位会话模块628)的一个或多个处理器602。

[0156] 在一个具体实施中,UE可以通过测量该UE与基站之间的往返传播时间(RTT)来确定传播延迟,其中该传播延迟等于该RTT的一半,例如,如在图3A、3B、4A和4B中所讨论的。用于测量UE与基站之间的往返传播时间(RTT)的部件可包括例如无线收发器610和具有专用硬件或实现图6所示的UE 600中的存储器604和/或介质620中的可执行代码或软件指令(诸如传播延迟模块626)的一个或多个处理器602,其中传播延迟等于RTT的一半。

[0157] 在一个具体实施中,UE可以通过从基站接收指示针对该基站的第一本地传输时间的第一消息来测量RTT,例如,如由图3B中的消息354和图4B中的消息455所图示的。用于从基站接收指示针对基站的第一本地传输时间的第一消息的部件可包括例如无线收发器610和具有专用硬件或实现图6所示的UE 600中的存储器604和/或介质620中的可执行代码或软件指令(诸如传播延迟模块626)的一个或多个处理器602。UE可基于针对基站的第一本地传输时间和在UE中接收到第一消息的本地时间来将UE中的本地定时与针对基站的本地传输时间相关联,例如,如图3B和图4B所讨论。用于基于针对基站的第一本地传输时间和在UE中接收到第一消息的本地时间来将UE中的本地定时与针对基站的本地传输时间相关联的部件可包括例如无线收发器610和具有专用硬件或实现图6中所示的UE 600中的存储器604和/或介质620中的可执行代码或软件指令(诸如传播延迟模块626)的一个或多个处理器602。UE可以在随机接入信道(RACH)上向基站传送第二消息,该第二消息包括随机变量,该第二消息在第一时间处被传送,其中该第一时间是UE中的本地时间或针对基站的相关联本地传输时间,例如,如由图3B中的消息356和图4B中的消息456所图示的。用于在随机接入信道(RACH)上向基站传送第二消息的部件可包括例如无线收发器610和具有专用硬件或实现图6中所示的UE 600中的存储器604和/或介质620中的可执行代码或软件指令(诸如传播延迟模块626)的一个或多个处理器602,该第二消息包括随机变量,该第二消息在第一时间被传送,其中该第一时间是UE中的本地时间或针对基站的相关联本地传输时间。UE可响应于第二消息而从基站接收第三消息,第三消息包括第二时间和随机变量,其中第二时间是在基站处接收到第二消息的针对基站的本地传输时间,例如,如图3B中的消息358和图4B中的消息459所例示。用于响应于第二消息而从基站接收第三消息的部件可包括例如无线收发器610和具有专用硬件或实现图6所示的UE 600中的存储器604和/或介质620中的可执行代码或软件指令(诸如传播延迟模块626)的一个或多个处理器602,第三消息包括第二时间和

随机变量,其中第二时间是在基站处接收到第二消息的针对基站的本地传输时间。UE可基于第一时间和第二时间来确定RTT,例如,如图3B和图4B所讨论。用于基于第一时间和第二时间来确定RTT的部件可包括例如无线收发器610和具有专用硬件或实现图6所示的UE 600中的存储器604和/或介质620中的可执行代码或软件指令(诸如传播延迟模块626)的一个或多个处理器602。

[0158] 在一些具体实施中,第三消息可以被加密,例如,如在图3B和图4B中所讨论的。第三消息还可包括针对基站的数字签名,并且UE可基于针对基站的数字签名来认证第三消息,例如,如图3B和图4B所讨论。用于基于针对基站的数字签名来认证第三消息的部件可包括例如具有专用硬件或实现图6所示的UE 600中的存储器604和/或介质620中的可执行代码或软件指令(诸如安全模块624)的一个或多个处理器602。

[0159] 在无线网络中在UE与基站之间可存在攻击设备,其中该消息是在重放攻击中经由攻击设备接收的,例如,如图4A、图4B和图5中所图示的。UE可根据定时提前或通过测量RTT来确定传播延迟(如先前所述)并可基于传播延迟超出预期范围来检测攻击设备的存在,例如,如图4B和图5所讨论。用于根据定时提前或通过测量RTT来确定传播延迟的部件可包括例如具有专用硬件或实现图6所示的UE 600中的存储器604和/或介质620中的可执行代码或软件指令(诸如传播延迟模块626)的一个或多个处理器602。用于基于传播延迟超出预期范围来检测攻击设备的存在的部件可包括例如具有专用硬件或实现图6所示的UE 600中的存储器604和/或介质620中的可执行代码或软件指令(诸如攻击检测模块630)的一个或多个处理器602。预期范围例如可包括基于到基站的预期最大传播延迟。UE可获得UE的所估计位置和基站的位置,例如,如在图5的阶段1中所讨论。UE可确定UE的所估计位置与基站的位置之间的距离估计,例如,如在图5的阶段1中所讨论。UE可基于距离估计来确定预期范围,例如,如在图5的阶段1中所讨论。用于获得UE的所估计位置和基站的位置的部件可包括例如无线收发器610和具有专用硬件或实现图6所示的UE 600中的存储器604和/或介质620中的可执行代码或软件指令(诸如定位会话模块628)的一个或多个处理器602。用于确定UE的所估计位置与基站的位置之间的距离估计的部件可包括例如无线收发器610和具有专用硬件或实现图6所示的UE 600中的存储器604和/或介质620中的可执行代码或软件指令(诸如传播延迟模块626)的一个或多个处理器602。用于基于距离估计来确定预期范围的部件可包括例如无线收发器610和具有专用硬件或实现图6所示的UE 600中的存储器604和/或介质620中的可执行代码或软件指令(诸如传播延迟模块626)的一个或多个处理器602。

[0160] 在一个具体实施中,该消息进一步包括针对基站的数字签名,例如,如图3A中的消息302、图3B中的消息352、图4A中的消息402和图4B中的消息452和453中所图示的。UE可基于针对基站的数字签名来认证消息中的当前时间,例如,如图3B所讨论。用于基于针对基站的数字签名来认证消息中的当前时间的部件可包括例如具有专用硬件或实现图6所示的UE 600中的存储器604和/或介质620中的可执行代码或软件指令(诸如安全模块624)的一个或多个处理器602。UE例如可从无线网络接收针对基站的公共加密密钥,其中数字签名基于与公共加密密钥对应的私有加密密钥,其中认证当前时间使用公共加密密钥,例如,如图3A、图3B、图4A、图4B所讨论。用于从无线网络接收针对基站的公共加密密钥的部件可包括例如具有专用硬件或实现图6所示的UE 600中的存储器604和/或介质620中的可执行代码或软

件指令(诸如安全模块624)的一个或多个处理器602,其中数字签名基于与公共加密密钥对应的私有加密密钥,其中认证当前时间使用公共加密密钥。

[0161] 图9示出了以与所公开的具体实施一致的方式由基站(诸如图1、图3A、图3B、图4A、图4B、图5和图7所示的gNB 110)执行的用于支持由用户装备(UE)在无线网络中获取可靠时间的示例性方法900的流程图。

[0162] 在框902处,基站可以获得当前时间,例如,如结合图1和图3A所讨论的。当前时间例如可包括协调世界时(UTC)时间、全球定位系统(GPS)时间、GLONASS时间、北斗时间、伽利略时间、全球导航卫星系统(GNSS)时间、或本地区域时间。用于获得当前时间的部件可包括例如SPS接收器715或外部收发器716和具有专用硬件或实现图7所示的基站700中的存储器704和/或介质720中的可执行代码或软件指令(诸如当前时间模块722)的一个或多个处理器702。

[0163] 在框904处,基站加密该当前时间的至少一部分,例如,如针对图3A中的消息302和图3B中的消息352所讨论的。用于对当前时间的至少一部分进行加密的部件可包括例如具有专用硬件或实现图7所示的基站700中的存储器704和/或介质720中可执行代码或软件指令(诸如安全模块724)的一个或多个处理器702。

[0164] 在框906处,基站广播包括该当前时间的消息,其中该UE接收该消息,通过该当前时间的至少该部分进行解密来获得未加密的当前时间,并且确定该基站与该UE之间的传播延迟,其中该UE基于未加密的当前时间和该传播延迟来确定校正的当前时间,例如,如针对图3A中的消息302、图3B中的消息352、图4A中的消息402和图4B中的消息452所讨论的。在一些具体实施中,基站可以在该消息中包括以下中的至少一者:当前时间到针对基站的子帧或时隙边界的隐式或显式对齐、当前时间的不确定性、从其获得当前时间的源、或它们的组合。用于广播包括该当前时间的消息的部件以及用于在该消息中包括以下中的至少一者:当前时间到针对基站的子帧或时隙边界的对齐、当前时间的不确定性、从其获得当前时间的源、或其组合的部件可包括例如收发器710和具有专用硬件或实现图7中所示的基站700中的存储器704和/或介质720中的可执行代码或软件指令(诸如当前时间模块722)的一个或多个处理器702。

[0165] 在一个具体实施中,基站可以通过向UE发送定时提前来辅助UE确定传播延迟,其中该定时提前实现由UE确定传播延迟(例如,其中该传播延迟被获得为定时提前的一半),例如,如在图3A和图4A中讨论的。用于向UE发送定时提前的部件可包括例如收发器710以及具有专用硬件或实现图7中所示的基站700中的存储器704和/或介质720中的可执行代码或软件指令(诸如传播延迟模块726)的一个或多个处理器702,其中该定时提前实现由UE确定传播延迟。

[0166] 在一个具体实施中,基站可以通过向UE发送消息来辅助UE确定传播延迟,该消息包括UE的位置和基站的位置中的至少一者,其中该传播延迟由UE基于UE的位置与基站的位置之间的距离来确定,例如,如针对图3A所讨论的。用于向UE发送包括UE的位置和基站的位置中的至少一者的消息的部件可包括例如收发器710和具有专用硬件或实现图7所示的基站700中的存储器704和/或介质720中的可执行代码或软件指令(诸如传播延迟模块726)的一个或多个处理器702,其中传播延迟由UE基于UE的位置与基站的位置之间的距离来确定。如关于图3A所述,基站例如可通过在系统信息块(SIB)中广播基站的位置来向UE发送包括

UE的位置和基站的位置中的至少一者的消息;向UE转发包含基站的位置的长期演进 (LTE) 定位协议 (LPP) 辅助数据消息;向该UE发送包含该UE的该位置的移动发起位置请求 (MO-LR) 响应消息;或者在该UE与针对该UE的位置服务器 (例如, LMF 152或SLP 162) 之间传递LPP消息以确定该UE的该位置、或它们的组合。用于在系统信息块 (SIB) 中广播基站的位置的部件可包括例如收发器710和具有专用硬件或实现图7所示的基站700中的存储器704和/或介质720中的可执行代码或软件指令 (诸如传播延迟模块728) 的一个或多个处理器702。用于向UE转发包含基站的位置的长期演进 (LTE) 定位协议 (LPP) 辅助数据消息的部件可包括例如收发器710和具有专用硬件或实现图7所示的基站700中的存储器704和/或介质720中的可执行代码或软件指令 (诸如定位会话模块728) 的一个或多个处理器702。用于向UE发送包含UE的位置的移动发起位置请求 (MO-LR) 响应消息的部件可包括例如收发器710和具有专用硬件或实现图7所示的基站700中的存储器704和/或介质720中的可执行代码或软件指令 (诸如定位会话模块728) 的一个或多个处理器702。用于在UE与针对该UE的位置服务器之间传递LPP消息以确定UE的位置的部件可包括例如收发器710和具有专用硬件或实现图7中所示的基站700中的存储器704和/或介质720中的可执行代码或软件指令 (诸如定位会话模块728) 的一个或多个处理器702。

