(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 113455019 B
(45)授权公告日 2024.04.12

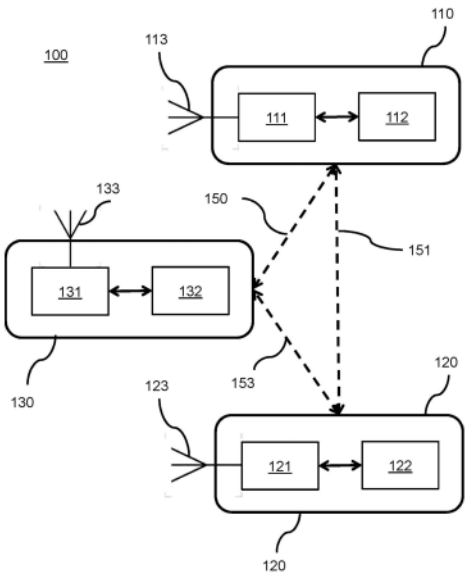
(21)申请号 202080015093.9
(22)申请日 2020.02.17
(65)同一申请的已公布的文献号
申请公布号 CN 113455019 A
(43)申请公布日 2021.09.28
(30)优先权数据
19158080.2 2019.02.19 EP
(85)PCT国际申请进入国家阶段日
2021.08.18
(86)PCT国际申请的申请数据
PCT/EP2020/054029 2020.02.17
(87)PCT国际申请的公布数据
WO2020/169505 EN 2020.08.27
(73)专利权人 皇家飞利浦有限公司
地址 荷兰艾恩德霍芬
(72)发明人 J·A·C·伯恩森
(74)专利代理机构 永新专利商标代理有限公司 72002
专利代理师 李光颖
(51)Int.Cl.
H04W 4/02(2018.01)
G01S 5/02(2010.01)
G01S 5/14(2006.01)
H04W 64/00(2009.01)
(56)对比文件
CN 101103282 A,2008.01.09
CN 108291960 A,2018.07.17
EP 2533569 A1,2012.12.12
EP 3072272 A1,2016.09.28
TW 201831027 A,2018.08.16
US 2012315895 A1,2012.12.13
US 2017257758 A1,2017.09.07
WO 2018122184 A1,2018.07.05
审查员 张慧丽
权利要求书4页 说明书33页 附图7页

(54)发明名称

用于受信距离测量的系统

(57)摘要

一种设备被布置用于使用来自第二设备的测量消息根据测距协议进行距离测量。基于所述测量消息的第一到达时间,确定所述第一设备(110)和所述第二设备(120)之间的第一距离(151)。第三设备(130)充当位于受信距离(150)处的协作设备。所述协作设备确定相同测量消息的第三到达时间,并且将支持数据传送到所述第一设备,所述支持数据基于所述第三到达时间。所述第一设备使用所述支持数据获得所述第三设备和所述第二设备之间的第三距离(153)。然后,对所述第一距离(151)、所述受信距离(150)和所述第三距离(153)执行验证测试。当所述距离对应于所述设备的可行空间群集(100)时,所述第一距离是可靠的。



CN 113455019 B

1.一种用于经由无线通信进行距离测量的设备,所述无线通信是用于无线通信的充当第一设备(110)的所述设备与第二设备(120)之间的无线通信,

所述无线通信包括用于基于测量消息到达所述第一设备的到达时间来确定所述第一设备与所述第二设备之间的距离的测距协议,所述协议包括由所述第二设备发送所述测量消息;

所述设备包括:

第一收发器(111),其用于消息的发送和接收,

第一消息处理器(112),其被布置用于:

根据所述测距协议处理所述消息,

确定所述测量消息到达所述第一设备的第一到达时间,并且

基于所述第一到达时间确定所述第一设备与所述第二设备之间的第一距离(151);

其中,所述第一消息处理器(112)被布置用于与第三设备(130)通信,充当协作设备的所述第三设备位于相距所述第一设备的受信距离(150)处,

并且

为了评价所确定的距离,所述第一消息处理器被布置为

从所述协作设备接收支持数据,所述支持数据基于所述测量消息到达所述协作设备的第三到达时间,

使用所述支持数据获得所述第三设备与所述第二设备之间的第三距离(153),并且

对所述第一距离(151)、所述受信距离(150)和所述第三距离(153)执行验证测试,当所述的距离对应于所述第一设备、所述第二设备和所述协作设备的可行空间群集(100)时,所述验证测试将所述第一距离接受为可靠的。

2.根据权利要求1所述的设备,其中,所述验证测试包括对所述可行空间群集的余弦规则检查或三角不等式检查。

3.根据权利要求1或2所述的设备,其中,所述测距协议包括交换基于密钥数据加密保护的消息,并且所述第一消息处理器(112)被布置为与所述协作设备共享所述密钥数据,以使得第三消息处理器(132)能够根据所述测距协议对所述消息进行加密处理。

4.根据权利要求1或2所述的设备,其中,所述第一消息处理器(112)被布置为根据所述测距协议来确定所述受信距离。

5.根据权利要求1或2所述的设备,其中,所述设备包括时钟单元以提供用于确定所述到达时间的时间参考,并且所述第一消息处理器(112)被布置为使所述时间参考与所述协作设备中的对应时钟单元同步。

6.根据权利要求1或2所述的设备,其中,所述测距协议包括充当发起设备的所述第一设备向所述第二设备发送发起消息,同时在接收到所述发起消息时,所述第二设备必须发送所述测量消息,并且所述第一消息处理器(112)被布置为:

与所述第三设备交换角色改变数据,以使得所述第三设备能够充当所述发起设备以用于距离测量;

所述第三设备被布置为在接收到所述角色改变数据时,

基于第二测量消息根据所述测距协议获得所述第三设备与所述第二设备之间的第三距离,并且

将第三支持数据传送到所述第一设备,所述第三支持数据指示所述第三距离;

同时所述第一消息处理器(112)被布置为:

当在所述第一设备处接收到所述第二测量消息时,确定所述第一设备与所述第二设备之间的第二距离,

从所述第三设备接收所述第三支持数据,并且

还使用所述第二距离和所述第三支持数据来执行所述验证测试。

7.根据权利要求3所述的设备,其中,

所述第三消息处理器(132)被布置为:

确定从所述第二设备接收的至少一个消息的第三信号强度,并且

将第三信号强度数据包括在到所述第一设备的所述支持数据中;并且

所述第一消息处理器(112)被布置为:

确定从所述第二设备接收的至少一个消息的第一信号强度,并且

通过将所述第一信号强度和所述第三信号强度与所确定的距离处的相应预期信号强度进行比较来验证所确定的距离是否可靠。

8.根据权利要求1或2所述的设备,其中,在评价所确定的距离不可靠时,所述第一消息处理器(112)被布置为执行以下中的至少一项:

要求与所述第二设备执行不同的安全协议;

使用不同的测距协议和/或不同类型的无线通信来请求另外的距离测量;

拒绝或限制对所述第一设备中的至少一些数据和/或至少一个功能的访问。

9.一种用于可靠距离测量的系统,包括根据前述权利要求1-8中的任一项所述的设备、根据权利要求1所述的第三设备和充当第二协作设备的第四设备,所述第四设备位于相距所述第一设备或相距所述第三设备的第二受信距离处,

所述第四设备包括:

第四无线接收器(141),其用于消息的接收,

第四消息处理器(142),其被布置用于:

确定所述测量消息到达所述第四设备的第四到达时间,并且

将第四支持数据传送到所述第一设备,所述第四支持数据基于所述第四到达时间;

其中,所述第一消息处理器(112)被布置用于:

从所述第二协作设备接收所述第四支持数据,

使用所述第四支持数据获得所述第四设备与所述第二设备之间的第四距离,并且

还使用所述第二受信距离和所述第四距离来执行所述验证测试。

10.根据权利要求9所述的系统,其中,所述第一消息处理器(112)被布置为:

使用关于所述第一设备、所述第二设备和所述第三设备的第一空间群集的第一三角不等式与关于所述第一设备、所述第二设备和所述第四设备的第二空间群集的第二三角不等式的组合来执行所述验证测试;或

验证所述第二设备根据所述第一空间群集的第一位置是否对应于所述第二设备根据所述第二空间群集的第二位置;或

使用不一致性检查来执行验证测试以便检测是否所有确定的距离都大于零;或

基于以下设置来执行所述验证测试,其中,所述第三设备和所述第四设备被布置为使

得从第三设备到第一设备的线与从第四设备到第一设备的线之间的受信角为至少90度;或

基于以下设置来执行所述验证测试,其中,所述第三设备和所述第四设备相对于所述第一设备彼此相对布置;或

基于以下设置来执行所述验证测试,其中,所述第二受信距离对应于所述受信距离。

11.根据权利要求9或10所述的系统,所述系统包括充当另外的协作设备的至少一个另外的设备,其中,所述第三设备、所述第四设备和所述至少一个另外的设备被布置在多边形的边处的平面中,所述第一设备在所述多边形内部,其中,所述第一消息处理器(112)被布置为:

使用在至少两个空间群集上的三角不等式的组合来执行所述验证测试,每个群集包括所述第一设备和所述协作设备的集合中的两个设备以及所述第二设备。

12.一种用于经由第一设备(110)和第二设备(120)之间的无线通信进行距离测量的方法,

所述无线通信包括用于基于测量消息到达所述第一设备的到达时间来确定所述第一设备与所述第二设备之间的距离(140)的测距协议,所述协议包括由所述第二设备发送所述测量消息;

所述方法包括:

基于所述测量消息到达所述第一设备的第一到达时间来获得所述第一设备与所述第二设备之间的第一距离,

与第三设备(130)通信,充当协作设备的所述第三设备位于距所述第一设备的受信距离处,

所述第三设备被布置用于:

确定所述测量消息到达所述第三设备的第三到达时间,并且

提供支持数据,所述支持数据基于所述第三到达时间;

为了评价所确定的距离,所述方法包括,

使用所述支持数据获得所述第三设备与所述第二设备之间的第三距离,

对所述第一距离、所述受信距离和所述第三距离执行验证测试,当所述的距离对应于所述第一设备、所述第二设备和所述协作设备的可行空间群集时,所述验证测试将所述第一距离接受为可靠的。

13.根据权利要求12所述的方法,其中,所述方法包括:

指示所述第一设备充当发起设备以提供所述第一到达时间或所述第一距离,或

指示所述第三设备充当所述协作设备以提供基于所述第三到达时间的所述支持数据。

14.一种用于在经由第一设备(110)和第二设备(120)之间的无线通信进行距离测量中充当协作设备的方法,

所述协作设备位于相距所述第一设备的受信距离处,

所述无线通信包括用于基于测量消息到达所述第一设备的到达时间来确定所述第一设备与所述第二设备之间的距离的测距协议,所述协议包括由所述第二设备发送所述测量消息;

所述第一设备被布置用于:

基于所述测量消息到达所述第一设备的第一到达时间来获得所述第一设备与所述第

二设备之间的第一距离，

所述方法包括：

确定所述测量消息到达所述协作设备的第三到达时间，并且

提供支持数据，所述支持数据基于所述第三到达时间；

为了评价所确定的距离，所述第一设备被布置用于

使用所述支持数据获得所述协作设备与所述第二设备之间的第三距离，并且

对所述第一距离、所述受信距离和所述第三距离执行验证测试，当所述的距离对应于所述第一设备、所述第二设备和所述协作设备的可行空间群集时，所述验证测试将所述第一距离接受为可靠的。

15.一种可从网络下载和/或存储在计算机可读介质和/或微处理器可执行介质上的计算机程序产品，所述产品包括程序代码指令，所述程序代码指令当在计算机上运行时用于实施根据权利要求12至14中的任一项所述的方法。

用于受信距离测量的系统

技术领域

[0001] 本发明涉及一种用于经由无线通信进行距离测量的设备,所述无线通信是用于无线通信的充当第一设备的所述设备与第二设备之间的无线通信,所述无线通信包括用于基于测量消息到达第一设备的到达时间来确定第一设备与第二设备之间的距离的测距协议,所述协议包括由第二设备发送测量消息。本发明还涉及一种用于距离测量的方法和在设备或服务器中使用的计算机程序产品。

[0002] 本发明总体上涉及定位系统的领域,并且更具体地提供了用于验证距离测量的各种设备和方法以及相应的计算机程序产品。

背景技术

[0003] 在室内区域中可能存在对位置感知服务的需求。例如,在大型室内综合体中,诸如在医院、大学、停车场、购物中心和/或办公室中,可以向近距离的移动设备提供无线服务。室内定位系统可以向消费者(下文中称为终端用户)提供服务;即终端用户最终将依赖的服务。可以仅向服务提供设备附近、即在距服务提供设备有限距离处的设备提供这样的基于位置的服务。在另一示例中,电子无线车门钥匙必须靠近汽车才能够打开车门。欺骗的门钥匙可能篡改距离测量协议,使得当其离汽车远超过其应该的距离时,其可以打开门。