[0167] 在一个具体实施中, 基站可以通过辅助UE测量该UE与基站之间的往返传播时间 (RTT) 来辅助UE确定传播延迟, 其中该传播延迟等于该RTT的一半, 例如, 如在图3B和图4B中所讨论的。用于辅助UE测量UE与基站之间的往返传播时间 (RTT) 的部件可包括例如收发器710和具有专用硬件或实现图7所示的基站700中的存储器704和/或介质720中的可执行代码或软件指令 (诸如传播延迟模块726) 的一个或多个处理器702, 其中传播延迟等于RTT的一半。

[0168] 在一个具体实施中, 基站可以通过向UE发送指示针对该基站的第一本地传输时间的第一消息来辅助UE测量RTT, 其中UE基于针对基站的第一本地传输时间和在UE中接收到第一消息的本地时间来将该UE中的本地定时与针对该基站的本地传输时间相关联, 例如, 如由图3B中的消息354和图4B中的消息454所图示的。用于向UE发送指示针对基站的第一本地传输时间的第一消息的部件可包括例如收发器710和具有专用硬件或实现图7所示的基站700中的存储器704和/或介质720中的可执行代码或软件指令 (诸如传播延迟模块726) 的一个或多个处理器702, 其中UE基于针对基站的第一本地传输时间和在UE中接收到第一消息的本地时间来将该UE中的本地定时与针对基站的本地传输时间相关联。基站可在随机接入信道 (RACH) 上从UE接收第二消息, 第二消息包括随机变量, 第二消息在第一时间被传输, 其中第一时间是UE中的本地时间或针对基站的相关联本地传输时间, 例如, 如图3B中的消息356和图4B中的消息457所例示。用于在随机接入信道 (RACH) 上从UE接收第二消息的部件可包括例如收发器710和具有专用硬件或实现图7所示的基站700中的存储器704和/或介质720中的可执行代码或软件指令 (诸如传播延迟模块726) 的一个或多个处理器702, 第二消息包括随机变量, 第二消息在第一时间被传输, 其中第一时间是UE中的本地时间或针对基站的相关联本地传输时间。基站可测量第二时间, 其中第二时间是在基站处接收到第二消息的针对基站的本地传输时间, 例如, 如图3B中的消息356和图4B中的消息457所例示。用于测量第二时间的部件可包括例如收发器710和具有专用硬件或实现图7所示的基站700中的存储器704和/或介质720中的可执行代码或软件指令 (诸如传播延迟模块726) 的一个或多

个处理器702,其中第二时间是在基站处接收到第二消息的针对基站的本地传输时间。基站可响应于第二消息而向UE发送第三消息,第三消息包括第二时间和随机变量,其中UE基于第一时间和第二时间来确定RTT,例如,如图3B中的消息358以及图4B中的消息458和459所例示。用于响应于第二消息而向UE发送第三消息的部件可包括例如收发器710和具有专用硬件或实现图7所示的基站700中的存储器704和/或介质720中的可执行代码或软件指令(诸如传播延迟模块726)的一个或多个处理器702,第三消息包括第二时间和随机变量。

[0169] 在一些具体实施中,基站可以加密第三消息,例如,如在图3B和图4B中所讨论的。用于对第三消息进行加密的部件可包括例如收发器710和具有专用硬件或实现图7所示的基站700中的存储器704和/或介质720中可执行代码或软件指令(诸如安全模块724)的一个或多个处理器702。基站可在第三消息中包括针对该基站的数字签名,其中UE基于针对基站的数字签名来认证第三消息,例如,如图3B和图4B所讨论。用于在第三消息中包括针对基站的数字签名的部件可包括例如收发器710和具有专用硬件或实现图7所示的基站700中的存储器704和/或介质720中的可执行代码或软件指令(诸如安全模块724)的一个或多个处理器702,其中UE基于针对基站的数字签名来认证第三消息。

[0170] 在一些具体实施中,在无线网络中在UE与基站之间可存在攻击设备,其中该消息是在重放攻击中经由攻击设备接收的,例如,如图4A和图4B中所图示的。UE可根据定时提前或通过测量RTT来确定传播延迟(如上文所述)并可基于传播延迟超出预期范围来检测攻击设备的存在,例如,如图4B和图5所例示。预期范围例如可以是基于UE与基站之间的最大预期距离的最大传播延迟。预期范围例如可基于UE的所估计位置和由UE获得的基站的位置。

[0171] 在一个具体实施中,基站可在该消息中包括针对该基站的数字签名,其中UE基于该基站的数字签名来认证该消息中的当前时间,例如,如图3A中的消息302、图3B中的消息352、图4A中的消息402、以及图4B中的消息452和453中所例示。用于在消息中包括针对基站的数字签名的部件可包括例如收发器710和具有专用硬件或实现图7所示的基站700中的存储器704和/或介质720中的可执行代码或软件指令(诸如当前时间模块722)的一个或多个处理器702,其中UE基于针对基站的数字签名来认证消息中的当前时间。基站可向UE发送针对基站的公共加密密钥,其中数字签名基于与公共加密密钥对应的私有加密密钥,其中UE使用公共加密密钥来认证当前时间,例如,如图3A和图3B所讨论。用于向UE发送针对基站的公共加密密钥的部件可包括例如收发器710和具有专用硬件或实现图7所示的基站700中的存储器704和/或介质720中的可执行代码或软件指令(诸如安全模块724)的一个或多个处理器702,其中数字签名基于与公共加密密钥对应的私有加密密钥,其中UE使用公共加密密钥来认证当前时间。

[0172] 贯穿本说明书引述的“一个示例”、“一示例”、“某些示例”或“示例性具体实施”意指结合特征和/或示例所描述的特定特征、结构或特性可被包括在所要求保护的主体内容的至少一个特征和/或示例中。由此,在说明书中各处出现的短语在“一个示例中”、“一示例”、“在某些示例中”或“在某些具体实施中”或其他类似短语并不一定都指相同的特征、示例和/或限定。此外,这些特定特征、结构或特性可在一个或多个示例和/或特征中加以组合。

[0173] 本文所包括的详细描述的一些部分是以对存储在特定装置或专用计算设备或平台的存储器内的二元数字信号的操作的算法或符号表示的形式来呈现的。在该特定说明书

的上下文中,术语特定装置等包括一旦被编程就根据来自程序软件的指令执行特定操作的通用计算机。算法描述或符号表示是在信号处理或相关领域的普通技术人员用来将他们的工作的实质传达给本领域其他技术人员的技术的示例。这里的算法一般被认为是导致期望结果的操作或类似信号处理的自相容序列。在该上下文中,操作或处理涉及物理量的物理操纵。典型地但不是必须地,此类量可以采取能够被存储、传递、组合、比较或以其他方式被操纵的电或磁信号的形式。主要出于普遍使用的原因,将此类信号称为比特、数据、值、元素、码元、字符、项、数字、数值等已证明有时是方便的。然而,应该理解,所有这些或类似的术语都应与适当的物理量相关联,并且仅仅是方便的标签。除非另外特别声明,否则如从本文中的讨论显而易见的,应领会,贯穿本说明书,利用诸如“处理”、“计算”、“演算”、“确定”等术语的讨论是指特定装置(诸如专用计算机、专用计算装置或类似的专用电子计算设备)的动作或过程。在本说明书的上下文中,因此,专用计算机或类似的专用电子计算设备能够操纵或变换通常表示为该专用计算机或类似的专用电子计算设备的存储器、寄存器、或其他信息存储设备、传输设备、或显示设备内的物理电子或磁性量的信号。

[0174] 在以上详细描述中,阐述了众多具体细节以提供对所要求保护的主体内容的透彻理解。然而,本领域技术人员将理解,没有这些具体细节也可实践所要求保护的主体内容。在其他实例中,本领域普通技术人员已知的方法和装置未详细描述以免混淆所要求保护的主体内容。

[0175] 如本文所使用的术语“和”、“或”以及“和/或”可包括还预期至少部分地取决于使用此类术语的上下文的各种含义。通常,“或”若被用于关联一列表,诸如A、B或C,则旨在表示A、B和C(这里使用的是包含性的含义)以及A、B或C(这里使用的是排他性的含义)。另外,本文所使用的术语“一个或多个”可用于描述单数形式的任何特征、结构或特性,或者可用于描述多个特征、结构或特征或其某种其他组合。但是,应注意,这仅是说明性示例,并且所要求保护的主体内容不限于此示例。

[0176] 虽然已经图示并描述了目前被认为是示例特征的内容,但是本领域技术人员将理解,在不脱离所要求保护的主体内容的情况下,可以进行各种其他修改,并且可以替换等同物。附加地,可以作出许多修改以使特定场景适应于要求保护的主体内容的教导,而不脱离本文所描述的中心概念。

[0177] 鉴于此说明书,各实施方案可包括特征的不同组合。在以下经编号条款中描述了具体实施示例:

[0178] 条款1.一种由用户装备(UE)执行的用于支持在无线网络中获取时间的方法,包括:接收从基站广播的消息,该消息包括当前时间,其中该当前时间的至少一部分被加密;通过对当前时间的至少部分进行解密来获得未加密的当前时间;确定该基站与该UE之间的传播延迟;以及基于该未加密的当前时间和该传播延迟来确定校正的当前时间。

[0179] 条款2.根据条款1所述的方法,其中该当前时间包括协调世界时(UTC)时间、全球定位系统(GPS)时间、GLONASS时间、北斗时间、伽利略时间、全球导航卫星系统(GNSS)时间、或本地区域时间。

[0180] 条款3.根据条款1或2中任一项所述的方法,其中确定该传播延迟包括以下中的一者:从该基站获得定时提前,其中该传播延迟是根据该定时提前来确定的;获得该UE的位置和该基站的位置,其中该传播延迟是基于该UE的该位置与该基站的该位置之间的距离来确

定的;或者测量该UE与该基站之间的往返传播时间(RTT),其中该传播延迟等于该RTT的一半。

[0181] 条款4.根据条款3所述的方法,其中获得该UE的该位置和该基站的该位置包括以下中的至少一者:在系统信息块(SIB)中接收来自该基站的对该基站的该位置的广播;接收包含基站的位置的长期演进(LTE)定位协议(LPP)辅助数据消息;接收包含该UE的该位置的移动发起位置请求(MO-LR)响应消息;或者执行定位会话以确定该UE的该位置。

[0182] 条款5.根据条款3或4中任一项所述的方法,其中测量该RTT包括:从该基站接收指示针对该基站的第一本地传输时间的第一消息;基于针对基站的第一本地传输时间和在UE中接收到第一消息的本地时间来将UE中的本地定时与针对基站的本地传输时间相关联;在随机接入信道(RACH)上向基站传送第二消息,该第二消息包括随机变量,该第二消息在第一时间被传送,其中该第一时间是该UE中的本地时间或针对该基站的相关联本地传输时间;响应于该第二消息而从该基站接收第三消息,该第三消息包括第二时间和该随机变量,其中该第二时间是在该基站处接收到该第二消息的针对该基站的本地传输时间;以及基于该第一时间和该第二时间来确定该RTT。

[0183] 条款6.根据条款5所述的方法,其中该第三消息被加密。

[0184] 条款7.根据条款5或6中任一项所述的方法,其中该第三消息进一步包括针对该基站的数字签名,该方法进一步包括:基于针对该基站的该数字签名来认证该第三消息。