[0004] 因此,重要的是距离测量是可靠的。在此背景下,可靠意味着响应设备提供所测量的可靠和正确的距离或到达数据,而不是为了故意引起与到响应设备的实际距离不同的距离而已经被篡改或已经被伪造的距离或到达时间数据。

[0005] 在IEEE 802.11中所定义的针对无线通信的协议的版本中新近开发了用于距离测量的已知系统,参见参考文献[802.11]。该版本包括用于确定两个设备之间的距离的测距协议,并且允许进行准确的距离测量以及确定高达1米或甚至更低分辨率的设备定位。称为精细定时测量流程(FTM)的测距协议被定义在[802.11]章节10.24.6中,并且准确地对测量消息的到达时间进行测量以确定信号的往返时间(RTT),并且基于测量的消息的到达时间结合发送定时导出距离。例如,假设无线信号在自由空气中以基本上光速传播,则辐射花费3.3ns来覆盖一米的距离,而Wi-Fi站可以能够达到大约0.1ns的时间粒度。

[0006] 注意,这种应用是在测距协议的领域中。这些对应于称为飞行时间测量的技术,其测量电磁辐射在发射器与接收器之间行进所花费的时间。其与在IP/HTTP协议中执行的距离测量、又名声脉冲(ping)时间显著不同,声脉冲时间测量IP数据包在网络中从源设备过渡到接收设备所花费的时间,其中,这样的过渡可以包括若干中间设备。

[0007] 为了两个设备基于到达时间测量来确定彼此之间的距离,它们需要根据测距协议进行操作。例如,发起无线设备可以发起开始往返时间测量的请求。响应设备可以确定发送消息和接收请求之间的间隔,并将时间间隔发送给发起设备。

[0008] 然而,通过发送虚假数据,设备实际上可以声称它比在现实中更靠近或更远离。而且,测量消息可能必须在预定时间处(例如,根据定时网格)发送。恶意设备可以在不同的时间处故意发送测量消息。如果发起设备相信所确定的距离/位置信息是准确的,则这种恶意

行为可能导致基于位置的服务的可能滥用。例如,基于位置的服务可以自动开始一些交易。

[0009] 因此,在已知系统中,测量或接收到的距离数据可能被篡改,并且因此不能被完全信任。

发明内容

[0010] 使用802.11的时间测量(TM)或精细时间测量(FTM)方法来测量到第二设备的距离的第一设备可以尝试保护其自身免受恶意设备的假到达时间(TOA)和假离开时间(TOD)的影响,恶意设备这样做以想要出现在不同的、尤其是比它们实际上更小的距离处。

[0011] 为了对抗这样的行为,距离测量系统可以包含第三设备,所述第三设备也执行距离测量以确定第三设备与第二潜在恶意设备之间的第二距离。通过比较两个距离并且知道并信任第一设备与协作设备之间的距离,可以对两个所确定的距离执行验证测试。然而,尽管恶意设备篡改两个距离测量使得它们通过验证测试可能是更复杂的,但是仍然是可能的。

[0012] 本发明的目的是提供一种用于使基于到达时间的距离测量更可信的系统。为此目的,提供了如权利要求中限定的设备和方法。

[0013] 根据本发明的第一方面,提供了一种用于经由无线通信进行距离测量的设备,所述无线通信是用于无线通信的充当第一设备的所述设备与第二设备之间的无线通信,所述无线通信包括用于基于测量消息到达所述第一设备的到达时间来确定所述第一设备与所述第二设备之间的距离的测距协议,所述协议包括由所述第二设备发送所述测量消息;

[0014] 所述设备包括:

[0015] 第一收发器,其用于消息的发送和接收,

[0016] 第一消息处理器,其被布置用于:

[0017] 根据所述测距协议处理所述消息,

[0018] 确定所述测量消息到达所述第一设备的第一到达时间,并且

[0019] 基于所述第一到达时间确定所述第一设备与所述第二设备之间的第一距离;

[0020] 其中,所述第一消息处理器被布置用于与第三设备通信,充当协作设备的所述第三设备位于相距所述第一设备的受信距离处,

[0021] 并且为了评价所确定的距离,所述设备被布置为

[0022] 从所述协作设备接收支持数据,所述支持数据基于所述第一消息到达所述协作设备的第三到达时间,

[0023] 使用所述支持数据获得所述第三设备与所述第二设备之间的第三距离,并且

[0024] 对所述第一距离、所述受信距离和所述第三距离执行验证测试,当所述距离对应于所述第一设备、所述第二设备和所述协作设备的可行空间群集时,所述验证测试将所述第一距离接受为可靠的。

[0025] 根据又一方面,提供了一种用于经由第一设备与第二设备之间的无线通信的距离测量的方法,所述方法包括:

[0026] 基于所述测量消息到达所述第一设备的第一到达时间来获得所述第一设备与所述第二设备之间的第一距离,

[0027] 与第三设备通信,充当协作设备的所述第三设备位于距所述第一设备的受信距离

处，

[0028] 所述第三设备被布置用于：

[0029] 确定所述测量消息到达所述第三设备的第三到达时间，并且

[0030] 提供支持数据，所述支持数据基于所述第三到达时间；

[0031] 为了评价所确定的距离，所述方法包括，

[0032] 使用所述支持数据获得所述第三设备与所述第二设备之间的第三距离，

[0033] 对所述第一距离、所述受信距离和所述第三距离执行验证测试，当所述距离对应于所述第一设备、所述第二设备和所述协作设备的可行空间群集时，所述验证测试将所述第一距离接受为可靠的。

[0034] 根据又一方面，提供了一种用于在经由第一设备与第二设备之间的无线通信的距离测量中充当协作设备的方法，所述协作设备位于相距所述第一设备的受信距离处。所述无线通信包括用于基于测量消息到达所述第一设备的到达时间来确定所述第一设备与所述第二设备之间的距离的测距协议，所述协议包括由所述第二设备发送所述测量消息。所述第一设备被布置用于基于所述测量消息到达所述第一设备的第一到达时间来获得所述第一设备与所述第二设备之间的第一距离。所述方法包括：

[0035] 确定所述测量消息到达所述协作设备处的第三到达时间，并且

[0036] 提供支持数据，所述支持数据基于所述第三到达时间。为了评价所确定的距离，所述第一设备被布置用于使用所述支持数据获得所述协作设备与所述第二设备之间的第三距离，并且对所述第一距离、所述受信距离和所述第三距离执行验证测试，当所述距离对应于所述第一设备、所述第二设备和所述协作设备的可行空间群集时，所述验证测试将所述第一距离接受为可靠的。

[0037] 上述特征具有以下效果：当第二设备参与测距协议时，第一设备可以基于由第二设备发送的测量消息的第一到达时间根据测距协议来确定距离。另外，第三设备确定相同测量消息到达第三设备的第三到达时间。第三设备位于相距第一设备的距离处，该距离对于第一设备是已知的并且被信任是可靠的。这样的距离在本文件中称为受信距离。受信距离可以是预定的，或可以单独测量，或可以由用户输入。这样的第三设备在本文件中可以称为协作设备。

[0038] 注意，充当协作设备的第三设备不使用一些另外的测量消息根据测距协议执行另外的距离测量。替代地，第三设备协作确定所述相同测量消息到达第三设备的第三到达时间，并且将支持数据传送到第一设备，支持数据基于第三到达时间。例如，支持数据可以包括相对于参考时钟或定时网格或相对于接收也由第一设备接收的一些其他消息的第三到达时间数据。备选地或附加地，支持数据可以包括第三距离数据，第三设备能够通过使用另外接收的消息和受信距离来确定第三设备与第二设备之间的第三距离。

[0039] 在接收到支持数据时，使得处理器能够使用支持数据来获得第三设备与第二设备之间的第三距离。随后，对第一距离、受信距离和第三距离执行验证测试。有利地，当所述距离对应于第一设备、第二设备和协作设备的可行空间群集时，验证测试可以将第一距离接受为可靠的。

[0040] 在实施例中，所述验证测试包括对所述可行空间群集的余弦规则检查或三角不等式检查。有利地，检查证明三角形的空间群集是否可以具有相应的边长。

[0041] 在实施例中,所述测距协议包括交换基于密钥数据加密保护的消息,并且所述第一消息处理器被布置为与所述协作设备共享所述密钥数据,以使得所述第三消息处理器能够根据所述测距协议加密处理所述消息。有利地,在第一设备与第三设备之间的加密消息保护了这些消息被潜在恶意的第二设备篡改。

[0042] 在实施例中,所述第一消息处理器被布置为根据所述测距协议来确定所述受信距离。有利地,在对第二设备的实际测量之前,使用相同的测距协议来确定受信距离。

[0043] 在实施例中,所述设备包括时钟单元以提供用于确定所述到达时间的时间参考,并且所述第一消息处理器被布置为使所述时间参考与所述协作设备中的对应时钟单元同步。有利地,在第一设备与第三设备之间共享时间参考。可以相对于时间参考来确定第三到达时间,这使得支持数据能够包括如此确定的第三到达时间,并且可由第一设备如此使用。

[0044] 在实施例中,所述测距协议包括充当发起设备的所述第一设备向所述第二设备发送发起消息,同时在接收到所述发起消息时,所述第二设备必须发送所述测量消息。所述第一消息处理器被布置为与所述第三设备交换角色改变数据,以使得所述第三设备能够充当用于距离测量的发起设备。所述第三设备被布置为在接收到所述角色改变数据时:

[0045] 基于第二测量消息根据所述测距协议获得所述第三设备与所述第二设备之间的第三距离,并且

[0046] 将第三支持数据传送到所述第一设备,所述第三支持数据指示所述第三距离。所述第一消息处理器被布置为:

[0047] 当在所述第一设备处接收到所述第二测量消息时,确定所述第一设备与所述第二设备之间的第二距离,

[0048] 从所述第三设备接收所述第三支持数据,并且

[0049] 还使用所述第二距离和所述第三支持数据来执行所述验证测试。有利地,通过确定所述第二距离并组合地验证两个距离,第二设备更难以一致地篡改两个距离测量。

[0050] 在实施例中,所述第三消息处理器被布置为确定从所述第二设备接收的至少一个消息的第三信号强度,并且将第三信号强度数据包括在到所述第一设备的所述支持数据中。所述第一消息处理器被布置为确定从所述第二设备接收的至少一个消息的第一信号强度,并且通过将所述第一信号强度和所述第三信号强度与所确定的距离处的相应预期信号强度进行比较来验证所确定的距离是否可靠。可选地,第一设备和第三设备两者都可以测量来自第二设备的相同消息的信号强度。有利地,添加了实现所确定的距离的验证的另外的独立机制。

[0051] 在实施例中,在评价所确定的距离不可靠时,所述第一消息处理器被布置为要求利用所述第二设备执行不同的安全协议。有利地,备选地或另外地,在评价所确定的距离不可靠时,所述第一消息处理器被布置为使用不同的测距协议和/或不同类型的无线通信来请求进一步的距离测量。备选地或另外地,在评价所确定的距离不可靠时,所述第一消息处理器被布置为拒绝或限制对所述第一设备中的至少一些数据和/或至少一个功能的访问。有利地,防止了对第一设备中的任何功能或数据的恶意访问或使用。

[0052] 根据本发明的又一方面,一种用于可靠距离测量的系统包括如上面描述的设备和第三设备、以及充当第二协作设备的第四设备,所述第四设备位于相距第一设备的第二受信距离处并且位于相距第三设备的第三受信距离处。所述第四设备包括第四无线接收器、

第四消息处理器,所述第四无线接收器用于消息的接收,所述第四消息处理器被布置用于确定所述测量消息到达所述第四设备的第四到达时间,并且将第四支持数据传送到所述第一设备,所述第四支持数据基于所述第四到达时间。所述第一消息处理器被布置用于从所述第二协作设备接收所述第四支持数据,使用所述第四支持数据获得所述第四设备与所述第二设备之间的第四距离,并且还使用所述第二受信距离和所述第四距离来执行所述验证测试。有利地,通过确定所述另外的距离并组合地验证所有距离,第二设备更难以一致地操纵所述距离。

[0053] 可选地,验证测试可以使用在至少两个空间群集上的三角不等式的组合,每个群集包括第二设备以及第一设备和协作设备的集合中的两个设备。可选地,所述第一消息处理器可以被布置为验证所述第二设备根据所述第一空间群集的第一位置是否对应于所述第二设备根据所述第二空间群集的第二位置。

[0054] 可选地,所述第一消息处理器可以被布置为使用不一致性检查来执行验证测试以便检测是否所有确定的距离都大于零。

[0055] 可选地,所述第一消息处理器可以被布置为基于以下设置来执行验证测试,其中,所述第三设备和所述第四设备被布置为使得从第三设备到第一设备的线与从第四设备到第一设备的线之间的受信角为至少90度。

[0056] 可选地,所述第一消息处理器可以被布置为基于以下设置来执行所述验证测试,其中,所述第三设备和所述第四设备相对于所述第一设备彼此相对布置。

[0057] 可选地,所述第一消息处理器可以被布置为基于以下设置来执行所述验证测试,其中,所述第二受信距离对应于所述受信距离。

[0058] 在实施例中,所述系统包括充当另外的协作设备的至少一个另外的设备,其中,所述第三设备、所述第四设备和所述至少一个另外的设备被布置在多边形的边处的平面中,所述第一设备在所述多边形内部,其中,所述第一消息处理器被布置为:

[0059] 使用在至少两个空间群集上的三角不等式的组合来执行验证测试,每个群集包括第二设备以及第一设备和协作设备的集合中的两个设备。有利地,通过确定所述另一距离并组合地验证所有距离,第二设备更难以一致地操纵所述距离。

[0060] 在实施例中,所述方法包括指示所述第一设备充当发起设备以提供所述第一到达时间或所述第一距离。备选地或另外地,所述方法包括指示所述第三设备充当所述协作设备以提供基于所述第三到达时间的所述支持数据。有效地,现在通过所述指示来执行距离测量的控制。

[0061] 注意,在上文中,出于清楚的原因,已经将其描述为执行距离测量和距离可靠性验证的第一设备。然而,第一设备、第三设备和/或另外的协作设备向执行距离测量和距离可靠性验证的控制设备提供所有所需的信息也是可能的。

[0062] 根据本发明的方法可以作为计算机实施的方法被实施在计算机上,或被实施在专用硬件或这两者的组合中。用于根据本发明的方法的可运行代码可以被存储在计算机程序产品上。所述计算机程序产品的范例包括诸如存储棒的存储设备、诸如光盘的光存储设备、集成电路、服务器、在线软件等。所述计算机程序产品可以包括被存储在计算机可读介质上的非瞬态程序代码模块,当所述程序产品在所述计算机上被运行时,所述非瞬态程序代码模块用于执行根据本发明的方法。在实施例中,所述计算机程序包括计算机程序代码模块,

当所述计算机程序在计算机上被运行时,所述计算机程序代码模块适于执行根据本发明的方法的所有步骤或阶段。优选地,所述计算机程序被包含在计算机可读介质上。提供了一种能从网络下载和/或存储在计算机可读介质和/或微处理器可执行介质上的计算机程序产品,所述产品包括在计算机上被运行时用于实施上述方法的程序代码指令。

[0063] 本发明的另一方面提供了一种使计算机程序能用于下载的方法,例如,被包括在基于位置的应用中。当将计算机程序上载到例如Apple的App Store、Google的Play Store或Microsoft的Windows Store时,并且在该计算机程序能从这样的商店下载时,使用该方面。

[0064] 在权利要求中给出了设备和方法的其他优选实施例,在此通过引用将其公开并入本文。

附图说明

[0065] 根据下文的描述并参考附图通过举例方式而描述的实施例,本发明的这些和其他方面将显而易见并参考其得以进一步阐释,在附图中:

[0066] 图1示出了用于无线通信和距离测量的设备,

[0067] 图2示出了用于无线通信的设备和协作设备的空间群集

[0068] 图3示出了用于无线通信的两个设备的空间群集,

[0069] 图4示出了用于无线通信的两个设备的又一空间群集,

[0070] 图5示出了具有两个协作设备的空间群集,

[0071] 图6示出了具有两个协作设备的第二空间群集,

[0072] 图7示出了具有两个协作设备的又一空间群集,

[0073] 图8示出了用于距离测量的方法,

[0074] 图9示出了用于在距离测量中充当协作设备的方法,

[0075] 图10a示出了计算机可读介质,并且

[0076] 图10b示出了处理器系统的示意性表示。

[0077] 附图仅仅是图解性的而并未按比例绘制。在附图中,对应于已描述元件的元件可以具有相同的附图标记。

具体实施方式

[0078] 如下所述的使用无线通信的距离测量方法和设备至少提供基本功能,即提供关于移动设备到另一设备(例如,在固定位置上)之间的当前距离的信息。现在将各种协议描述为使用测量消息的到达时间的合适测距协议的示例,其可以使用此后描述的实施例来增强。

[0079] 距离测量的第一示例在[802.11]中描述。条款11.24.6规定了精细定时测量(FTM)过程。FTM机制旨在测量两个设备中的时钟之间的绝对时间差,使得一个设备也可以补偿RF波以光速从一个设备行进到另一个设备所花费的时间。在FTM过程中,设备中的一个以另一个设备可以测量两者之间的往返时间(RTT)的方式将其时钟的时间戳发送到另一个设备(稍后解释)。通过使用[802.11]的条款11.24.6中规定的精细定时测量(FTM)过程测量往返时间(RTT)、将RTT乘以光速并除以2来完成使用802.11(Wi-Fi)的两个设备之间的距离测

量。

[0080] 以下是[802.11]中的FTM的解释,参见例如图11-35、11-36、11-37和周围的文本。下面的时间戳的编号来自图11-36。发起STA(站)想要知道RTT或到另一STA(响应STA)的距离。为了实现此,发起STA将初始FTM请求发送到响应STA。响应STA将FTM_1(0,0)消息发送到发起STA,并且测量确切发送时间。响应STA将该时间存储为t1_1。发起STA将FTM_1(0,0)消息的接收测量为t2_1。它将所得到的ACK的发送时间测量为t3_1。然而,发起STA尚不能使用值t2_1和t3_1。

[0081] 响应STA测量作为对FTM_1(0,0)的响应而接收的ACK的接收时间,并将此存储为t4_1。在一会儿(至少最小ΔFTM秒)之后,响应STA发送FTM_2(t1_1,t4_1)并且将发送时间记录为t1_2。该发起STA经历与上面描述的相同例程,即,将FTM_2的接收时间(t1_1,t4_1)测量为t2_2并且将ACK的发送时间测量为t3_2。然而,此时,发起STA能够根据来自[802.11]的以下等式(11-5)测量RTT。

[0082] RTT=[(t4_1-t1_1)-(t3_1-t2_1)] (1)

[0083] 重新排列上面的公式的右侧得到

[0084] RTT=(t2_1-t1_1)+(t4_1-t3_1) (2)

[0085] 从其中可以容易地看出,(t2_1-t1_1)是在传送FTM帧时FTM帧在RF介质上从请求STA行进到发起STA的时间,并且(t4_1-t3_1)是ACK帧在RF介质上从发起STA行进到响应STA的时间,使得其和确实是往返时间。

[0086] 为了提高准确度,可以重复上述操作,并且可以将RTT计算为所有测量的平均值。

[0087] t1_X是离开时间(TOD)。TOD在[802.11]中被定义为“TOD[...]表示相对于时间基准的时间,在该时间处,最后发射的精细定时测量帧的前导码的开始出现在发射天线连接器处”。前导码是PHY帧的第一部分,这尤其意味着发射器刚好在前导码之前不发送任何RF能量。因此,发起STA必须以相同方式测量t3_X,即,t3_X表示相对于时间基准的时间,在所述时间处,作为对所接收的精细定时测量帧的响应的最后发送的ACK帧的前导码的开始出现在发射天线连接器处。

[0088] t4_x是到达时间。TOA在[802.11]中被定义为“TOA[...]表示相对于时间基准的时间,在该时间处到最后发送的精细定时测量帧的Ack帧的前导码的开始到达接收天线连接器”。因此,发起STA必须以相同方式测量t2_X,即t2_X表示相对于时间基准的时间,在所述时间处最后接收到的精细定时测量帧的前导码的开始到达接收天线连接器。

[0089] 因此,最小时间t3-t2等于接收到的FTM(,)帧+SIFS的长度,并且最大时间t3-t2等于接收到的FTM(,)帧+DIFS的长度。FTM(,)帧的长度可以变化。在本文件其余部分中,我们使用以下定义:

[0090] 使用Lftm来表示导致发起STA测量t2和t3的物理FTM帧的时间长度;

[0091] 使用术语反应时间或发起STA的反应时间和符号R作为发起STA从刚好在物理FTM帧的最后一个符号(即,CRC检查的最后一个符号)到达其接收天线连接器之后到其响应于FTM帧而发送的ACK帧的TOD所花费的时间。由于发送ACK帧是相当简单的动作,因此它可能在硬件中完成,并且因此可以是恒定的。

[0092] [802.11]的条款11.24.5规定了定时测量(TM)过程。与FTM过程存在一些差异,最值得注意的是时间戳的更好分辨率,这原则上允许更精确的距离测量。下面的实施例可以

以与这里针对FTM描述的相同的方式用于TM。

[0093] 在US8762727B2中描述了类似于FTM的距离测量系统的又一示例。不同之处在于发起者STA称为源节点,响应者STA称为目标节点,并且源节点测量t1和t4,而目标节点测量t2和t3,并将这些发送到源节点。

[0094] 在3GPP中描述了距离测量系统的又一示例,称为OTDOA(观察到达时间差),参见[OTDOA],其是rel9 E-UTRA(LTE无线电)中引入的定位特征,参见如下所述的参考文献[36.nnn]。它是一种多点定位方法,其中,用户设备(UE)测量来自若干eNodeB(比如说基站)的一些特定信号(定位参考信号-PRS)之间的时间差,并将这些时间差报告给网络中的特定设备,位置服务器(演进服务移动位置中心-E-SMLC)。基于这些时间差和eNodeB位置的知识,E-SMLC计算UE的位置。LPP(LTE定位协议)的描述可以在[36.355]规范中找到。PRS信号的确切细节可以在[36.211]的第6.10.4节中找到,并且简单的OTDOA过程可以在[37.571-1]规范的第9节中的RAN5 OTDOA测试案例的描述中找到。正如Wi-Fi中的对于定位的测量一样,移动设备可以伪造这些OTDOA报告以在其想要的任何地方出现于网络。下面的这些实施例可以用于防止这种类型的欺骗。用于由UE在OTDOA中进行的相同测量的另一术语是RSTD(参考信号时间差)。RSTD测量准确度要求在[36.133]中规定。

[0095] 3GPP中的距离测量的又一示例是基于参考时间网格的消息的到达时间,并且称为基于增强单元ID或E-CID。基于单元ID的方法在rel9之前已经是可能的。增强单元ID将一些已经可用的测量聚合在一起,它们中的一些具有增加的准确度要求以改善定位准确度能力。增强单元ID、E-Cell ID或E-CID是rel9 E-UTRA(LTE无线电)中引入的定位特征。UE向网络(通过服务单元或eNodeB向位置服务器、演进服务移动位置中心-E-SMLC)报告服务单元ID、与服务单元的定时提前(其发送和接收时间之间的差)、参考(窄带)信号接收功率(RSRP/NRSRP)、(窄带)参考信号接收质量(RSRQ/RSRQ)。可以从任何相邻单元测量和报告RSRP/NRSRP和RSRQ/RSRQ,而仅针对主单元(服务单元)测量定时提前。服务单元或eNodeB可以向ESMLC报告额外的信息,如到达角度。ESMLC基于该信息及其对单元位置的了解来估计UE位置。

[0096] 测量定时提前如下。在LTE或GSM中,单元发送具有固定定时的发送或接收机会的频率-时间网格。对于LTE,个体频率是OFDM子载波的频率,并且通常间隔15kHz。时域由10ms的连续帧组成,其中,每个帧由十个子帧组成,并且每个子帧由两个0.5ms的时隙组成。该频率-时间网格由单元以非常严格的定时维持。按照网格元素,单元可以向范围内的所有移动设备(广播)或一个特定设备进行发送。在一些网格元素(频率、子帧组合或有时频率-时隙组合)中,单元将总是发送,如3GPP规范中所定义的。因此,这些网格元素理想地适合于向单元中的移动设备发送系统信息,诸如可以灵活使用的每个网格元素的目的。在其他网格元素中的每一个中,因此可以更灵活地使用元素,单元可以向范围内的所有移动设备广播,它可以向特定移动设备发送,或它可以已经给予特定移动设备发送到单元或单元中的另一移动设备的许可。

[0097] 因为RF波从单元行进到移动设备花费时间(大约每微秒300米),所以网格将看起来被延迟到达移动设备达该行进时间。假设该行进时间为t秒。当移动设备恰好从允许发送的子帧的开始而开始发送时,它比单元处的子帧的开始晚t秒开始发送。由移动设备发送的信号到达单元再次花费t秒。因此,单元接收来自移动设备的不是恰好在分配给它的子帧的

开始处开始而是在2t秒之后开始的发送。通过测量该延迟,单元可以确定到移动设备的距离。

[0098] 如果移动设备远离单元,则其在子帧中的发送的结束可能比下一个子帧的开始更晚地到达,因此引起干扰。为了克服这个问题,单元可以要求移动设备使用一定量的定时提前,其编码在寻址到特定移动设备的定时提前命令中的所谓TA值中。然后,移动设备比由移动设备确定的子帧的开始更早地开始其发送TA。可能用于定时提前的最大值是0.67ms,对应于略微大于100km的移动设备到单元的距离。技术规范3GPP TS36.321[36.321]第6.1.3.5节“Timing Advance Command MAC Control Element”描述了用于LTE的TA值调整过程。

[0099] 想要出现在不同距离处的移动设备可以在想要看起来更靠近单元时比频率-时间网格和它从单元接收的TA值所假设的更早地开始其发送,或在想要看起来比现实中更远离单元时比它所假设的更晚地开始发送。