[0185] 条款8.根据条款3-7中任一项所述的方法,其中在该无线网络中在该UE与该基站之间存在攻击设备,其中该消息是在重放攻击中经由该攻击设备接收的,该方法进一步包括:根据该定时提前或通过测量该RTT来确定该传播延迟;以及基于该传播延迟超出预期范围来检测该攻击设备的存在。

[0186] 条款9.根据条款8所述的方法,其中该预期范围包括基于到该基站的预期距离的最大传播延迟。

[0187] 条款10.根据条款8或9中任一项所述的方法,进一步包括:获得该UE的所估计位置 and 该基站的该位置;确定该UE的所估计位置与该基站的该位置之间的距离估计;以及基于该距离估计来确定该预期范围。

[0188] 条款11.根据条款1-10中任一项所述的方法,其中该消息进一步包括以下中的至少一者:当前时间到基站子帧或时隙边界的隐式或显式对齐、当前时间的不确定性、当前时间的源、它们的组合。

[0189] 条款12.根据条款1-11中任一项所述的方法,其中该消息进一步包括针对该基站的数字签名,该方法进一步包括:基于针对该基站的该数字签名来认证该消息中的该当前时间。

[0190] 条款13.根据条款12所述的方法,进一步包括:从该无线网络接收针对该基站的公共加密密钥,其中该数字签名基于与该公共加密密钥对应的私有加密密钥,其中认证该当前时间使用该公共加密密钥。

[0191] 条款14.一种被配置用于支持在无线网络中获取时间的用户装备(UE),包括:无线收发器,该无线收发器被配置成与该无线网络中的基站进行无线通信;至少一个存储器;耦合到该无线收发器和该至少一个存储器的至少一个处理器,其中该至少一个处理器被配置成:经由该无线收发器接收从基站广播的消息,该消息包括当前时间,其中该当前时间的至

少一部分被加密;通过对当前时间的至少部分进行解密来获得未加密的当前时间;确定该基站与该UE之间的传播延迟;以及基于该未加密的当前时间和该传播延迟来确定校正的当前时间。

[0192] 条款15.根据条款14所述的UE,其中该当前时间包括协调世界时(UTC)时间、全球定位系统(GPS)时间、GLONASS时间、北斗时间、伽利略时间、全球导航卫星系统(GNSS)时间、或本地区域时间。

[0193] 条款16.根据条款14或15中任一项所述的UE,其中该至少一个处理器被配置成通过以下中的一者来确定该传播延迟:经由该无线收发器从该基站获得定时提前,其中该传播延迟是根据该定时提前来确定的;获得该UE的位置和该基站的位置,其中该传播延迟是基于该UE的该位置与该基站的该位置之间的距离来确定的;或者测量该UE与该基站之间的往返传播时间(RTT),其中该传播延迟等于该RTT的一半。

[0194] 条款17.根据条款16所述的UE,其中该至少一个处理器被配置成通过以下中的至少一者来获得该UE的该位置 and 该基站的该位置:经由该无线收发器在系统信息块(SIB)中接收来自该基站的对该基站的该位置的广播;经由所述无线收发器接收包含基站的位置的长期演进(LTE)定位协议(LPP)辅助数据消息;经由该无线收发器接收包含该UE的该位置的移动发起位置请求(MO-LR)响应消息;或者执行定位会话以确定该UE的该位置。

[0195] 条款18.根据条款16或17中任一项所述的UE,其中该至少一个处理器被配置成通过被配置成进行以下操作来测量该RTT:经由该无线收发器从该基站接收指示针对该基站的第一本地传输时间的第一消息;基于针对基站的第一本地传输时间和在UE中接收到第一消息的本地时间来将UE中的本地定时与针对基站的本地传输时间相关联;经由无线收发器在随机接入信道(RACH)上向基站传送第二消息,该第二消息包括随机变量,第二消息在第一时间被传送,其中第一时间是UE中的本地时间或针对基站的相关联本地传输时间;经由该无线收发器响应于该第二消息而从该基站接收第三消息,该第三消息包括第二时间和该随机变量,其中该第二时间是在该基站处接收到该第二消息的针对该基站的本地传输时间;以及基于该第一时间和该第二时间来确定该RTT。

[0196] 条款19.根据条款18所述的UE,其中该第三消息被加密。

[0197] 条款20.根据条款18或19中任一项所述的UE,其中该第三消息进一步包括针对该基站的数字签名,该至少一个处理器被进一步配置成:基于针对该基站的数字签名来认证该第三消息。

[0198] 条款21.根据条款16-20中任一项所述的UE,其中在该无线网络中在该UE与该基站之间存在攻击设备,其中该消息是在重放攻击中经由该攻击设备接收的,该至少一个处理器被进一步配置成:根据该定时提前或通过测量该RTT来确定该传播延迟;以及基于该传播延迟超出预期范围来检测该攻击设备的存在。

[0199] 条款22.根据条款21所述的UE,其中该预期范围包括基于到该基站的预期距离的最大传播延迟。

[0200] 条款23.根据条款21或22中任一项所述的UE,其中该至少一个处理器被进一步配置成:获得该UE的所估计位置和该基站的该位置;确定该UE的所估计位置与该基站的该位置之间的距离估计;以及基于该距离估计来确定该预期范围。

[0201] 条款24.根据条款14-23中任一项所述的UE,其中该消息进一步包括以下中的至少

一者:当前时间到基站子帧或时隙边界的隐式或显式对齐、当前时间的不确定性、当前时间的源、或它们的组合。

[0202] 条款25.根据条款14-24中任一项所述的UE,其中该消息进一步包括针对该基站的数字签名,其中该至少一个处理器被进一步配置成:基于针对该基站的数字签名来认证该消息中的该当前时间。

[0203] 条款26.根据条款25所述的UE,其中该至少一个处理器被进一步配置成:从该无线网络接收针对该基站的公共加密密钥,其中该数字签名基于与该公共加密密钥对应的私有加密密钥,其中认证该当前时间使用该公共加密密钥。

[0204] 条款27.一种被配置用于支持在无线网络中获取时间的用户装备(UE),包括:用于接收从基站广播的消息的部件,该消息包括当前时间,其中该当前时间的至少一部分被加密;用于通过对该当前时间的至少该部分进行解密来获得未加密的当前时间的部件;用于确定该基站与该UE之间的传播延迟的部件;以及用于基于该未加密的当前时间和该传播延迟来确定校正的当前时间的部件。

[0205] 条款28.根据条款27所述的UE,其中该当前时间包括协调世界时(UTC)时间、全球定位系统(GPS)时间、GLONASS时间、北斗时间、伽利略时间、全球导航卫星系统(GNSS)时间、或本地区域时间。

[0206] 条款29.根据条款27或28中任一项所述的UE,其中该用于确定该传播延迟的该部件包括以下中的一者:用于从该基站获得定时提前的部件,其中该传播延迟是根据该定时提前来确定的;用于获得该UE的位置和该基站的位置的部件,其中该传播延迟是基于该UE的该位置与该基站的该位置之间的距离来确定的;或者用于测量该UE与该基站之间的往返传播时间(RTT)的部件,其中该传播延迟等于该RTT的一半。

[0207] 条款30.根据条款29所述的UE,其中该用于获得该UE的该位置和该基站的该位置的部件包括以下中的至少一者:用于在系统信息块(SIB)中接收来自该基站的对该基站的该位置的广播的部件;用于接收包含该基站的该位置的长期演进(LTE)定位协议(LPP)辅助数据消息的部件;用于接收包含该UE的该位置的移动发起位置请求(MO-LR)响应消息的部件;或者用于执行定位会话以确定该UE的该位置的部件。

[0208] 条款31.根据条款29或30中任一项所述的UE,其中该用于测量该RTT的部件包括:用于从该基站接收指示针对该基站的第一本地传输时间的第一消息的部件;用于基于针对该基站的第一本地传输时间和在该UE中接收到该第一消息的本地时间来将该UE中的本地定时与针对该基站的本地传输时间相关联的部件;用于在随机接入信道(RACH)上向该基站传输第二消息的部件,该第二消息包括随机变量,该第二消息在第一时间被传送,其中该第一时间是该UE中的本地时间或针对该基站的相关联本地传输时间;用于响应于该第二消息而从该基站接收第三消息的部件,该第三消息包括第二时间和该随机变量,其中该第二时间是在该基站处接收到该第二消息的针对该基站的本地传输时间;以及用于基于该第一时间和该第二时间来确定该RTT的部件。

[0209] 条款32.根据条款31所述的UE,其中该第三消息被加密。

[0210] 条款33.根据条款31或32中任一项所述的UE,其中该第三消息进一步包括针对该基站的数字签名,该UE进一步包括:用于基于针对该基站的该数字签名来认证该第三消息的部件。

[0211] 条款34.根据条款29-33中任一项所述的UE,其中在该无线网络中在该UE与该基站之间存在攻击设备,其中该消息是在重放攻击中经由该攻击设备接收的,该UE进一步包括:用于根据该定时提前或通过测量该RTT来确定该传播延迟的部件;以及用于基于该传播延迟超出预期范围来检测该攻击设备的存在的部件。

[0212] 条款35.根据条款34所述的UE,其中该预期范围包括基于到该基站的预期距离的最大传播延迟。

[0213] 条款36.根据条款34或35中任一项所述的UE,进一步包括:用于获得该UE的所估计位置 and 该基站的该位置的部件;用于确定该UE的所估计位置与该基站的该位置之间的距离估计的部件;以及用于基于该距离估计来确定该预期范围的部件。

[0214] 条款37.根据条款27-36中任一项所述的UE,其中该消息进一步包括以下中的至少一者:该当前时间到基站子帧或时隙边界的隐式或显式对齐、该当前时间的不确定性、该当前时间的源、或它们的组合。

[0215] 条款38.根据条款27-37中任一项所述的UE,其中该消息进一步包括针对该基站的数字签名,该UE进一步包括:用于基于针对该基站的该数字签名来认证该消息中的该当前时间的部件。

[0216] 条款39.根据条款38所述的UE,进一步包括:用于从该无线网络接收针对该基站的公共加密密钥的部件,其中该数字签名基于与该公共加密密钥对应的私有加密密钥,其中认证该当前时间使用该公共加密密钥。

[0217] 条款40.一种包括存储在其上的程序代码的非暂态计算机可读存储介质,该程序代码能够操作用于配置用户装备 (UE) 中的至少一个处理器以用于支持在无线网络中获取时间,该程序代码包括用于进行以下操作的指令:接收从基站广播的消息,该消息包括当前时间,其中该当前时间的至少一部分被加密;通过对所述当前时间的至少所述部分进行解密来获得未加密的当前时间;确定该基站与该UE之间的传播延迟;以及基于该未加密的当前时间和该传播延迟来确定校正的当前时间。

[0218] 条款41.根据条款40所述的非暂态计算机可读存储介质,其中该当前时间包括协调世界时 (UTC) 时间、全球定位系统 (GPS) 时间、GLONASS时间、北斗时间、伽利略时间、全球导航卫星系统 (GNSS) 时间、或本地区域时间。

[0219] 条款42.根据条款40或41中任一项所述的非暂态计算机可读存储介质,其中该用于确定该传播延迟的指令包括用于以下中的一者的指令:从该基站获得定时提前,其中该传播延迟是根据该定时提前来确定的;获得该UE的位置和该基站的位置,其中该传播延迟是基于该UE的该位置与该基站的该位置之间的距离来确定的;或者测量该UE与该基站之间的往返传播时间 (RTT), 其中该传播延迟等于该RTT的一半。