[0100] 准确且正确的距离测量在若干应用中是重要的。例如当Wi-Fi FTM用于通过Wi-Fi测量从汽车到钥匙扣的距离因此汽车可以决定在测量的距离小于比如说5米时打开其门时,重要的是到钥匙扣的实际距离确实小于5米。另一示例可以是,如果另一设备不比某个距离更远,则仅允许该设备将版权内容流式传输到该另一设备。当建立安全认证信道时,还可以使用准确且正确的距离测量来防止中间人攻击。这将在后续的段落中解释。

[0101] 当两个设备需要保护它们的有线或无线通信时,它们可以加密它们的通信。然而,这要求两个无线设备都知道相同的密钥。Diffie-Hellman[DH]是用于在两方之间建立秘密密钥的众所周知的技术,其中,用于建立秘密密钥的各方之间的通信不向第三方揭示关于所建立的秘密密钥的任何信息。双方均使用其自己的公钥/私钥对并彼此交换公钥。每一方能够使用其自己的私钥和另一方的公钥以及可能的一些其他信息,例如,来自每一方的新鲜值(随机数)来计算秘密密钥。每一方可以在每次执行Diffie-Hellman时重新生成密钥对,或重新使用较旧的密钥对。

[0102] 当通过网络执行Diffie-Hellman时,接收用于执行Diffie-Hellman的公钥的设备不知道该公钥来自哪个设备。这可以被攻击者在所谓的中间人攻击中利用。攻击者E可能伪装成设备A想要连接的真实设备B。攻击者E与设备A执行Diffie-Hellman并与设备A建立秘密密钥Kae。类似地,攻击者对设备B伪装成设备A并与设备B建立秘密密钥Kbe。当消息从设备A或B中的一个进入时,攻击者用一个秘密密钥解密该消息,用另一个秘密密钥加密该消息并将其转发到另一个设备。这样,除了一些额外的延迟之外,设备A和B在它们的通信中不会注意到任何奇怪的事情。当他们通过使用另一种通信方式发送相同的信息并比较结果来检查他们的通信时,他们不会注意到对他们的通信的任何篡改。但是攻击者完全了解他们通信了什么。

[0103] 在设备供应协议[DPP]中,第一步骤是执行DPP引导,即,获得对另一设备的公共引导密钥的信任的过程,并且该公共引导密钥不是中间人设备的公钥。引导方法之一是扫描包含由另一设备显示或打印在另一设备上的另一设备的公共引导密钥的QR码。另一设备还可以扫描第一设备的QR码(相互认证)。在此之后,在DPP认证协议中使用(一个或多个)引导密钥,其中,检查另一设备是否也拥有属于公共引导密钥的私钥。如果DPP中的公共引导密钥将已经通过Wi-Fi(任何形式的Wi-Fi,例如邻居感知联网[NAN])交换,它们不能被信任,

因为它们可能已经由RF范围内的任何设备发送。继续DPP,DPP认证协议将导致公共共享密钥Ke的建立,但是设备不知道它们是与预期设备还是与中间人设备共享该密钥。类似地,当使用机会无线加密[OWE]时,通过Wi-Fi交换公钥,并且通过使用Diffie-Hellman,建立公共共享密钥用于两个设备之间的后续通信的加密。

[0104] 然而,限制与中间人设备建立公共共享密钥的概率的方式是设备测量到另一设备的距离,并且如果它小于由设备中的规则或由其用户确定的某个距离(例如几米),则它们信任从另一设备接收的公共密钥。在这种情况下,用户将知道通过Wi-Fi发送公钥的设备,因此预期的设备或中间人设备小于距离限制。然后,用户可以判断在该范围内是否存在除预期设备之外的任何其他设备。

[0105] 使用距离测量限制与中间人设备建立公共共享密钥的概率可以通过首先通过Wi-Fi交换公钥并且然后计算共享会话密钥来完成,例如,通过OWE或通过DPP的DPP认证协议部分(其中,DPP引导通过Wi-Fi,例如,Wi-Fi感知,完成),并且通过随后使用加密的FTM_X帧(加密的FTM_X帧使用通过机会无线加密[OWE]或DPP或一些其他方法确定的共享会话密钥)执行FTM过程,或通过至少加密FTM_X帧中包含t1和t4值的字段。如果如此测量的到请求STA的距离小于x米,则发起STA可以信任所接收的公钥,并且可以继续使用商定的会话密钥与另一设备进一步通信。在DPP的情况下,进一步的通信将是DPP配置协议。在OWE的情况下,它将是AP和STA之间的加密WAN连接。发起STA还可以向用户询问用户是否确信在所测量的到响应STA的距离内仅存在一个Wi-Fi设备,并且如果用户确认此,则发起STA继续使用共享会话密钥。

[0106] 如上面解释的,响应STA可具有使发起STA相信其处于与其实际距离不同的另一距离的原因。特别地,响应STA可以通过减小t4_X值及/或增大t1_x值而使发起STA相信其比其实际上更靠近。这从[802.11]的等式(11-5)中是显而易见的

[0107] RTT＝[(t4_X-t1_X)-(t3_X-t2_X)] (3)

[0108] 两个设备之间的距离为

[0109] d＝c*RTT/2 (4)

[0110] 其中,c是光速(约3*10^8m/s)。

[0111] 为了将由发起STA测量的距离减小1米,响应STA必须将t4_Z与t1_X的差从其测量值减小约

[0112] delta_t＝2*1m/3*10^8m/s＝2*3.33*10^-9s＝6.66ns (5)

[0113] 然而,响应STA在将它们报告给发起STA时必须小心不要将t4_X与t1_X的差从其测量值减小太多,这是因为发起STA然后将测量负RTT。当所报告的t4_Z与t1_X的差等于发起STA的反应时间(即,t3_X与t2_X之间的差)时,发起STA将测量到0的往返时间。因此,对于成功欺骗重要的是,响应STA知道发起STA的t3_X和t2_X的差。

[0114] 如上面解释的,发起STA的t3_X与t2_X的差由两个部分组成,所发送的FTM PHY帧的长度(Lftm)和反应时间R。响应STA已发送FTM帧自身,因此知道其时间长度Lftm。反应时间R可以以各种方式为响应STA所知。我们假设欺骗设备以某种方式知道到发起STA的真实距离,并且因此可以通过调适所报告的t1及t4而精确地伪造发起STA将测量的距离。因此,使用如上面描述的FTM进行测量的问题是恶意响应STA可以操纵其所报告的到达时间t1和t4,使得其可以看起来比其实际上更靠近或更远离发起STA。

[0115] 为了防止成功地伪造距离,发起设备可以包含相对于发起设备处于已知位置的一个或多个协作设备。协作设备可以采用与发起设备中的时钟同步的时钟,或可以共享一些其他时间参考。(一个或多个)协作设备独立地测量测量消息的(一个或多个)到达时间,并将这些报告给发起设备。发起设备使用来自三角形的性质来尝试和检测由欺骗响应设备操纵的到达时间测量。对于基于3GPP的系统,发起设备和一个或多个协作设备可以由基站实现,并且响应设备由用户设备UE实现。

[0116] 通过使基于距离的测量更值得信任,其成为针对基于可靠接近度的服务的可行工具。一些范例使用情况包括:

[0117] 如果你连接到附近的无线键盘、附近的无线存储设备、附近的传感器或附近的无线网络摄像头,则你希望确认你连接到正确一个,而不是连接到想要监视、复制或跟踪你正在做什么的中间人设备。

[0118] 如果你遇到你的朋友并且希望连接到你朋友的手机以交换一些照片,则你希望确认你连接到你朋友的手机而不是中间人。

[0119] 如果在房间或商店中,你希望在一些设备上自动地切换,打开某扇门或允许某人在非常接近时以其移动设备连接到某项服务,那么你希望确认该移动设备的位置是正确的而不是宣称接近的伪装设备。

[0120] 如果在商店中你希望发起交易,例如,当接近收银台时,那么你希望确认你并未受到“网络钓鱼”攻击,由此用户可能未意识到并连接到更远的网络钓鱼设备而不是由商店所提供的官方服务。

[0121] 图1示出了用于无线通信和距离测量的设备。用于无线通信的设备的空间群集100包括第一设备110和第二设备120,所述设备以距离151在物理上分开。第一设备具有用于发送和接收消息的第一收发器111和第一消息处理器112。第二设备具有无线接收器121、或第二收发器和第二消息处理器122。而且,第三设备具有第三收发器131和第三消息处理器132。设备被配备用于无线通信,如通过连接到收发器111、121、131的天线113、123、133示意性地指示的。

[0122] 设备被布置用于根据第一设备和第二设备之间的测距协议经由无线通信进行距离测量,以便确定第一设备和第二设备之间的距离,如下面进一步详细描述的。无线通信包括用于基于测量消息到达所述第一设备的到达时间来确定第一和第二设备之间的距离的测距协议。该协议可以包括由第二设备发送测量消息。在示例中,无线通信和测距协议是根据[802.11]的,但是也可以使用其他无线协议,诸如蓝牙,其中,基于到达时间测量提供适当的测距协议。

[0123] 第一消息处理器112被布置用于根据测距协议处理消息并且确定测量消息到达第一设备的第一到达时间,并且基于第一到达时间确定第一设备与第二设备之间的第一距离151。另外,第一消息处理器被布置用于与第三设备130通信。第三设备充当协作设备,并且位于相距第一设备的受信距离150处。受信距离对于第一设备是已知的并且被信任是可靠的。受信距离可以是预定的,或可以单独测量或可以由用户输入。可选地,第一消息处理器被布置为根据利用第三设备执行的测距协议来确定受信距离。在对第二设备的实际测量之前,可以使用相同或另一测距协议来确定受信距离。

[0124] 在第三设备(也称为协作设备)中,第三消息处理器132被布置用于确定测量消息

到达第三设备的第三到达时间。值得注意地,第三设备通过确定所述相同测量消息到达第三设备的第三到达时间并且通过将支持数据传送到第一设备来与第一设备协作,所述支持数据基于第三到达时间。例如,支持数据可以包括相对于参考时钟或定时网格或相对于接收也由第一设备接收的一些其他消息的第三到达时间数据。备选地或另外地,支持数据可以包括第三距离数据。此外,第三设备可以能够例如通过使用进一步接收的消息和受信距离来确定第三设备与第二设备之间的第三距离。

[0125] 为了评价所确定的距离,第一消息处理器被布置为从协作设备接收支持数据,并且使用支持数据获得第三设备与第二设备之间的第三距离153。第一消息处理器被布置用于随后对第一距离151、受信距离150和第三距离153执行验证测试。当所述距离对应于第一设备、第二设备和协作设备的可行空间群集时,验证测试可以将第一距离接受为可靠的。例如,验证测试包括对可行空间常数的余弦规则检查或三角不等式检查,如下面进一步阐明的。检查旨在证明三角形的真实空间群集是否可以根据所确定的距离具有相应的边长。

[0126] 测距协议可以包括交换基于密钥数据加密保护的消息。可选地,第一消息处理器被布置为与协作设备共享密钥数据,以使得第三消息处理器能够根据测距协议加密地处理消息。根据本身已知的无线通信协议对第一和第三设备之间的消息进行加密保护了这些消息被潜在恶意的第二设备篡改。

[0127] 可选地,设备可以具有时钟单元,以提供用于确定所述到达时间的时间参考。第一消息处理器可以被布置为将时间参考与协作设备中的对应时钟单元同步,例如,与来自[802.1AS]的协议同步。有效地,可以在第一和第三设备之间共享时间参考。可以相对于时间参考来确定第三到达时间,这使得支持数据能够包括如此确定的第三到达时间,并且可由第一设备如此使用。

[0128] 在下文中,描述添加一或多个协作STA可以如何及在哪种程度上帮助检测到响应STA想要看起来比其实际上更靠近发起STA。以下假设可以应用:

[0129] 响应STA知道如何调整其向发起STA报告的测量以出现在距发起STA的任何距离处;

[0130] 发起STA和(一个或多个)协作STA可以具有它们的时钟,它们利用这些时钟对与802.1AS协议[802.1AS]同步的物理帧的到达和离开时间进行定时,或以其他方式通信使得发起STA知道(一个或多个)对应STA的哪些测量与其自己的哪些测量组合;

[0131] 发起STA和(一个或多个)协作STA共享(一个或多个)协作STA所需的信息,使得协作STA可以接收、识别且在必要时解密来自响应STA的FTM(,)消息,因此(一个或多个)协作STA可以测量来自响应STA的FTM(,)消息的到达时间并且将这些报告给发起STA,使得发起STA可将这些到达时间与其自己的对相同消息的测量组合;

[0132] FTM测量可以执行多于一次,并且所有STA的测量和报告的时间t1、t2、t3和t4可以在它们用于距离和位置计算之前首先被平均,使得测量准确性对于可靠结果是足够好的。

[0133] 下面描述了对于针对仅可以进行定时测量的STA的强攻击的良好防御。在这样的防御中,发起STA与一或多个协作STA一起工作,并且应用所示的三角不等式,并且在两个或更多个协作STA的情况下,在所计算位置中应用差异检查。使用[802.11]的FTM协议给出了详细示例。然而,它与使用Wi-Fi、蓝牙或任何其他无线(也是光学)技术的距离测量技术一起也很好地工作,其中,一个设备向另一个设备报告协议消息的到达时间、离开时间或其差

异。

[0134] 图2示出了用于无线通信的设备和协作设备的空间群集。群集200包括类似于参考图1描述的设备的称为发起STA的第一设备210、称为响应STA的第二设备220和称为协作STA的第三设备230。确定第一设备210和第二设备220之间的第一距离d1_c,第一设备210和第二设备220在真实距离d1(或d)处。确定第三设备230和第二设备220之间的第三距离d2_c。受信距离L在第一设备210和第三设备230之间,第一设备210和第三设备230在真实距离d2处。

[0135] 在示例中,从欺骗响应STA到发起STA的真实距离是d,其也是从欺骗响应STA到协作STA的距离。发起STA利用上面描述的方法中的任一者执行到欺骗响应STA的距离测量。在其余部分中,采用FTM协议。

[0136] 对于每个距离测量,发起STA询问协作STA其已测量什么作为欺骗响应STA已发送的FTM(t1_x,t4_X)物理帧的到达时间t2_X。附有_c的距离是由设备计算的对应距离。

[0137] 发起STA然后照常计算距离d:

[0138] RTT=[(t4_X-t1_X)-(t3_X-t2_X)] (6)

[0139] 两个设备之间的距离为

[0140] d1_c=c*RTT/2=c*[(t4_X-t1_X)-(t3_X-t2_X)]/2 (7)

[0141] 其中,c是光速(约3*10^8m/s)。如果已经完成并准确地报告了所有测量,则所计算的d1_c将对应于测量准确性内的真实距离d。

[0142] 假设欺骗响应STA想要发起STA认为其在假距离f而非d处。欺骗响应STA已经测量了t4_X和t1_X。为此目的,响应STA改变其报告的t4_r_X和t1_r_X的值,使得它们的差为小于实际测量的t4_X和t1_X的差的2*(d-f)/c。因此,欺骗响应STA向发起STA报告的时间为

(t4_r_X,t1_r_X)=(t4_X-(1-α)*(2*(d-f)/c,t1_X+α*(2*(d-f)/c)) (8)

[0143] 其中,α可以自由选择。

[0144] 使用如由响应STA报告的(t4_r_X,t1_r_x),发起STA可以将响应STA与其自身之间的距离d1_c计算为

[0145] d1_c=c*RTT/2

[0146] =c*[(t4_X-(1-α)*(2*(d-f)/c)-(t1_X+α*(2*(d-f)/c)))-(t3_X-t2_X)]/2

[0147] =c*[(t4_X-t1_X)-(t3_X-t2_X)-(2*(d-f)/c)]/2

[0148] =c*[(t4_X-t1_X)-(t3_X-t2_X)]/2-c*(2*(d-f)/c)/2

[0149] =d-(d-f)

[0150] =f (9)

[0151] 该计算的距离实际上是欺骗响应STA想要发起STA计算的距离。

[0152] 使用由响应STA报告的(t4_r_X,t1_r_x)和从协作STA获得的t2c_X,发起STA可以将响应STA与协作STA之间的距离d2_c计算为

[0153] d2_c=d1_c+c*(t2c_X-t2_X) (10)

[0154] 对于具有边A、B和C的任何三角形,以下不等式必须成立(三角不等式)

[0155] |C|≤|A|+|B| (11)

[0156] 因此,在图2的群集中,以下两个不等式对于真实距离以及对于由发起STA测量的距离必须为真

[0157] $$L \le d1 + d2 \quad \Leftrightarrow \qquad (12)$$

[0158] L≤2*d1+c*(t2c_X-t2_X) (13)

[0159] 发起STA可以检查上面两个不等式是否适用于测量的距离d1_c和d2_c。

[0160] $$L \le d1\_c + d2\_c \quad \Leftrightarrow \qquad (14)$$

[0161] $$L \le d1\_c + d1\_c + c * (\mathrm{t2c\_X} - \mathrm{t2\_X}) \quad \Leftrightarrow \qquad (15)$$

[0162] L≤2*f+c*(t2c_X-t2_X) (16)

[0163] 在图2的群集中,d1和d2相等,因此t2c_X和t2_X相等。这意味着如果欺骗响应STA如下选择f,则不等式(16)将不再成立:

[0164] f<L/2 (17)

[0165] 这意味着在图2的群集中,发起STA可以检测到响应STA伪造其测量,使得其想要看起来比L/2更靠近发起STA。

[0166] 图3示出了用于无线通信的两个设备的空间群集。群集300包括类似于参照图1描述的设备的称为发起STA的第一设备310、称为响应STA的第二设备320、以及称为协作STA的第三设备330。确定第一设备310和第二设备320之间的第一距离d1_c,第一设备310和第二设备320在真实距离d1(或d)处。确定第三设备330和第二设备320之间的第三距离d2_c,第三设备330和第二设备320在真实距离d2处。受信距离L在第一设备310和第三设备330之间。

[0167] 在示例中,发起STA将测量f作为到欺骗响应STA的距离的L,且将确定f-L作为协作STA与欺骗响应STA之间的距离。

[0168] 不等式(14)现在将是

[0169] $$L \le d1\_c + d2\_c \Leftrightarrow \qquad (18)$$

[0170] $$L \le 2 * f - L \quad \Leftrightarrow \qquad (19)$$

[0171] L≤f (20)

[0172] 只有f大于或等于L,这才成立。因此,所提出的防御确实适用于图3中的群集,并且发起STA可检测到响应STA伪造其测量,使得其希望看起来比L更靠近发起STA。

[0173] 图4示出了用于无线通信的两个设备的又一空间群集。群集400包含类似于参考图1描述的设备的称为发起STA的第一设备410、称为响应STA的第二设备420和称为协作STA的第三设备430。确定第一设备410和第二设备420之间的第一距离d1_c,第一设备410和第二设备420在真实距离d1(或d)处。确定第三设备430和第二设备420之间的第三距离d2_c,第三设备430和第二设备420在真实距离d2处。受信距离L在第一设备410和第三设备430之间。

[0174] 在该示例中,使用余弦规则。d2被计算为

[0175] $$d2^2 = d1^2 + L^2 - 2 * d1 * L * \cos(\varphi) \qquad (21)$$

[0176] 以以下方式使用α使d1和L相关

[0177] d1=α*L (22)

[0178] 我们得到

[0179] $$\begin{aligned} d2 &= \mathrm{sqrt}\left((\alpha * L)^2 + L^2 - 2 * \alpha * L * L * \cos(\varphi)\right) \\ &= L * \mathrm{sqrt}(\alpha^2 + 1 - 2 * \alpha * \cos(\varphi) \qquad (23) \end{aligned}$$

[0180] 然而,欺骗响应STA改变其向发起STA发送的信息,使得发起STA将变为的距离d1_c和d2_c

[0181] d1_c＝d1-(d1-f) (24)

[0182] d2_c＝d2-(d1-f) (25)

[0183] 发起STA检查不等式(14)对于其测量的距离是否成立

[0184] $$L \le d1\_c + d2\_c \Leftrightarrow \quad (26)$$

[0185] $$L \le f + L * \mathrm{sqrt}(\alpha^2 + 1 - 2 * \alpha * \cos(\varphi)) - \alpha * L + f \Leftrightarrow \quad (27)$$

[0186] $$L \le 2 * f + L * \{\mathrm{sqrt}(\alpha^2 + 1 - 2 * \alpha * \cos(\varphi)) - \alpha\} \Leftrightarrow \quad (28)$$

[0187] $$f \ge 0.5 * L * \{1 + \alpha - \mathrm{sqrt}(\alpha^2 + 1 - 2 * \alpha * \cos(\varphi))\} \quad (29)$$

[0188] 因此,当响应STA如在以下不等式中选择f时,发起STA将检测到伪造其所报告的测量的响应STA。

[0189] $$f / L < 0.5 * \{1 + \alpha - \mathrm{sqrt}(\alpha^2 + 1 - 2 * \alpha * \cos(\varphi))\} = T1 \quad (30)$$

[0190] 表1示出了针对α≥0并且$0 \le \varphi \le 90$度的组合的T1的值。

[0191]

α \ φ	0.0	10.0	20.0	30.0	40.0	50.0	60.0	70.0	80.0	90.0
0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
0.10	0.10	0.10	0.10	0.09	0.09	0.08	0.07	0.06	0.06	0.05
0.20	0.20	0.20	0.19	0.18	0.17	0.16	0.14	0.12	0.11	0.09
0.30	0.30	0.30	0.29	0.27	0.25	0.23	0.21	0.18	0.15	0.13
0.40	0.40	0.39	0.38	0.36	0.33	0.30	0.26	0.23	0.19	0.16
0.50	0.50	0.49	0.47	0.44	0.40	0.36	0.32	0.27	0.23	0.19

[0192]

0.51	0.51	0.50	0.48	0.45	0.41	0.37	0.32	0.28	0.23	0.19
0.55	0.55	0.54	0.52	0.48	0.44	0.39	0.34	0.29	0.25	0.20
0.60	0.60	0.59	0.56	0.52	0.47	0.42	0.36	0.31	0.26	0.22
0.70	0.70	0.68	0.64	0.59	0.53	0.47	0.41	0.35	0.29	0.24
0.80	0.80	0.77	0.72	0.65	0.58	0.51	0.44	0.38	0.32	0.26
0.90	0.90	0.85	0.78	0.70	0.62	0.55	0.47	0.40	0.34	0.28
1.00	1.00	0.91	0.83	0.74	0.66	0.58	0.50	0.43	0.36	0.29
1.10	1.00	0.95	0.86	0.77	0.69	0.60	0.52	0.45	0.37	0.31
1.20	1.00	0.96	0.89	0.80	0.71	0.63	0.54	0.46	0.39	0.32
1.30	1.00	0.97	0.90	0.82	0.73	0.65	0.56	0.48	0.40	0.33
1.40	1.00	0.97	0.91	0.83	0.75	0.66	0.58	0.49	0.41	0.34
1.50	1.00	0.98	0.92	0.85	0.76	0.68	0.59	0.50	0.42	0.35
1.60	1.00	0.98	0.93	0.86	0.77	0.69	0.60	0.51	0.43	0.36
1.70	1.00	0.98	0.93	0.86	0.78	0.70	0.61	0.52	0.44	0.36
1.80	1.00	0.98	0.94	0.87	0.79	0.71	0.62	0.53	0.45	0.37
1.90	1.00	0.98	0.94	0.88	0.80	0.71	0.63	0.54	0.46	0.38
2.00	1.00	0.99	0.94	0.88	0.80	0.72	0.63	0.55	0.46	0.38
3.00	1.00	0.99	0.96	0.90	0.84	0.76	0.68	0.59	0.50	0.42
4.00	1.00	0.99	0.96	0.91	0.85	0.78	0.70	0.61	0.52	0.44
5.00	1.00	0.99	0.96	0.92	0.86	0.79	0.71	0.62	0.54	0.45
6.00	1.00	0.99	0.96	0.92	0.86	0.79	0.72	0.63	0.55	0.46
7.00	1.00	0.99	0.97	0.92	0.87	0.80	0.72	0.64	0.55	0.46
8.00	1.00	0.99	0.97	0.92	0.87	0.80	0.73	0.64	0.56	0.47
9.00	1.00	0.99	0.97	0.93	0.87	0.80	0.73	0.65	0.56	0.47
10.00	1.00	0.99	0.97	0.93	0.87	0.81	0.73	0.65	0.56	0.48
100.00	1.00	0.99	0.97	0.93	0.88	0.82	0.75	0.67	0.58	0.50
1000.00	1.00	0.99	0.97	0.93	0.88	0.82	0.75	0.67	0.59	0.50

[0193] 表2示出了针对$\alpha \geq 0$并且$90 \leq \varphi \leq 180$度的组合的T1的值。

[0194]