[0220] 条款43.根据条款42所述的非暂态计算机可读存储介质,其中该用于获得该UE的该位置和该基站的该位置的指令包括用于以下中的至少一者的指令:在系统信息块 (SIB) 中接收来自该基站的对该基站的该位置的广播;接收包含该基站的位置的长期演进 (LTE) 定位协议 (LPP) 辅助数据消息;接收包含该UE的该位置的移动发起位置请求 (MO-LR) 响应消息;或者执行定位会话以确定该UE的该位置。

[0221] 条款44.根据条款42或43中任一项所述的非暂态计算机可读存储介质,其中该用于测量该RTT的指令包括用于进行以下操作的指令:从该基站接收指示针对该基站的第一

本地传输时间的第一消息;基于针对基站的第一本地传输时间和在UE中接收到第一消息的本地时间来将UE中的本地定时与针对基站的本地传输时间相关联;在随机接入信道(RACH)上向该基站传输第二消息,该第二消息包括随机变量,该第二消息在第一时间被传输,其中该第一时间是该UE中的本地时间或针对该基站的相关联本地传输时间;响应于该第二消息而从该基站接收第三消息,该第三消息包括第二时间和该随机变量,其中该第二时间是在该基站处接收到该第二消息的针对该基站的本地传输时间;以及基于该第一时间和该第二时间来确定该RTT。

[0222] 条款45.根据条款44所述的非暂态计算机可读存储介质,其中该第三消息被加密。

[0223] 条款46.根据条款44或45中任一项所述的非暂态计算机可读存储介质,其中该第三消息进一步包括针对该基站的数字签名,该程序代码进一步包括用于进行以下操作的指令:基于针对该基站的该数字签名来认证该第三消息。

[0224] 条款47.根据条款42-46中任一项所述的非暂态计算机可读存储介质,其中在该无线网络中在该UE与该基站之间存在攻击设备,其中该消息是在重放攻击中经由该攻击设备接收的,该程序代码进一步包括用于进行以下操作的指令:根据该定时提前或通过测量该RTT来确定该传播延迟;以及基于该传播延迟超出预期范围来检测该攻击设备的存在。

[0225] 条款48.根据条款47所述的非暂态计算机可读存储介质,其中该预期范围包括基于到该基站的预期最大传播延迟。

[0226] 条款49.根据条款47或48中任一项所述的非暂态计算机可读存储介质,其中该程序代码进一步包括用于以下操作的指令:获得该UE的所估计位置与该基站的该位置;确定该UE的所估计位置与该基站的该位置之间的距离估计;以及基于该距离估计来确定该预期范围。

[0227] 条款50.根据条款40-49中任一项所述的非暂态计算机可读存储介质,其中该消息进一步包括以下中的至少一者:当前时间到基站子帧或时隙边界的隐式或显式对齐、当前时间的不确定性、当前时间的源、或它们的组合。

[0228] 条款51.根据条款40-50中任一项所述的非暂态计算机可读存储介质,其中该第三消息进一步包括针对该基站的数字签名,该程序代码进一步包括用于进行以下操作的指令:基于针对该基站的数字签名来认证该消息中的该当前时间。

[0229] 条款52.根据条款51所述的非暂态计算机可读存储介质,其中该程序代码进一步包括用于进行以下操作的指令:从该无线网络接收针对该基站的公共加密密钥,其中该数字签名基于与该公共加密密钥对应的私有加密密钥,其中认证该当前时间使用该公共加密密钥。

[0230] 条款53.一种由基站执行的用于支持由用户装备(UE)在无线网络中获取时间的方法,包括:获得当前时间;对该当前时间的至少一部分进行加密;以及广播消息,该消息包括该当前时间,其中该UE接收该消息,通过对该当前时间的至少该部分进行解密来获得未加密的当前时间,并且确定该基站与该UE之间的传播延迟,其中该UE基于该未加密的当前时间和该传播延迟来确定校正的当前时间。

[0231] 条款54.根据条款53所述的方法,其中该当前时间包括协调世界时(UTC)时间、全球定位系统(GPS)时间、GLONASS时间、北斗时间、伽利略时间、全球导航卫星系统(GNSS)时间、或本地区域时间。

[0232] 条款55.根据条款53或54中任一项所述的方法,进一步包括通过执行以下中的一者来辅助该UE确定该传播延迟:向该UE发送定时提前,其中该定时提前实现由该UE确定该传播延迟;向该UE发送包括该UE的位置和该基站的位置中的至少一者的消息,其中该传播延迟由该UE基于该UE的该位置与该基站的该位置之间的距离来确定;或者辅助该UE测量该UE与该基站之间的往返传播时间(RTT),其中该传播延迟等于该RTT的一半。

[0233] 条款56.根据条款55所述的方法,其中向该UE发送包括该UE的该位置 and 该基站的该位置中的至少一者的该消息包括以下中的至少一者:在系统信息块(SIB)中广播该基站的该位置;向UE转发包含基站的位置的长期演进(LTE)定位协议(LPP)辅助数据消息;向该UE发送包含该UE的该位置的移动发起位置请求(MO-LR)响应消息;或者在该UE与针对该UE的位置服务器之间传递LPP消息以确定该UE的该位置。

[0234] 条款57.根据条款55或56中任一项所述的方法,其中辅助该UE测量该RTT包括:向该UE发送指示针对该基站的第一本地传输时间的第一消息,其中该UE基于针对该基站的该第一本地传输时间和在该UE中接收到该第一消息的本地时间来将该UE中的本地定时与针对该基站的本地传输时间相关联;在随机接入信道(RACH)上从UE接收第二消息,该第二消息包括随机变量,该第二消息在第一时间被传送,其中第一时间是UE中的本地时间或针对基站的相关本地传输时间;测量第二时间,其中该第二时间是在该基站处接收到该第二消息的针对该基站的本地传输时间;以及响应于该第二消息而向该UE发送第三消息,该第三消息包括该第二时间和该随机变量,其中该UE基于该第一时间和该第二时间来确定该RTT。

[0235] 条款58.根据条款57所述的方法,进一步包括加密该第三消息。

[0236] 条款59.根据条款57或58中任一项所述的方法,进一步包括在该第三消息中包括针对该基站的数字签名,其中该UE基于针对该基站的数字签名来认证该第三消息。

[0237] 条款60.根据条款55-59中任一项所述的方法,其中在该无线网络中在该UE与该基站之间存在攻击设备,其中该消息是由该UE在重放攻击中经由该攻击设备接收的,其中该UE根据该定时提前或通过测量该RTT来确定该传播延迟;并且其中该UE基于该传播延迟超出预期范围来检测该攻击设备的存在。

[0238] 条款61.根据条款60所述的方法,其中该预期范围包括基于该UE与该基站之间的最大预期距离的最大传播延迟。

[0239] 条款62.根据条款60或61中任一项所述的方法,其中该预期范围基于该UE的所估计位置和由该UE获得的该基站的位置。

[0240] 条款63.根据条款53-62中任一项所述的方法,进一步包括在该消息中包括以下中的至少一者:当前时间到基站子帧或时隙边界的隐式或显式对齐、当前时间的不确定性、从其获得当前时间的源、或它们的组合。

[0241] 条款64.根据条款53-63中任一项所述的方法,进一步包括在该消息中包括针对该基站的数字签名,其中该UE基于针对该基站的数字签名来认证该消息中的当前时间。

[0242] 条款65.根据条款64所述的方法,进一步包括:向该UE发送针对该基站的公共加密密钥,其中该数字签名基于与该公共加密密钥对应的私有加密密钥,其中该UE使用该公共加密密钥来认证该当前时间。

[0243] 条款66.一种被配置用于支持由用户装备(UE)在无线网络中获取时间的基站,包

括:外部接口,该外部接口被配置成与该无线网络中的实体进行无线通信;至少一个存储器;至少一个处理器,该至少一个处理器耦合到该外部接口和该至少一个存储器,其中该至少一个处理器被配置成:获得当前时间;对该当前时间的至少一部分进行加密;以及广播消息,该消息包括该当前时间,其中该UE接收该消息,通过对该当前时间的至少该部分进行解密来获得未加密的当前时间,并且确定该基站与该UE之间的传播延迟,其中该UE基于该未加密的当前时间和该传播延迟来确定校正的当前时间。

[0244] 条款67.根据条款66所述的基站,其中该当前时间包括协调世界时(UTC)时间、全球定位系统(GPS)时间、GLONASS时间、北斗时间、伽利略时间、全球导航卫星系统(GNSS)时间、或本地区域时间。

[0245] 条款68.根据条款66或67中任一项所述的基站,其中该至少一个处理器被进一步配置成通过被配置用于以下中的一者来辅助该UE确定该传播延迟:向该UE发送定时提前,其中该定时提前实现由该UE确定该传播延迟;向该UE发送包括该UE的位置和该基站的位置中的至少一者的消息,其中该传播延迟由该UE基于该UE的该位置与该基站的该位置之间的距离来确定;或者辅助该UE测量该UE与该基站之间的往返传播时间(RTT),其中该传播延迟等于该RTT的一半。

[0246] 条款69.根据条款68所述的基站,其中该至少一个处理器被进一步配置成通过被配置用于以下中的至少一者来向该UE发送包括该UE的该位置 and 该基站的该位置中的至少一者的该消息:在系统信息块(SIB)中广播该基站的该位置;向UE转发包含基站的位置的长期演进(LTE)定位协议(LPP)辅助数据消息;向该UE发送包含该UE的该位置的移动发起位置请求(MO-LR)响应消息;或者在该UE与针对该UE的位置服务器之间传递LPP消息以确定该UE的该位置。

[0247] 条款70.根据条款68或69中任一项所述的基站,其中该至少一个处理器被进一步配置成通过被配置成进行以下操作来辅助该UE测量该RTT:向该UE发送指示针对该基站的第一本地传输时间的第一消息,其中该UE基于针对该基站的该第一本地传输时间和在该UE中接收到该第一消息的本地时间来将该UE中的本地定时与针对该基站的本地传输时间相关联;在随机接入信道(RACH)上从UE接收第二消息,该第二消息包括随机变量,该第二消息在第一时间被传送,其中第一时间是UE中的本地时间或针对基站的相关联本地传输时间;测量第二时间,其中该第二时间是在该基站处接收到该第二消息的针对该基站的本地传输时间;以及响应于该第二消息而向该UE发送第三消息,该第三消息包括该第二时间和该随机变量,其中该UE基于该第一时间和该第二时间来确定该RTT。

[0248] 条款71.根据条款70所述的基站,其中该至少一个处理器被进一步配置成加密该第三消息。

[0249] 条款72.根据条款70或71中任一项所述的基站,其中该至少一个处理器被进一步配置成在第三消息中包括针对该基站的数字签名,其中该UE基于针对该基站的数字签名来认证该第三消息。

[0250] 条款73.根据条款68-72中任一项所述的基站,其中在该无线网络中在该UE与该基站之间存在攻击设备,其中该消息是由该UE在重放攻击中经由该攻击设备接收的,其中该UE根据该定时提前或通过测量该RTT来确定该传播延迟;并且其中该UE基于该传播延迟超出预期范围来检测该攻击设备的存在。