φ / α	90.0	100.0	110.0	120.0	130.0	140.0	150.0	160.0	170.0	180.0
0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
0.10	0.05	0.04	0.03	0.02	0.02	0.01	0.01	0.00	0.00	0.00
0.20	0.09	0.07	0.06	0.04	0.03	0.02	0.01	0.01	0.00	0.00
0.30	0.13	0.10	0.08	0.06	0.04	0.03	0.02	0.01	0.00	0.00
0.40	0.16	0.13	0.10	0.08	0.05	0.03	0.02	0.01	0.00	0.00
0.50	0.19	0.15	0.12	0.09	0.06	0.04	0.02	0.01	0.00	0.00
0.60	0.22	0.17	0.13	0.10	0.07	0.05	0.03	0.01	0.00	0.00
0.70	0.24	0.19	0.15	0.11	0.08	0.05	0.03	0.01	0.00	0.00
0.80	0.26	0.21	0.16	0.12	0.08	0.05	0.03	0.01	0.00	0.00
0.90	0.28	0.22	0.17	0.13	0.09	0.06	0.03	0.01	0.00	0.00
1.00	0.29	0.23	0.18	0.13	0.09	0.06	0.03	0.02	0.00	0.00
1.10	0.31	0.25	0.19	0.14	0.10	0.06	0.04	0.02	0.00	0.00
1.20	0.32	0.25	0.20	0.15	0.10	0.07	0.04	0.02	0.00	0.00
1.30	0.33	0.26	0.20	0.15	0.11	0.07	0.04	0.02	0.00	0.00
1.40	0.34	0.27	0.21	0.16	0.11	0.07	0.04	0.02	0.00	0.00
1.50	0.35	0.28	0.22	0.16	0.11	0.07	0.04	0.02	0.00	0.00
1.60	0.36	0.29	0.22	0.16	0.11	0.07	0.04	0.02	0.00	0.00
1.70	0.36	0.29	0.23	0.17	0.12	0.08	0.04	0.02	0.00	0.00
1.80	0.37	0.30	0.23	0.17	0.12	0.08	0.04	0.02	0.00	0.00
1.90	0.38	0.30	0.23	0.17	0.12	0.08	0.04	0.02	0.00	0.00
2.00	0.38	0.31	0.24	0.18	0.12	0.08	0.05	0.02	0.01	0.00
3.00	0.42	0.34	0.26	0.20	0.14	0.09	0.05	0.02	0.01	0.00
4.00	0.44	0.36	0.28	0.21	0.15	0.10	0.05	0.02	0.01	0.00
5.00	0.45	0.37	0.29	0.22	0.15	0.10	0.06	0.03	0.01	0.00
6.00	0.46	0.37	0.29	0.22	0.16	0.10	0.06	0.03	0.01	0.00

[0195]

7.00	0.46	0.38	0.30	0.23	0.16	0.10	0.06	0.03	0.01	0.00
8.00	0.47	0.38	0.30	0.23	0.16	0.11	0.06	0.03	0.01	0.00
9.00	0.47	0.39	0.31	0.23	0.16	0.11	0.06	0.03	0.01	0.00
10.00	0.48	0.39	0.31	0.23	0.16	0.11	0.06	0.03	0.01	0.00
100.00	0.50	0.41	0.33	0.25	0.18	0.12	0.07	0.03	0.01	0.00
1000.00	0.50	0.41	0.33	0.25	0.18	0.12	0.07	0.03	0.01	0.00

[0196] 假设对检测到响应STA想要伪造其在距离0.5*L处或更靠近感兴趣。因此,如果伪STA(其比0.5L更远)想要看起来比0.5L更靠近,如果伪STA在非阴影区域中,则可以检测到此。因此,这些伪STA的测量距离将小于0.5L,因为那是它们的意图。

[0197] 如果STA确实在0.5*L内,则它不必伪造它,因此$\alpha \leq 0.5$的区域在表1中没有阴影。

[0198] 表1和表2中的灰色阴影区域是,响应与发起STA之间的真实距离在那里大于0.5*L,并且发起STA在那里不能检测到响应STA想要出现在0.5*L或更小的距离处。所提出的方法防止欺骗驻留在$0 \leq \varphi \leq 90$度的大区域中的响应STA。然而,该方法不保护$90 < \varphi \leq 180$度的区域中的欺骗响应STA。此外,提出了使用另外的协作装置。因此,用于距离测量的系统可以包含第一设备和至少两个协作设备。下面讨论各种示例。在这样的系统中,充当第二协作设备的第四设备可以具有第四消息处理器,该第四消息处理器被布置用于确定测量消息到达第四设备的第四到达时间,并且将第四支持数据传送到第一设备,第四支持数据基于第四到达时间。第一消息处理器被布置用于从第二协作设备接收第四支持数据,使用第四支持数据获得第四设备和第二设备之间的第四距离,并且还使用第二受信距离和第四距离执行验证测试。

[0199] 在实施例中,验证测试使用关于第一设备、第二设备和第三设备的第一空间群集的第一三角不等式与关于第一设备、第二设备和第四设备的第二空间群集的第二三角不等式的组合。验证测试可以包括在下面关于使用三角不等式和两个协作STA的部分中讨论的测试。备选地,验证测试可以使用两个协作STA,如在后面的章节中关于以更好的方式使用三角不等式和两个协作STA所描述的。为此,第一设备可以知道两个协作设备之间的距离。

[0200] 在实施例中,验证测试可以验证第二设备根据第一空间群集的第一位置是否对应于第二设备根据第二空间群集的第二位置。可选地,验证测试可以使用不一致性检查用于检测是否所有所确定的距离都大于零。

[0201] 而且,验证测试可以基于多于第一和第二受信距离,即第一、第三和第四设备的整个群集。例如,这可以通过使用发起设备和两个协作设备之间的连接线之间的受信角度来完成。可选地,验证测试可以基于其中第三设备和第四设备被布置为使得从第三设备到第一设备的线与从第四设备到第一设备的线之间的受信角为至少90度的设置。可选地,验证测试可以基于其中第三设备和第四设备相对于第一设备彼此相对地布置的设置。可选地,验证测试可以基于其中第二受信距离对应于受信距离的设置。在以下章节中讨论验证测试的各种情况和计算。以下示例使用三角不等式和两个协作STA。

[0202] 图5示出了具有两个协作设备的空间群集。群集500包括类似于参考图1描述的设

备的标记“发起STA”的第一设备和两个“协作STA”。第一受信距离L在第一设备和第一协作STA之间,而第二受信距离L在第一设备和第二协作STA之间。

[0203] 使用示例群集,通过使用与第一协作STA完全相反的第二协作STA,对于$90 < \varphi \leq 180$实现更好的性能。在这种情况下,发起STA可以检测到许多(尽管不是全部)想要看起来比0.5*L更靠近的欺骗响应STA。对于该群集,在图5中以灰色示出了想要伪装其在距离0.5L处或更靠近的响应STA的区域。该区域类似于具有楔形横截面的环。

[0204] 图6示出了具有两个协作设备的第二空间群集。群集600包含类似于参考图1描述的设备的称为发起STA的第一设备和两个协作STA。第一受信距离L在第一设备和第一协作STA之间,而第二受信距离L在第一设备和第二协作STA之间。

[0205] 使用示例群集,发起STA使用如上面描述的两个协作STA,并且对响应STA想要伪造其在距离0.3L处或更靠近感兴趣。在这种情况下,从表1可以看出,至少1.1L远的所有响应STA都被捕获,并且许多STA比1.1L更靠近。

[0206] 图7示出了具有两个协作设备的又一空间群集。群集700包括类似于参照图1描述的设备的称为发起STA的第一设备710、称为响应设备的第二设备720、以及两个协作STA730、731。第一受信距离L在第一设备和第一协作STA之间,而第二受信距离L在第一设备和第二协作STA之间。注意,在该特定群集中,第二设备720可以在圆上的3d中的任何地方,其中其中心在通过第一、第三和第四设备的线上。因此,我们在这里仅将第二设备的位置计算为通过第一、第二、第三和第四设备的平面中的2d坐标。

[0207] 在示例群集中,使用三角不等式和两个协作STA。三角不等式用在经由协作STA1和2的测量上。使用余弦规则,我们可以将d2_1计算为

[0208] $$d2\_1^2 = L * \mathrm{sqrt}(\alpha^2 + 1 - 2 * \alpha * \cos(\varphi)) \quad (31)$$

[0209] 并且d2_2为

[0210] $$d2\_2^2 = L * \mathrm{sqrt}(\alpha^2 + 1 - 2 * \alpha * \cos(180 - \varphi)) = L * \mathrm{sqrt}(\alpha^2 + 1 + 2 * \alpha * \cos(\varphi)) \quad (32)$$

[0211] 欺骗响应STA改变其向发起STA发送的信息,使得发起STA将变为的距离d1_c、d2_1_c和d2_2_c

[0212] d1_c=d1-(d1-f) (33)

[0213] d2_1_c=d2_1-(d1-f) (34)

[0214] d2_2_c=d2_2-(d1-f) (35)

[0215] 发起STA检查不等式(14)对于其从协作STA1和2接收的距离是否成立

[0216] $$2*L \leq d2\_1\_c + d2\_2\_c \Leftrightarrow \quad (36)$$

[0217] $$2*L \leq L * \mathrm{sqrt}(\alpha^2 + 1 - 2 * \alpha * \cos(\varphi)) + L * \mathrm{sqrt}(\alpha^2 + 1 + 2 * \alpha * \cos(\varphi)) - 2 * (\alpha * L - f) \Leftrightarrow \quad (37)$$

[0218] $$L \leq f + L * \{\mathrm{sqrt}(\alpha^2 + 1 - 2 * \alpha * \cos(\varphi)) + \mathrm{sqrt}(\alpha^2 + 1 + 2 * \alpha * \cos(\varphi)) - 2 * \alpha\} / 2 \Leftrightarrow \quad (38)$$

[0219] $$f \geq 0.5 * L * \{ 2 + 2 * \alpha - \text{sqrt}(\alpha^2 + 1 - 2 * \alpha * \cos(\varphi)) - \text{sqrt}(\alpha^2 + 1 + 2 * \alpha * \cos(\varphi)) \} \Leftrightarrow \quad (39)$$

[0220] 因此,当响应STA如在以下不等式中选择f时,发起STA将检测到伪造其所报告的测量的响应STA。

[0221] $$f / L < 0.5 * \{ 2 + 2 * \alpha - \text{sqrt}(\alpha^2 + 1 - 2 * \alpha * \cos(\varphi)) - \text{sqrt}(\alpha^2 + 1 + 2 * \alpha * \cos(\varphi)) \} = T3 \quad (40)$$

[0222] 表3示出了针对α≥0并且$0 \leq \varphi \leq 180$度的组合的T3的值。T3的值的表围绕$\varphi = 90$度对称。

[0223]

φ / α	0.0 180.0	10.0 170.0	20.0 160.0	30.0 150.0	40.0 140.0	50.0 130.0	60.0 120.0	70.0 110.0	80.0 100.0	90.0
0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10
0.20	0.20	0.20	0.20	0.19	0.19	0.19	0.18	0.18	0.18	0.18
0.30	0.30	0.30	0.29	0.29	0.28	0.27	0.27	0.26	0.26	0.26
0.40	0.40	0.40	0.39	0.38	0.36	0.35	0.34	0.33	0.32	0.32
0.50	0.50	0.50	0.48	0.46	0.44	0.42	0.41	0.39	0.38	0.38
0.51	0.51	0.50	0.49	0.47	0.45	0.43	0.41	0.40	0.39	0.39
0.55	0.55	0.54	0.53	0.50	0.48	0.46	0.44	0.42	0.41	0.41
0.60	0.60	0.59	0.57	0.54	0.51	0.49	0.46	0.45	0.44	0.43
0.70	0.70	0.69	0.65	0.61	0.58	0.54	0.52	0.50	0.48	0.48
0.80	0.80	0.78	0.73	0.68	0.63	0.59	0.56	0.54	0.52	0.52
0.90	0.90	0.86	0.79	0.73	0.68	0.63	0.60	0.57	0.56	0.55
1.00	1.00	0.92	0.84	0.78	0.72	0.67	0.63	0.61	0.59	0.59
1.10	1.00	0.95	0.88	0.81	0.75	0.70	0.66	0.64	0.62	0.61
1.20	1.00	0.97	0.90	0.84	0.78	0.73	0.69	0.66	0.64	0.64
1.30	1.00	0.97	0.92	0.86	0.80	0.75	0.71	0.68	0.67	0.66
1.40	1.00	0.98	0.93	0.87	0.82	0.77	0.73	0.70	0.69	0.68
1.50	1.00	0.98	0.94	0.89	0.83	0.79	0.75	0.72	0.70	0.70
1.60	1.00	0.99	0.95	0.90	0.85	0.80	0.76	0.74	0.72	0.71
1.70	1.00	0.99	0.95	0.91	0.86	0.81	0.78	0.75	0.73	0.73
1.80	1.00	0.99	0.96	0.91	0.87	0.83	0.79	0.76	0.75	0.74
1.90	1.00	0.99	0.96	0.92	0.88	0.84	0.80	0.77	0.76	0.75

[0224]

2.00	1.00	0.99	0.96	0.93	0.88	0.84	0.81	0.79	0.77	0.76
3.00	1.00	0.99	0.98	0.96	0.93	0.90	0.87	0.85	0.84	0.84
4.00	1.00	1.00	0.98	0.97	0.95	0.93	0.91	0.89	0.88	0.88
5.00	1.00	1.00	0.99	0.97	0.96	0.94	0.92	0.91	0.90	0.90
6.00	1.00	1.00	0.99	0.98	0.97	0.95	0.94	0.93	0.92	0.92
7.00	1.00	1.00	0.99	0.98	0.97	0.96	0.95	0.94	0.93	0.93
8.00	1.00	1.00	0.99	0.98	0.97	0.96	0.95	0.94	0.94	0.94
9.00	1.00	1.00	0.99	0.99	0.98	0.97	0.96	0.95	0.95	0.94
10.00	1.00	1.00	0.99	0.99	0.98	0.97	0.96	0.96	0.95	0.95
100.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
1000.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00