[0251] 条款74.根据条款73所述的基站,其中该预期范围包括基于该UE与该基站之间的最大预期距离的最大传播延迟。

[0252] 条款75.根据条款73或74中任一项所述的基站,其中该预期范围基于该UE的所估计位置和由该UE获得的该基站的位置。

[0253] 条款76.根据条款66-75中任一项所述的基站,其中该至少一个处理器被进一步配置成在该消息中包括以下中的至少一者:当前时间到针对该基站的子帧或时隙边界的隐式或显式对齐、当前时间的不确定性、从其获得该当前时间的源、或它们的组合。

[0254] 条款77.根据条款66-76中任一项所述的基站,其中该至少一个处理器被进一步配置成在该消息中包括针对该基站的数字签名,其中该UE基于针对该基站的数字签名来认证该消息中的当前时间。

[0255] 条款78.根据条款77所述的基站,其中该至少一个处理器被进一步配置成:向该UE发送针对该基站的公共加密密钥,其中该数字签名基于与该公共加密密钥对应的私有加密密钥,其中该UE使用该公共加密密钥来认证该当前时间。

[0256] 条款79.一种被配置用于支持由用户装备(UE)在无线网络中获取时间的基站,包括:用于获得当前时间的部件;用于对该当前时间的至少一部分进行加密的部件;以及用于广播消息的部件,该消息包括该当前时间,其中该UE接收该消息,通过对该当前时间的至少该部分进行解密来获得未加密的当前时间,并且确定该基站与该UE之间的传播延迟,其中该UE基于该未加密的当前时间和该传播延迟来确定校正的当前时间。

[0257] 条款80.根据条款79所述的基站,其中该当前时间包括协调世界时(UTC)时间、全球定位系统(GPS)时间、GLONASS时间、北斗时间、伽利略时间、全球导航卫星系统(GNSS)时间、或本地区域时间。

[0258] 条款81.根据条款79或80中任一项所述的基站,进一步包括用于辅助该UE确定该传播延迟的部件,其包括以下中的一者:用于向该UE发送定时提前的部件,其中该定时提前实现由该UE确定该传播延迟;用于向该UE发送包括该UE的位置和该基站的位置中的至少一者的消息的部件,其中该传播延迟由该UE基于该UE的该位置与该基站的该位置之间的距离来确定;或者用于辅助该UE测量该UE与该基站之间的往返传播时间(RTT)的部件,其中该传播延迟等于该RTT的一半。

[0259] 条款82.根据条款81所述的基站,其中该用于向该UE发送包括该UE的该位置和该基站的该位置中的至少一者的该消息的部件包括以下中的至少一者:用于在系统信息块(SIB)中广播该基站的该位置的部件;用于向该UE转发包含该基站的该位置的长期演进(LTE)定位协议(LPP)辅助数据消息的部件;用于向该UE发送包含该UE的该位置的移动发起位置请求(MO-LR)响应消息的部件;或者用于在该UE与针对该UE的位置服务器之间传递LPP消息以确定该UE的该位置的部件。

[0260] 条款83.根据条款81或82中任一项所述的基站,其中该用于辅助该UE测量该RTT的部件包括:用于向该UE发送指示针对该基站的第一本地传输时间的第一消息的部件,其中该UE基于针对该基站的该第一本地传输时间和在该UE中接收到该第一消息的本地时间来将该UE中的本地定时与针对该基站的本地传输时间相关联;用于在随机接入信道(RACH)上从该UE接收第二消息的部件,该第二消息包括随机变量,该第二消息在第一时间被传送,其中该第一时间是该UE中的本地时间或针对该基站的相关联本地传输时间;用于测量第二时

间的部件,其中该第二时间是在该基站处接收到该第二消息的针对该基站的本地传输时间;以及用于响应于该第二消息而向该UE发送第三消息的部件,该第三消息包括该第二时间和该随机变量,其中该UE基于该第一时间和该第二时间来确定该RTT。

[0261] 条款84.根据条款83所述的基站,进一步包括用于加密该第三消息的部件。

[0262] 条款85.根据条款83或84中任一项所述的基站,进一步包括用于在第三消息中包括针对该基站的数字签名的部件,其中该UE基于针对该基站的数字签名来认证该第三消息。

[0263] 条款86.根据条款81-85中任一项所述的基站,其中在该无线网络中在该UE与该基站之间存在攻击设备,其中该消息是由该UE在重放攻击中经由该攻击设备接收的,其中该UE根据该定时提前或通过测量该RTT来确定该传播延迟;并且其中该UE基于该传播延迟超出预期范围来检测该攻击设备的存在。

[0264] 条款87.根据条款86所述的基站,其中该预期范围包括基于该UE与该基站之间的最大预期距离的最大传播延迟。

[0265] 条款88.根据条款86或87中任一项所述的基站,其中该预期范围基于该UE的所估计位置和由该UE获得的该基站的该位置。

[0266] 条款89.根据条款79-88中任一项所述的基站,进一步包括用于在该消息中包括以下中的至少一者的部件:当前时间到针对该基站的子帧或时隙边界的隐式或显式对齐、当前时间的不确定性、从其获得当前时间的源、或它们的组合。

[0267] 条款90.根据条款79-89中任一项所述的基站,进一步包括用于在该消息中包括针对该基站的数字签名的部件,其中该UE基于针对该基站的数字签名来认证该消息中的当前时间。

[0268] 条款91.根据条款90所述的基站,进一步包括:用于向该UE发送针对该基站的公共加密密钥的部件,其中该数字签名基于与该公共加密密钥对应的私有加密密钥,其中该UE使用该公共加密密钥来认证该当前时间。

[0269] 条款92.一种包括存储在其上的程序代码的非暂态计算机可读存储介质,该程序代码能够操作以配置基站中的至少一个处理器用于支持由用户装备(UE)在无线网络中获取时间,该程序代码包括用于进行以下操作的指令:获得当前时间;对该当前时间的至少一部分进行加密;以及广播消息,该消息包括该当前时间,其中该UE接收该消息,通过对该当前时间的至少该部分进行解密来获得未加密的当前时间,并且确定该基站与该UE之间的传播延迟,其中该UE基于该未加密的当前时间和该传播延迟来确定校正的当前时间。

[0270] 条款93.根据条款92所述的非暂态计算机可读存储介质,其中该当前时间包括协调世界时(UTC)时间、全球定位系统(GPS)时间、GLONASS时间、北斗时间、伽利略时间、全球导航卫星系统(GNSS)时间、或本地区域时间。

[0271] 条款94.根据条款92或93中任一项所述的非暂态计算机可读存储介质,进一步包括用于辅助该UE确定该传播延迟的指令,其包括用于以下中的一者的指令:向该UE发送定时提前,其中该定时提前实现由该UE确定该传播延迟;向该UE发送包括该UE的位置和该基站的位置中的至少一者的消息,其中该传播延迟由该UE基于该UE的该位置与该基站的该位置之间的距离来确定;或者辅助该UE测量该UE与该基站之间的往返传播时间(RTT),其中该传播延迟等于该RTT的一半。

[0272] 条款95.根据条款94所述的非暂态计算机可读存储介质,其中该用于向该UE发送包括该UE的该位置和该基站的该位置中的至少一者的该消息的指令包括用于以下中的至少一者的指令:在系统信息块(SIB)中广播该基站的该位置;向UE转发包含基站的位置的长期演进(LTE)定位协议(LPP)辅助数据消息;向该UE发送包含该UE的该位置的移动发起位置请求(MO-LR)响应消息;或者在该UE与针对该UE的位置服务器之间传递LPP消息以确定该UE的该位置。

[0273] 条款96.根据条款94或95中任一项所述的非暂态计算机可读存储介质,其中该用于辅助该UE测量该RTT的指令包括用于进行以下操作的指令:向该UE发送指示针对该基站的第一本地传输时间的第一消息,其中该UE基于针对该基站的该第一本地传输时间和在该UE中接收到该第一消息的本地时间来将该UE中的本地定时与针对该基站的本地传输时间相关联;在随机接入信道(RACH)上从UE接收第二消息,该第二消息包括随机变量,该第二消息在第一时间被传送,其中第一时间是UE中的本地时间或针对基站的相关联本地传输时间;测量第二时间,其中该第二时间是在该基站处接收到该第二消息的针对该基站的本地传输时间;以及响应于该第二消息而向该UE发送第三消息,该第三消息包括该第二时间和该随机变量,其中该UE基于该第一时间和该第二时间来确定该RTT。

[0274] 条款97.根据条款96所述的非暂态计算机可读存储介质,其中该程序代码进一步包括用于加密该第三消息的指令。

[0275] 条款98.根据条款96或97中任一项所述的非暂态计算机可读存储介质,其中该程序代码进一步包括用于在第三消息中包括针对该基站的数字签名的指令,其中该UE基于针对该基站的数字签名来认证该第三消息。

[0276] 条款99.根据条款94-98中任一项所述的非暂态计算机可读存储介质,其中在该无线网络中在该UE与该基站之间存在攻击设备,其中该消息是由该UE在重放攻击中经由该攻击设备接收的,其中该UE根据该定时提前或通过测量该RTT来确定该传播延迟;并且其中该UE基于该传播延迟超出预期范围来检测该攻击设备的存在。

[0277] 条款100.根据条款99所述的非暂态计算机可读存储介质,其中该预期范围包括基于该UE与该基站之间的最大预期距离的最大传播延迟。

[0278] 条款101.根据条款99或100中任一项所述的非暂态计算机可读存储介质,其中该预期范围基于该UE的所估计位置和由该UE获得的该基站的位置。

[0279] 条款102.根据条款92-101中任一项所述的非暂态计算机可读存储介质,其中该程序代码进一步用于在该消息中包括以下中的至少一者的指令:当前时间到针对该基站的子帧或时隙边界的隐式或显式对齐、当前时间的不确定性、从其获得当前时间的源、或它们的组合。

[0280] 条款103.根据条款92-102中任一项所述的非暂态计算机可读存储介质,其中该程序代码进一步包括用于在该消息中包括针对该基站的数字签名的指令,其中该UE基于针对该基站的数字签名来认证该消息中的当前时间。

[0281] 条款104.根据条款103所述的非暂态计算机可读存储介质,其中该程序代码进一步包括用于进行以下操作的指令:向该UE发送针对该基站的公共加密密钥,其中该数字签名基于与该公共加密密钥对应的私有加密密钥,其中该UE使用该公共加密密钥来认证该当前时间。