[0225] 假设我们对检测到响应STA想要伪造其在距离0.5*L处或更靠近有兴趣。如果STA确实在0.5*L内,它不必伪造它,因此在表3中α<0.5的区域没有阴影。

[0226] 表3中的灰色阴影区域是,响应与发起STA之间的真实距离在那里大于0.5*L,并且发起STA在那里不能检测到响应STA想要出现在0.5*L或更小的距离处。清楚的是,所提出的方法防止欺骗驻留在$0\leq \varphi \leq 90$度的大区域中的响应STA,并且它不保护的区域(灰色阴影区域)明显比表1中的区域小得多。

[0227] 在图7的群集中,以若干方式通过4个设备计算平面中的位置(x,y)是可能的。如果响应STA忠实地报告其测量,则这些计算的位置将一致,除了测量误差。但是如果响应STA正在伪造其测量,则它们将不会,尤其是当其想要看起来比其实际上更靠近时。

[0228] 假设发起STA在(x,y)=(0,0)处,协作STA1在(L,0)处并且协作STA2在(-L,0)处。注意,这些STA和响应STA当然位于3-d世界中。平面(x,y)可为3-d中的任何平面,通过发起STA和两个协作STA的线位于所述平面中。在本节中,对于y坐标的计算应该产生两个值+/-y。仅保持正解不存在任何问题,因为当平面围绕通过发起STA和两个协作STA的线旋转180度时,获得对于y的另一个解。

[0229] 首先,检查由发起STA确定的距离是否大于零,如下面在章节“余弦规则检查与三角不等式检查之间的关系”中解释的。

[0230] $d1\_c>0$ (41)

[0231] $d2\_1\_c>0$ (42)

[0232] $d2\_2\_c>0$ (43)

[0233] 如果上面的三个不等式中的任一个不成立,我们假设欺骗响应STA。

[0234] 如果这三个不等式成立,我们使用余弦规则

[0235] $\cos(\angle ACB)=(|A|^2+|B|^2-|C|^2)/(2*|A|*|B|)$ (44)

[0236] 对于为了计算响应STA的位置的边的4种组合。我们总是使用点b作为响应STA的位置。

[0237] 使用点a＝(L,0)和c＝(0,0),我们可以将响应STA测量为是在b1＝(x1,y1)处

[0238] $cos\_c1＝(d1\_c^2+L^2-d2\_1\_c^2)/(2*d1\_c*L)$ (45)

[0239] 使用点a＝(-L,0)和c＝(0,0),我们可以将响应STA测量为是在b＝(x2,y2)处

[0240] $cos\_c2＝(d1\_c^2+L^2-d2\_2\_c^2)/(2*d1\_c*L)$ (46)

[0241] 使用点a＝(L,0)和c＝(-L,0),我们可以将响应STA测量为是在b＝(x3,y3)处

[0242] $cos\_c3＝(d2\_1\_c^2+4L^2-d2\_2\_c^2)/(2*d2\_1\_c*2L)$ (47)

[0243] 使用点a＝(-L,0)和c＝(L,0),我们可以将响应STA测量为是在b＝(x4,y4)处

[0244] $cos\_c4＝(d2\_2\_c^2+4L^2-d2\_1\_c^2)/(2*d2\_2\_c*2L)$ (48)

[0245] 然后,我们检查所有4个计算的余弦是否都在区间[-1,1]中。从下面的章节“余弦规则检查和三角不等式检查之间的关系”,我们知道我们到目前为止已经执行了与三角不等式测试相同的测试,因此在到目前为止的检查的情况下,上面的三个表适用。

[0246] 如果四个计算的余弦都在区间[-1,1]中,则我们如下计算响应STA的位置的四个点b1、b2、b3和b4。

[0247] $x1＝cos\_c1*d1\_c$ (49)

[0248] $y1＝sqrt(1-cos\_c1^2)*d1\_c$ (50)

[0249] $x2＝-cos\_c2*d1\_c$ (51)

[0250] $y2＝sqrt(1-cos\_c2^2)*d1\_c$ (52)

[0251] $x3＝L-cos\_c3*d2\_1\_c$ (53)

[0252] $y3＝sqrt(1-cos\_c3^2)*d2\_1\_c$ (54)

[0253] $x4＝-L+cos\_c4*d2\_2\_c$ (55)

[0254] $y4＝sqrt(1-cos\_c4^2)*d2\_2\_c$ (56)

[0255] 如果响应STA忠实地报告其时间测量,那么这4个点应当相同,除了定时测量误差的影响。注意,也如在其他地方解释的,通过多次执行测量并对结果进行平均,可以使测量误差更小。然而,当响应STA伪造其测量看起来比其实际上更靠近时并且当响应STA不在通过协作STA1和2的线上时,这4个点彼此不同。我们计算4个点b1、b2、b3和b4之间的所有距离的最大值emax

[0256] $emax＝MAX|bi-bj|$对于$i∈\{1,2,3,4\}$并且$j∈\{1,2,3,4\}$ (57)

[0257] 注意,不需要计算b4,因为b3和b4将被计算为相同点,除了数值误差。

[0258] 表4示出了除了当任何余弦检查失败时的emax/L的值,在此情况下示出了99的值。欺骗响应STA想要看起来所处的值f对于这些检查是重要的。

[0259] 我们在表4中将f选择为0.9。

[0260]

φ / α	0.0 180.0	10.0 170.0	20.0 160.0	30.0 150.0	40.0 140.0	50.0 130.0	60.0 120.0	70.0 110.0	80.0 100.0	90.0
0.00	1.85	1.85	1.85	1.85	1.85	1.85	1.85	1.85	1.85	1.85
0.10	1.65	1.59	1.55	1.53	1.50	1.48	1.47	1.46	1.45	1.45
0.20	1.46	1.38	1.31	1.27	1.23	1.20	1.18	1.16	1.15	1.15
0.30	1.26	1.16	1.09	1.03	0.99	0.95	0.93	0.91	0.90	0.89
0.40	1.07	0.96	0.87	0.81	0.77	0.73	0.71	0.69	0.68	0.68
0.50	0.87	0.76	0.67	0.61	0.57	0.54	0.52	0.50	0.50	0.49
0.51	0.85	0.74	0.65	0.59	0.55	0.52	0.50	0.49	0.48	0.48
0.55	0.77	0.66	0.57	0.51	0.48	0.45	0.43	0.42	0.42	0.41

[0261]

0.60	0.68	0.56	0.48	0.42	0.39	0.37	0.36	0.35	0.34	0.34
0.70	0.48	0.36	0.30	0.26	0.24	0.23	0.22	0.21	0.21	0.21
0.80	0.28	0.18	0.14	0.12	0.11	0.10	0.10	0.10	0.10	0.10
0.90	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
1.00	99.00	99.00	0.11	0.10	0.09	0.09	0.09	0.08	0.08	0.08
1.10	99.00	99.00	0.21	0.18	0.17	0.16	0.16	0.16	0.16	0.15
1.20	99.00	99.00	99.00	0.25	0.23	0.22	0.22	0.22	0.22	0.22
1.30	99.00	99.00	99.00	0.31	0.29	0.28	0.28	0.27	0.27	0.27
1.40	99.00	99.00	99.00	0.36	0.34	0.33	0.32	0.32	0.32	0.32
1.50	99.00	99.00	99.00	0.41	0.38	0.37	0.36	0.36	0.36	0.36
1.60	99.00	99.00	99.00	0.47	0.42	0.41	0.40	0.40	0.40	0.40
1.70	99.00	99.00	99.00	99.00	0.46	0.44	0.43	0.43	0.44	0.44
1.80	99.00	99.00	99.00	99.00	0.49	0.47	0.46	0.46	0.47	0.47
1.90	99.00	99.00	99.00	99.00	0.52	0.50	0.49	0.49	0.49	0.49
2.00	99.00	99.00	99.00	99.00	0.56	0.53	0.51	0.52	0.52	0.52
3.00	99.00	99.00	99.00	99.00	99.00	0.80	0.72	0.68	0.68	0.68
4.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	0.84	0.78	0.76
5.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00
6.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00
7.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00
8.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00
9.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00
10.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00
100.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00
1000.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00	99.00

[0262] 如从该表中可以看出的,对于α>0.9,示出99的单元与表3中具有值>0.9的单元一致,其示出了下面在章节“余弦规则检查和三角不等式检查之间的关系”中讨论的等效性。实际上在相距发起STA的0.9L的范围内的响应STA不必伪造它们在该范围内,因此该区域在表4中未加阴影。使用0.25L作为用于针对响应STA的位置的测量b1、b2、b3和b4中的最大差异的阈值,我们对表4的单元具有小于0.25的值并且α>0.9的区域进行阴影化。

[0263] 那意味着在阴影区域中,因此基本上对于具有相距发起STA的在0.9L与1.2L之间

的距离的响应STA,所提出的系统不能确定这些响应STA将其定时测量伪装为看起来位于相距发起STA的0.9L内。

[0264] 因此,使用位于相距发起STA距离L处的相对位置上的两个协作STA,所提出的系统可以检测位于相距发起STA的大于1.2L的所有距离处的响应STA,所述响应STA将其定时测量伪装为看起来位于相距发起STA的0.9L内。

[0265] 以下章节使用三角不等式和多于两个协作STA。可以通过在发起STA周围放置多于两个协作STA来获得更好的性能。为了最好地检测位于发起STA周围尽可能多的位置中的欺骗响应STA,当使用三个协作STA时,最好将发起STA和协作STA放置在平面中。这是因为如果发起STA不在通过三个协作STA的平面上,那么将存在欺骗响应STA总是比三个协作STA中的任一个更靠近发起STA并且因此所提出的方法不起作用的体积(参见例如表2)。

[0266] 使用未定位在一条线上但是该群集形成三角形的两个协作STA和发起STA也是可能的。使用距离d1、d2_1、d2_2以及由两个协作STA和发起STA形成的三角形的边长,发起STA可以使用余弦规则对由第二设备和来自两个协作STA和发起STA的集合的任何设备对形成的三角形执行检查。

[0267] 当使用四个协作STA时,它们应当理想地放置在正四面体的角上,并且发起STA位于正四面体的质心处。该群集是最对称的可能群集,并且因此提供最好的保护。

[0268] 具有单位球面上的其4个点、原点处的质心并且具有水平的且下面水平面的正四面体的顶点是

[0269] A=(sqrt(8/9),0,-1/3)

[0270] B=(-sqrt(2/9),sqrt(2/3),-1/3)

[0271] C=(-sqrt(2/9),-sqrt(2/3),-1/3)

[0272] D=(0,0,1)

[0273] 因此,协作STA位于顶点的位置处,并且发起STA位于原点处,并且在这种情况下,距离L等于1。任何两个STA之间的最大距离是任何两个协作STA之间的距离,因此正四面体的每个边的长度,其为

[0274] ||A-D||=||(sqrt(8/9),0,-1/3)-(0,0,1)||

[0275] =||(sqrt(8/9),0,-4/3)||

[0276] =sqrt(8/3)≈1.63 (58)

[0277] 任何协作STA、原点和响应STA之间的最大角度处于当响应STAA处于通过正四面体的四个面中的任一个的原点和质心的线时。面ABD的质心是F={(sqrt(8/9),0,-1/3)+(-sqrt(2/9),sqrt(2/3),-1/3)+(0,0,1)}/3

[0278] =(sqrt(8/9)-sqrt(2/9),sqrt(2/3),1/3)/3 (59)

[0279] 角度∠AOF、∠BOF和∠DOF都相同。可以使用余弦规则计算该角度

[0280] $\cos(\angle DOF)=(||D||^2+||F||^2-||D-F||^2)/(2*||D||*||F||)$ (60)

[0281] $||D||^2=1$ (61)

[0282] $||F||^2=\{(sqrt(8/9)-sqrt(2/9))^2+2/3+1/9\}/9$

[0283] =\{8/9+2/9-2*sqrt(16/81)+7/9\}/9

[0284] =1/9 (62)

[0285] $||D-F||^2=\{(sqrt(8/9)-sqrt(2/9))^2+2/3\}/9+(8/9)^2$

[0286] ＝{8/9+2/9-2*sqrt(16/81)+2/3}/9+64/81

[0287] ＝{2/9+6/9}/9+64/81

[0288] ＝72/81＝8/9 (63)

[0289] 因此

[0290] cos(∠DOF)＝(1+1/9-8/9)/(2*1*1/3)

[0291] ＝3*(2/9)/2

[0292] ＝1/3 (64)

[0293] ∠DOF)＝arccos(1/3)＝70.53度 (65)

[0294] 因此,在一个发起STA位于正四面体的质心处且四个协作STA位于相距发起STA的距离L处的该四面体的顶点处的群集的情况下,如果它们相距发起STA比1.5L更远(参见表1),则可以检测到想要伪装它们比0.5L更靠近发起STA的所有响应STA。可以检测到0.5L和1.5L之间的区域中的许多这样的STA。