[0282] 因此,所要求保护的主体内容旨在不限于所公开的特定示例,而是所要求保护的主体内容还可包括落入所附权利要求及其等同物的范围内的所有方面。

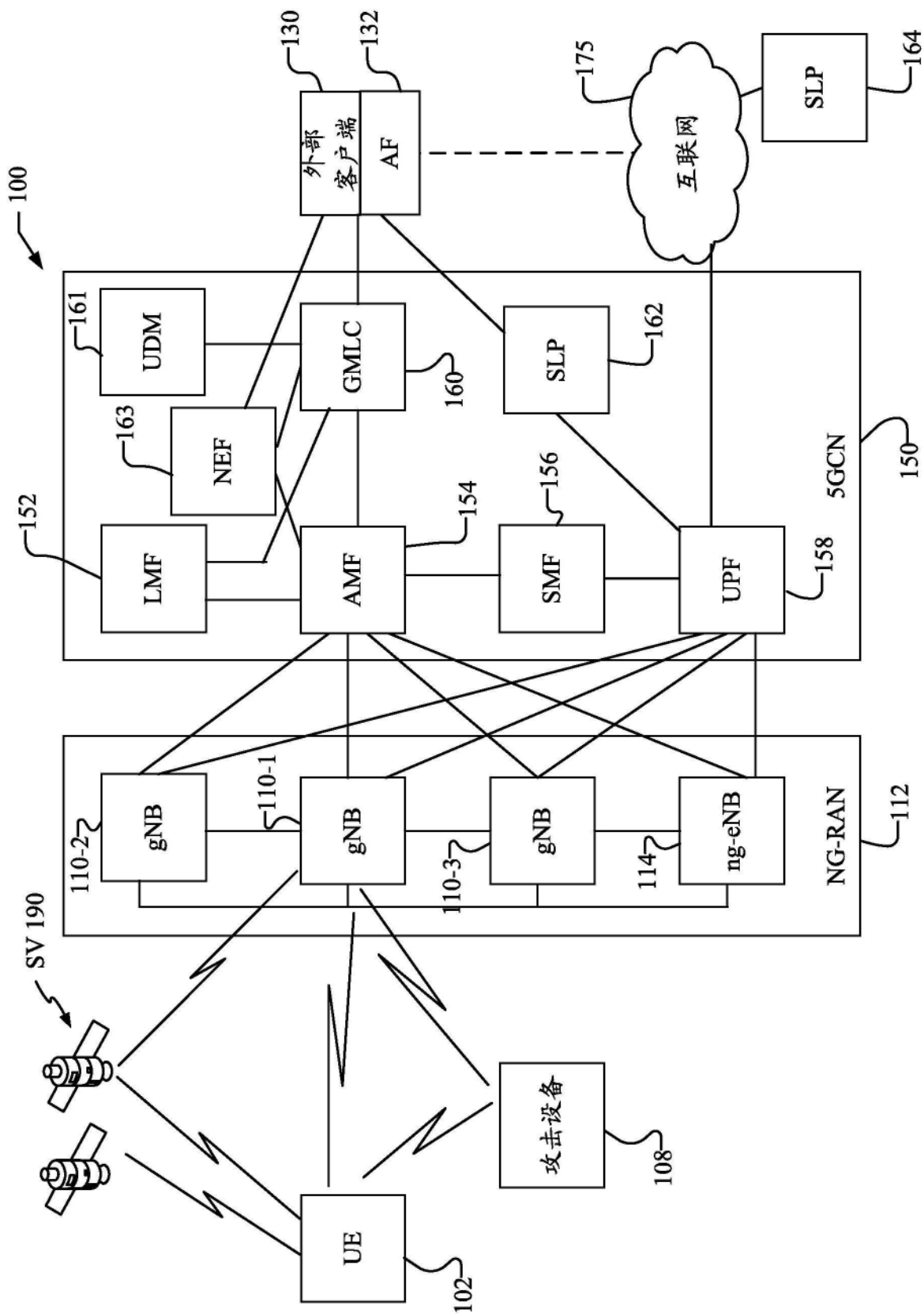


图1

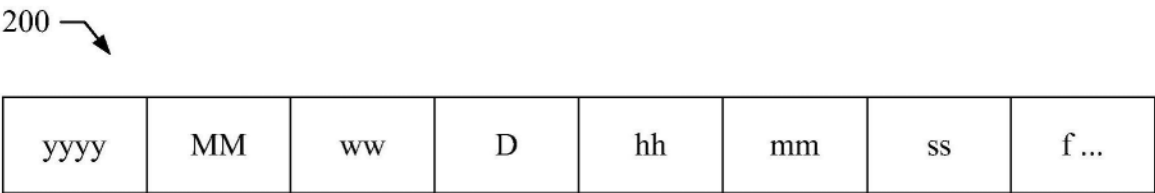


图2A

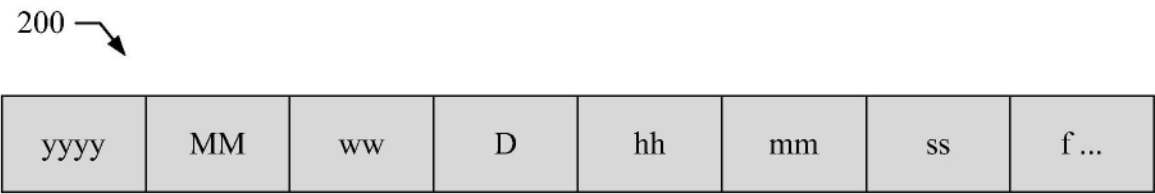


图2B

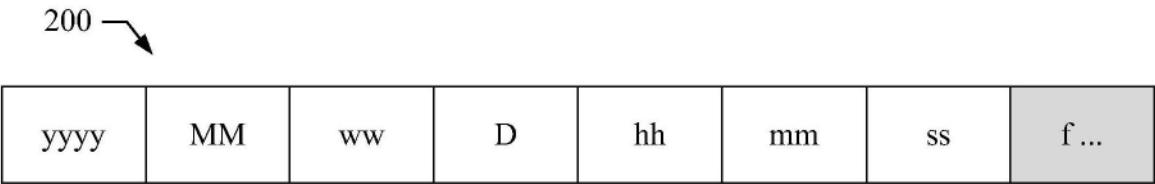


图2C

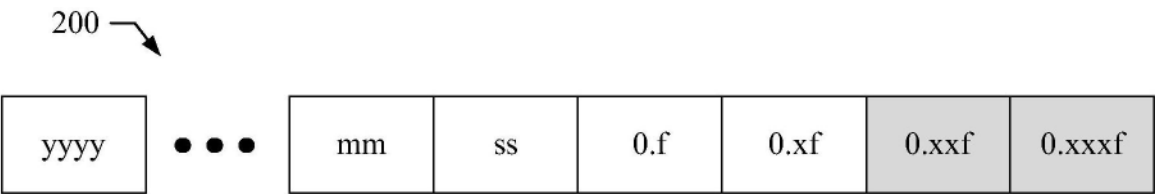


图2D

当前时间 (UTC)	本地时间	准确度/ 不确定性	时间源	DigSig
---------------	------	--------------	-----	--------

图2E

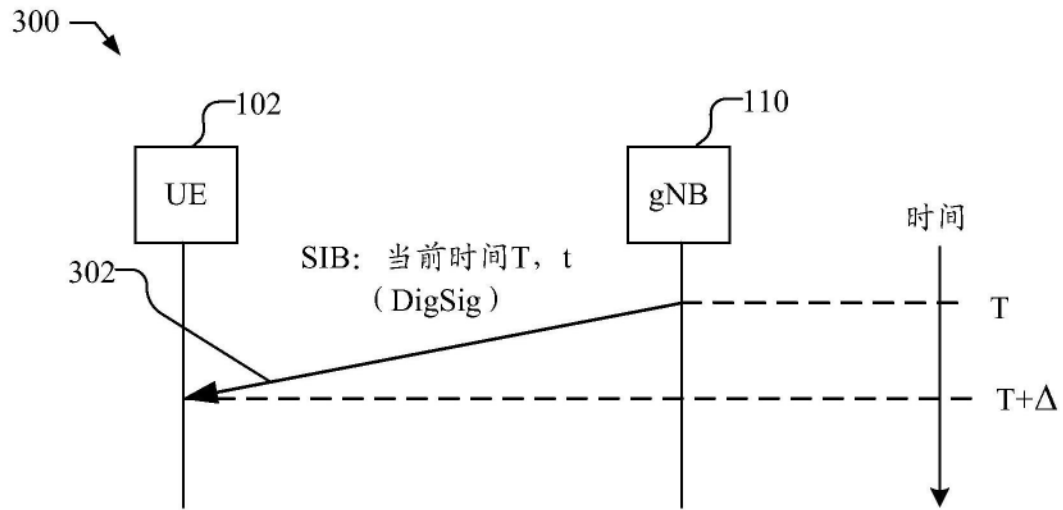


图3A

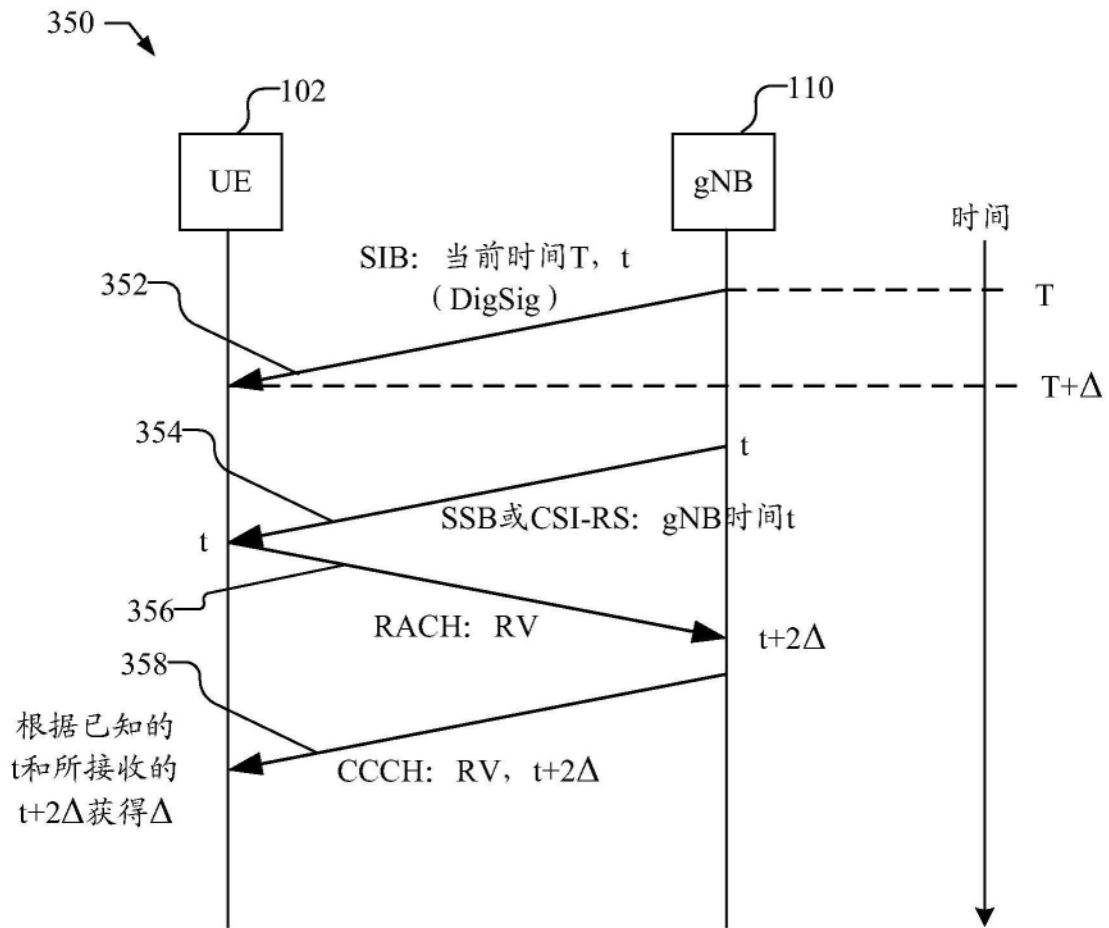


图3B

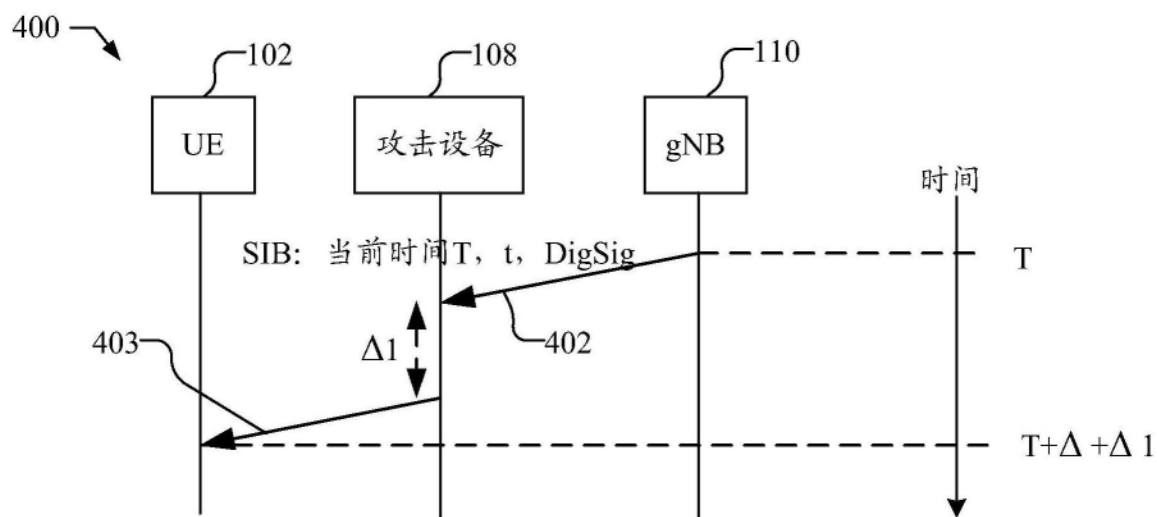


图4A

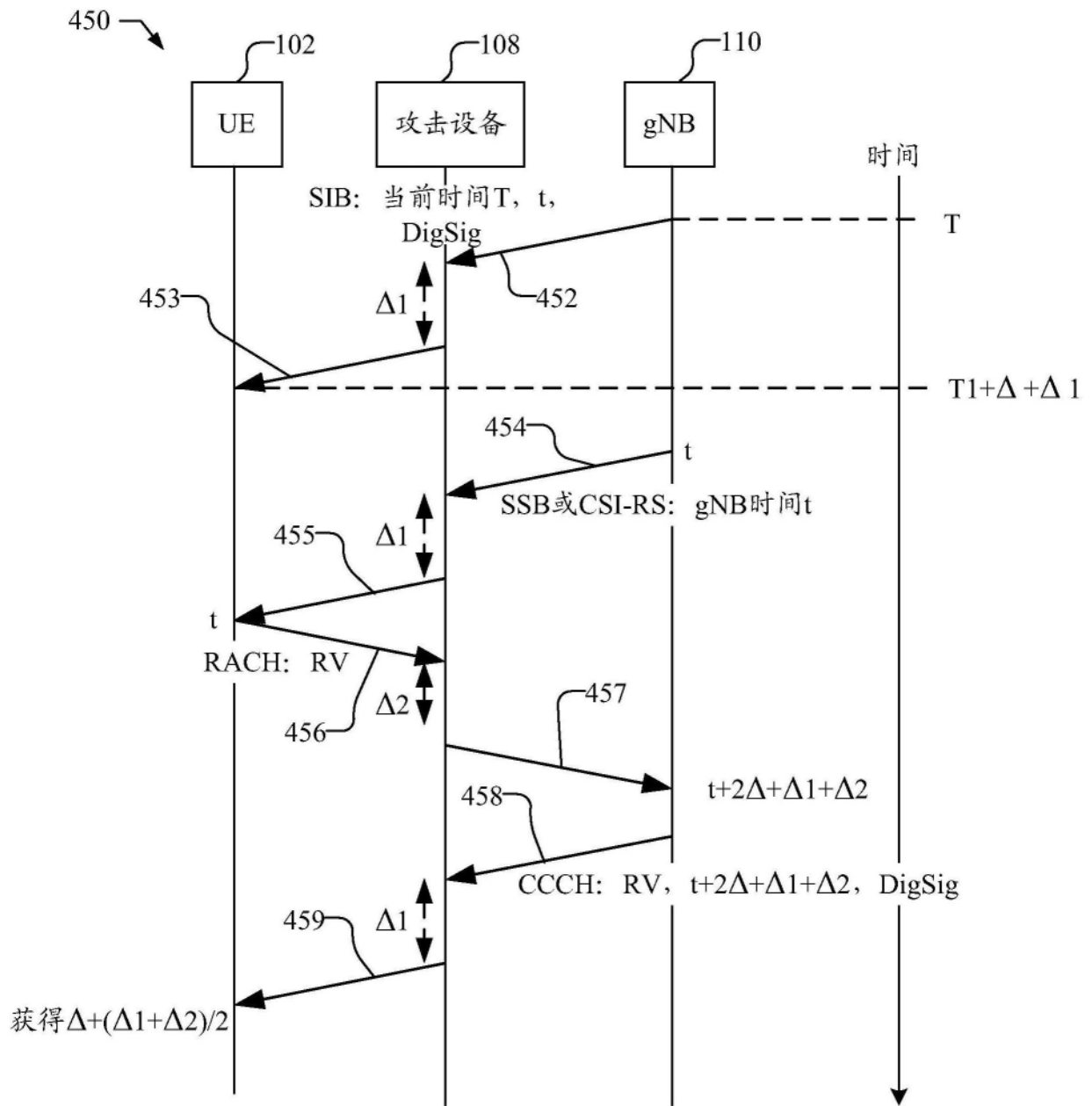


图4B

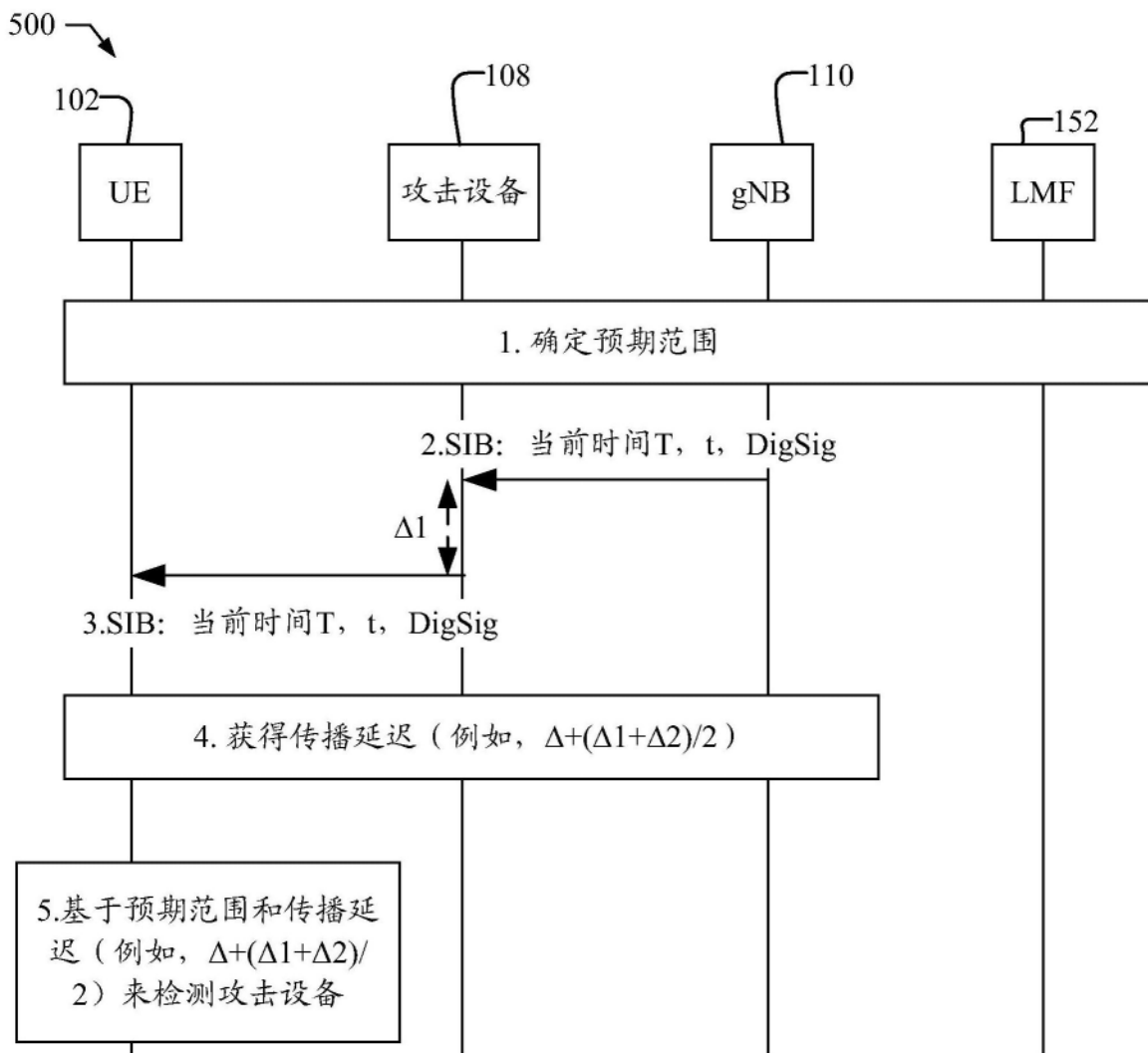


图5

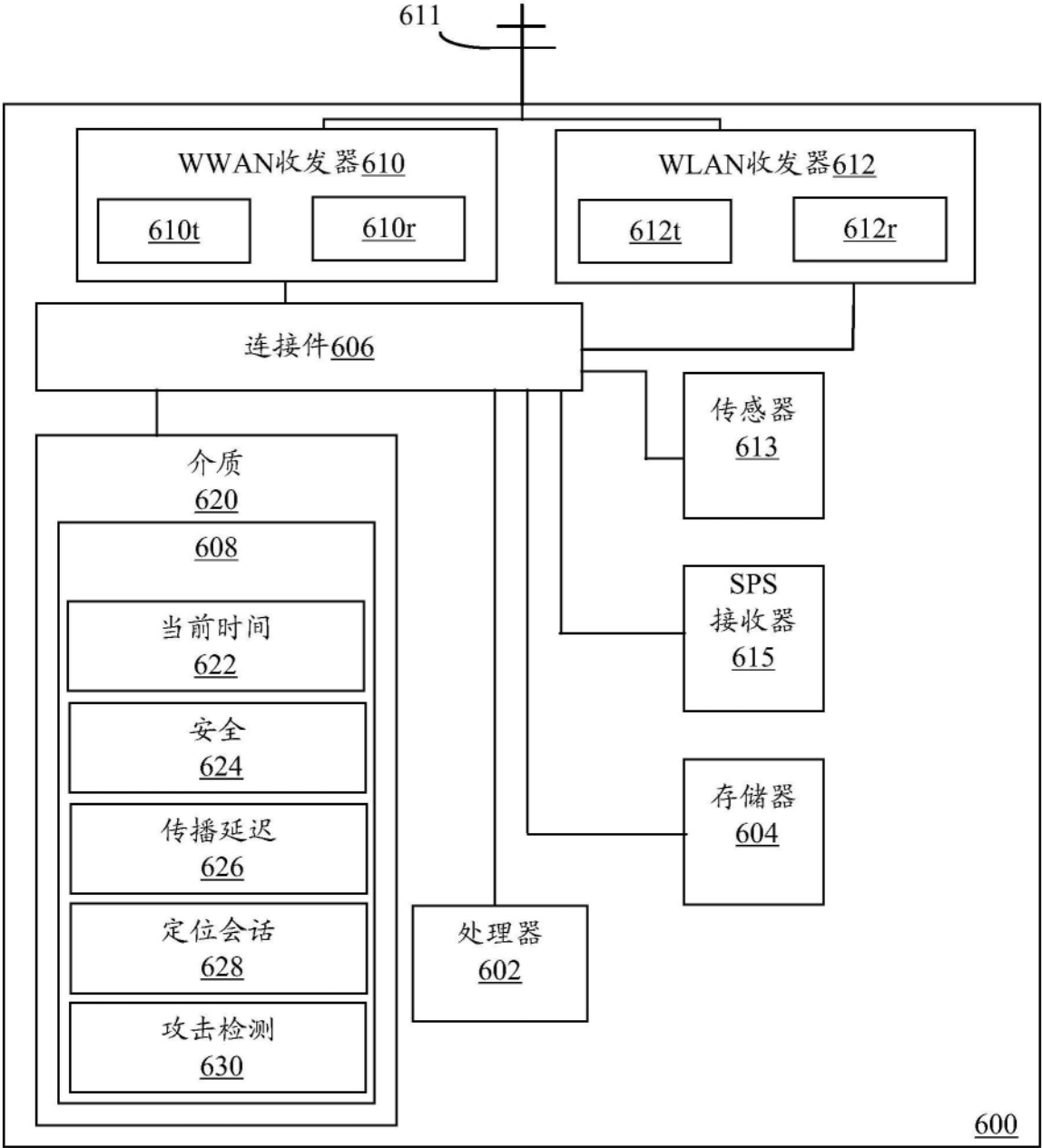


图6

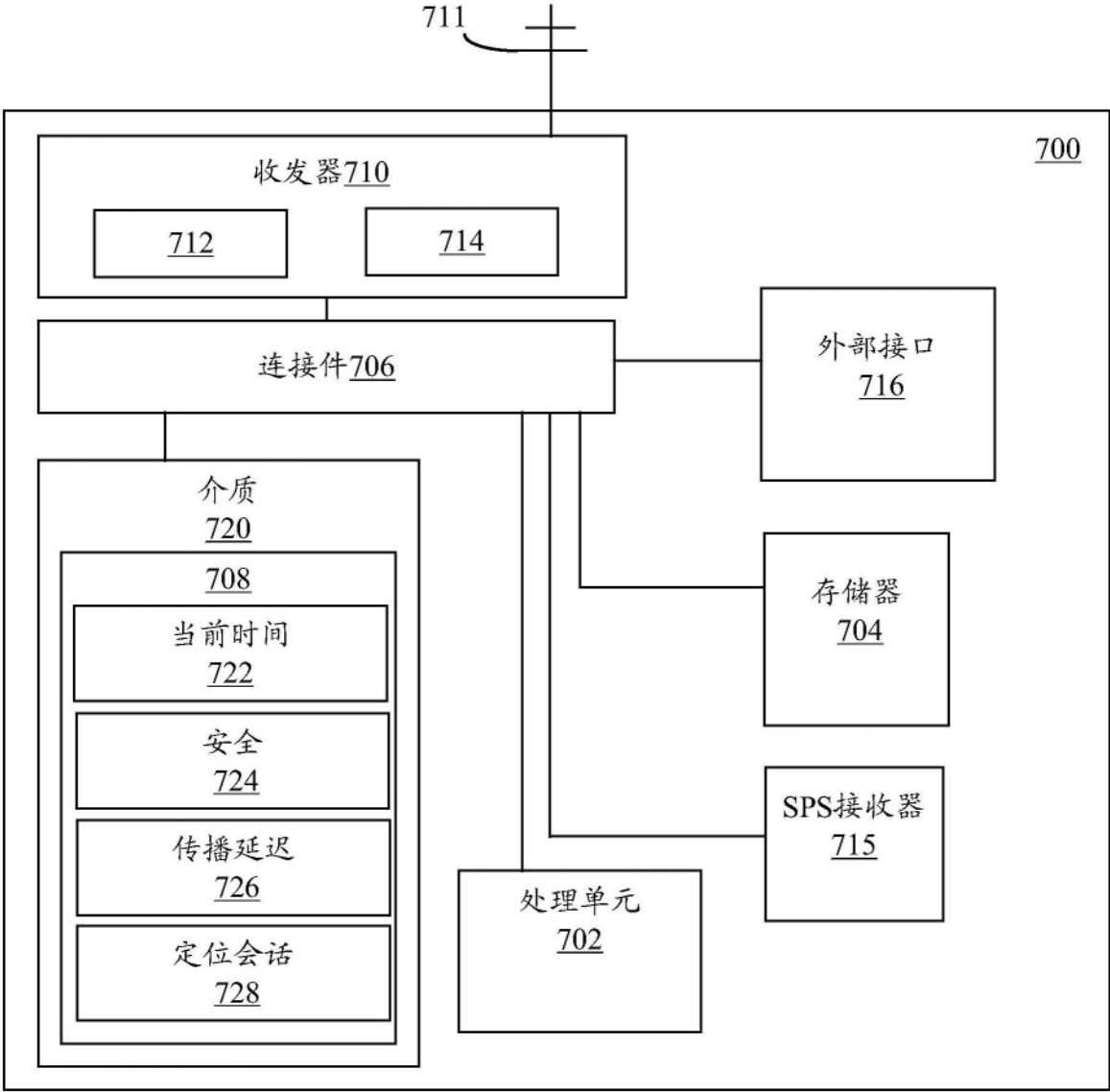


图7

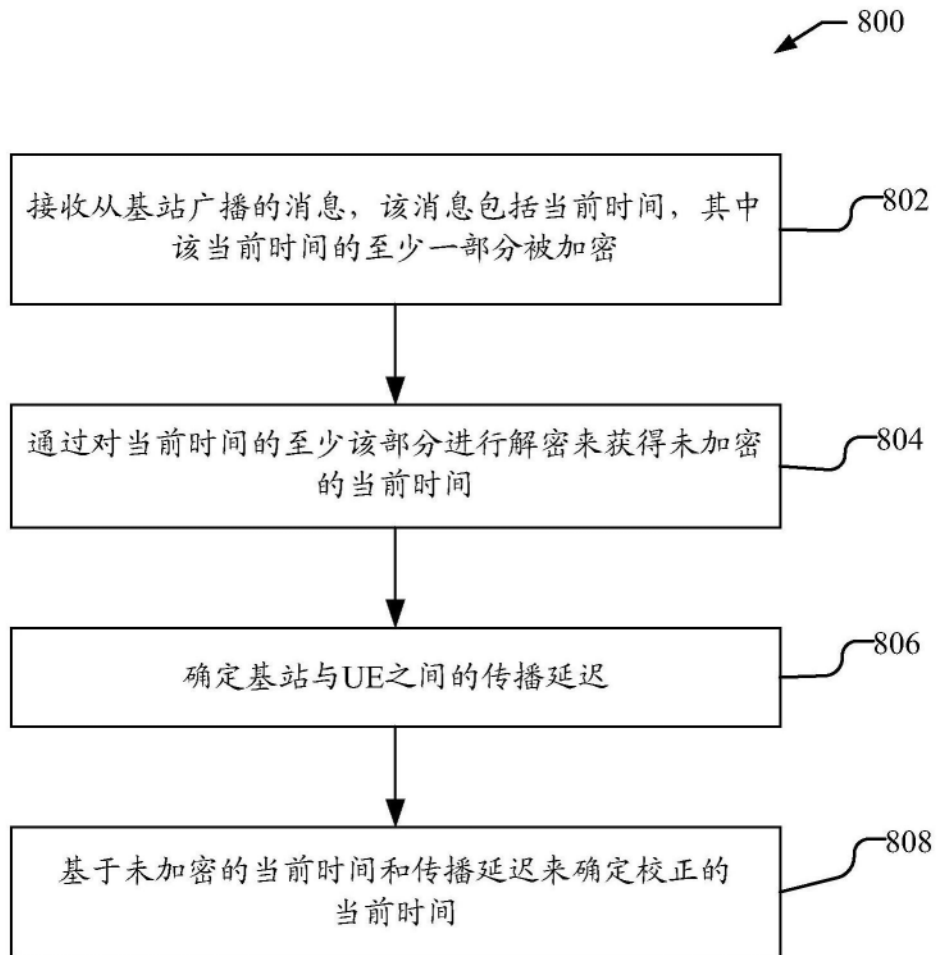


图8

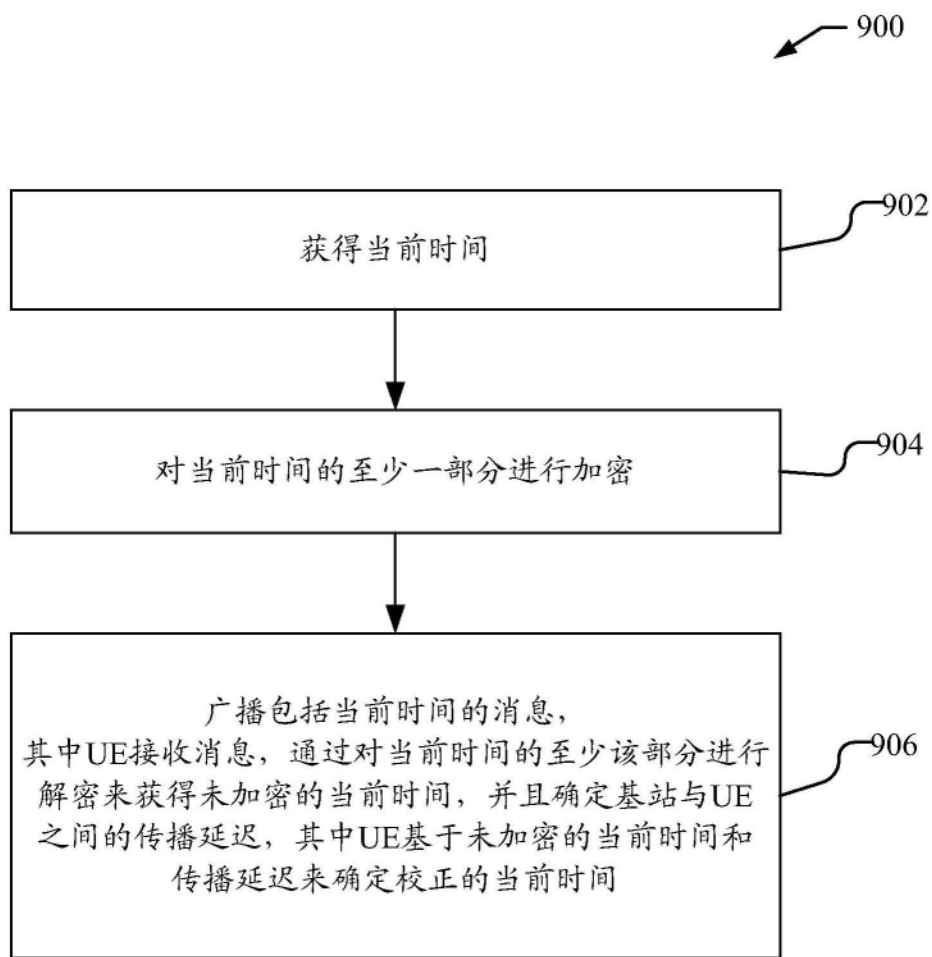


图9