[0295] 可选地,可以通过使用发起STA和协作STA在计算的位置中添加不一致性检查来改善防御,类似于在先前章节中解释的防御。

[0296] 在实施例中,测距协议可以包括充当发起设备的第一设备向第二设备发送发起消息,同时在接收到发起消息时,第二设备必须发送测量消息。第一消息处理器被布置为与第三设备交换角色改变数据,以使得第三设备能够充当用于距离测量的发起设备。此外,第三设备被布置为在接收到角色改变数据时,基于第二测量消息根据测距协议获得第三设备和第二设备之间的第三距离,并且将第三支持数据传送到第一设备,第三支持数据指示第三距离。例如,第三支持数据可以包含第三设备已经测量的FTM协议的t2和t3值。t1和t4值也可以是它的一部分,但这不是必需的,因为第一设备可以接收并使用来自第二设备的包含t1和t4的原始消息。

[0297] 而且,第一消息处理器被布置为当在第一设备处接收第二测量消息时确定第一设备与第二设备之间的第二距离,从第三设备接收第三支持数据,并且还使用第二距离和第三支持数据来执行验证测试。在该实施例中,发起STA和协作STA交换角色,或换句话说,使用两个发起STA计算位置两次。

[0298] 在图4的群集中,我们现在有充当第一STA1和第二STA2的两个设备410、430,两个设备410、430一起工作以确定到响应STA的距离。在一系列测量中,STA1充当发起STA并且STA2充当协作STA,而在第二系列测量中,它们承担相反的角色。每个系列中的个体时间测量在计算距离之前进行平均,以便改善距离测量结果。可以在角色被交换之前完成第一系列的所有个体测量,并且执行第二系列的个体测量。但是角色交换也可以在任何数量的个体测量之后完成。

[0299] 使用来自第一系列测量的定时测量,因此在STA1是发起STA的情况下,我们可以使用等式(49)和(50)来计算响应STA的位置r1＝(x1,y1)。使用来自第二系列测量的定时测量,因此在STA2是发起STA的情况下,我们可以使用类似的等式来计算响应STA的位置r2＝(x2,y1)。注意,在该特定群集中,第二设备420可以在圆上的3d中的任何地方,其中,其中心在通过第一和第三设备的线上。因此,我们在这里仅将第二设备的位置计算为通过第一、第二和第三设备的平面中的2d坐标。

[0300] 如果响应STA忠实地报告其定时测量,则计算的点r1和r2应当相等,除了测量误差

之外。但是当响应STA想要看起来比其实际上更靠近时,这可能是不同的。

[0301] 在先前章节中,欺骗响应STA试图出现在相距发起STA的距离f处。假设响应STA不知道两个STA不时地交换角色,并且尝试出现在相距它们中的每一个的假距离f处。在这种情况下,r1和r2将明显不同,特别是如果L<0.5L。

[0302] 因此,使用均充当发起STA的两个或更多个STA并且使用由发起STA中的每一个测量的距离计算响应STA的位置并判断所计算位置的差异是检测伪装其定时测量的响应STA的好想法。

[0303] 然而,在这种情况下,上面描述的攻击不是最好的可能攻击。更好的攻击是当响应STA知道它正在利用哪个发起STA执行FTM协议并且它知道群集的参数(因此L和φ或d1和d2)时。这在实践中可能难以知道,但不是不可能的。假设攻击者知道除了秘密加密密钥之外的所有内容是良好的安全实践。因此,优选地使用如先前章节中描述的防御。

[0304] 以下章节讨论余弦法则检查与三角不等式检查之间的关系。检查三角不等式对于三个长度|A|、|B|和|C|是否成立

[0305] $|C| \leq |A| + |B|$ (66)

[0306] $|A| \leq |B| + |C|$ (67)

[0307] $|B| \leq |A| + |C|$ (68)

[0308] 与检查是否以下成立相同

[0309] $-1 \leq \cos(\angle ACB) \leq 1$ (69)

[0310] 对于角度∠ACB的余弦规则是

[0311] $\cos(\angle ACB) = (|A|^2 + |B|^2 - |C|^2)/(2*|A|*|B|)$ (70)

[0312] 检查余弦是否不小于-1产生

[0313] $\cos(\angle ACB) \geq -1 \Leftrightarrow$

[0314] $(|A|^2 + |B|^2 - |C|^2)/(2*|A|*|B|) \geq -1$ (71)

[0315] 只有|A|*|B|)>0时,我们才可以从不等式(71)导出以下不等式

[0316] $(|A|^2 + |B|^2 - |C|^2) \geq -2 * |A| * |B| \Leftrightarrow$

[0317] $(|A|^2 + |B|^2 + 2 * |A| * |B| - |C|^2) \geq 0 \Leftrightarrow$

[0318] $(|A| + |B|)^2 - |C|^2 \geq 0 \Leftrightarrow$

[0319] $(|A| + |B|)^2 \geq |C|^2 \Rightarrow$

[0320] $|C| \leq (|A| + |B|)$ (72)

[0321] 其与不等式(66)相同。

[0322] 类似地,检查余弦是否不大于1产生

[0323] $\cos(\angle ACB) \leq 1 \Leftrightarrow$

[0324] $(|A| - |B|)^2 - |C|^2 \leq 0 \Leftrightarrow$

[0325] $(|A| - |B|)^2 \leq |C|^2 \Leftrightarrow$

[0326] $\mathrm{abs}(|A| - |B|) \leq |C| \Leftrightarrow$

[0327] $|A|\leqslant(|B|+|C|)\&|B|\leqslant(|A|+|C|)$ (73)

[0328] 这两个不等式对于三角形也必须成立。

[0329] 注意,真实距离总是大于或等于0。上面的推理适用于正距离,但不适用于负距离。当响应STA伪装其测量以变得更靠近时,由发起STA获得的距离可能是负的。因此,对三个三角不等式进行检查相当于检查所测量的三个距离是否大于或等于0并且检查余弦不等式(69)是否成立。

[0330] 在实施例中,第三消息处理器被布置为确定从第二设备接收的至少一个消息的第三信号强度,并且将第三信号强度数据包括在到第一设备的支持数据中。第一消息处理器被布置为确定从第二设备接收的至少一个消息的第一信号强度,并且通过将第一信号强度和第三信号强度与所确定的距离处的相应预期信号强度进行比较来验证所确定的距离是否可靠。在该实施例中,另外执行基于信号强度的距离测量以增加可靠性。除了到达和发送时间之外,接收信号强度也可以用作距离的测量。设备包括发送功率,利用该发送功率将消息发送到该消息中的另一设备,另一个设备测量接收信号强度,并且另一个设备可以基于假定的发射器天线性质(例如,它是全向的)来确定距离,并且信号强度随着距离以2的幂减小。当至少一个协作设备测量该相同消息的信号强度并且将这样的数据包括在传送给第一设备的支持数据中时,第一设备可以基于接收信号强度来确定相距第二设备的距离的比。

[0331] 在实施例中,第一设备和第三设备可以由3GPP网络中的基站实现,而第二设备由UE实现。3GPP中的基站在所谓的资源元素的时频网格中进行发送和接收。时频网格中的一些位置由3GPP标准固定,并且用于向基站范围内的所有UE广播系统信息,例如,基站将在何时并在哪些频率上向特定UE(下行链路)发送某些内容以及特定UE可以在何时并利用哪些频率向基站(上行链路)或特定的其他UE(侧链路)发送某些内容的信息。当基站根据本发明协作时,它们的时频网格应当对准并同步,并且它们均应当使网格中的相同时频位置(资源元素)可用,因此它们都能够测量来自相同UE的相同消息的到达时间或接收信号强度。

[0332] 在又一实施例中,测距协议包括附加性质或附加消息,其可以例如被添加到如[802.11]中定义的测距协议,包含凭证(例如,公钥)或凭证的散列或加密凭证。这样的消息是基于密钥数据进行密码保护的消息的示例。第二设备可以包括这样的凭证或凭证的散列或加密凭证作为测距协议的消息交换的一部分。为了对称,第一设备也可以在另外的消息中包括这样的凭证、凭证的散列或加密凭证。在测距协议的消息中包含凭证或凭证的散列或加密凭证的优选字段是这样的字段,其中,传送该字段的信号或信号的至少一部分用于测量消息的发送或到达时间,使得另一设备即使不是不可能也很难将其凭证或其凭证的散列或其加密凭证插入在用于测量第一设备和第二设备之间的距离的消息中。携带凭证或凭证的散列或加密凭证的信号越靠近(在时间上)用于测量距离的信号或这些信号之间的重叠越多,越好。这样,第一设备可以确定测距协议的消息中的凭证或凭证的散列或加密凭证确实是与其一起执行距离测量协议的第二设备中的一个。在一个实施例中,第一消息处理器被布置为处理该凭证或凭证的散列或加密凭证,并且验证它是否匹配先前已经由以下设备使用的凭证:利用该设备已经成功执行设备认证并建立相互信任的,诸如通过使用Wi-Fi保护设置协议、设备供应协议、Diffie-Hellman密钥交换和/或4路WPA2握手。如果找到匹配,则第一设备可以假设第一和第二设备之间的距离测量可以是可信的并且被认为是可靠的。如果没有找到匹配,则第一设备将不信任第一和第二设备之间的距离测量,并且执行附

加步骤来验证距离测量的可靠性,诸如使用如在其他实施例中描述的机制。在另一实施例中,测量值(例如,第一时间数据和/或第二时间数据)使用如在第一和第二设备之间执行的更早设备认证过程期间建立的在第一和第二设备之间商定或从在第一和第二设备之间商定的凭证导出的密钥来加密。

[0333] 在备选实施例中,第二设备可以包括将在稍后的连接建立期间使用的凭证或凭证的散列或加密凭证。第一消息处理器被布置为结合第一设备和第二设备之间的测量距离来处理和存储接收到的凭证或凭证的散列或加密凭证,以便将测量距离与和该凭证连接的特定设备安全地相关。在建立第一设备与第二设备之间的连接时,第一设备验证在执行设备认证时(诸如在执行Wi-Fi保护设置协议、设备供应协议、Diffie-Hellman密钥交换期间和/或在执行4路WPA2握手时)是否使用相同的凭证或其衍生物。通过这样做,第一设备可以确定它与之连接的设备是与针对其完成特定距离测量的设备相同的设备。特别地,如果凭证是公钥并且如果建立第一设备和第二设备之间的连接包括第二设备已经向设备1成功地证明其拥有属于公钥的私钥作为距离测量中的凭证,则第一设备可以确定第二设备是其测量距离的设备而不是冒名顶替者。

[0334] 在实施例中,第一消息处理器被布置为在评价所确定的距离不可靠时进行到不同的过程或功能(对数据或功能的拒绝访问),而非预期的过程。例如,基于正常距离的过程可以是授权对基于位置的服务或本地外围设备的访问。而且,可以基于距离测量来控制或拒绝通过另一网络(例如,以太网、互联网、3GPP核心网络)去往或来自第一设备的路由。如果所确定的距离被认为是不可靠的,则可以拒绝所有进一步的通信和/或访问,和/或可以向管理系统或护卫员发送警告消息。而且,第一消息处理器可以被布置为在进行到任何基于正常距离的过程之前接合与第二设备可以执行的不同的安全协议,诸如请求用户的附加凭证和/或个人身份。不同的安全协议可以是主协议的附加过程或进一步增强的执行,并且可以例如导致正常安全过程中的更严格或严厉的步骤。可选地,第一消息处理器被布置为使用不同的测距协议和/或不同类型的无线通信(例如非常近距离处的NFC)或由第二设备的操作人员请求进一步的距离测量,以提供一些身份和/或生物统计数据(如指纹)。而且,在进行到任何基于正常距离的过程之前,第一消息处理器可以被布置为拒绝或限制对第一设备中的至少一些数据和/或至少一个应用的访问。例如,即使距离被认为是不可靠的,也可以提供基本服务,而如果距离被认为是可靠的,则提供扩展服务。

[0335] 图8示出了一种用于经由第一设备和第二设备之间的无线通信的距离测量的方法,该无线通信包括如上面描述的测距协议。第一设备和第二设备类似于如参考图1示出并进一步描述的第一设备和第二设备。第三设备充当位于相距第一设备的受信距离处的协作设备。该方法可以由第一设备中的处理器执行,但是也可以由不同设备中的处理器和/或基于接收到的到达时间和支持数据在不同的时间处理。例如,该方法可以在不主动参与测距协议但是接收所有消息并且知道受信距离的又一设备处执行。

[0336] 该方法在节点“开始801”处开始。在第一阶段RNGP 802中,该方法可以执行测距协议,并且执行到达时间测量,如参考图1描述的。该方法通过基于测量消息到达第一设备的第一到达时间来获得第一设备与第二设备之间的第一距离而继续阶段OD1 803,并且随后在阶段CO_COP 804中与协作设备进行通信。协作设备被布置用于确定测量消息到达协作设备的第三到达时间,并且提供支持数据,所述支持数据基于第三到达时间。然后,该方法继

续评价所确定的距离。在下一阶段OD3 805中,使用例如基于第三到达时间和测量消息的发送时间计算的支持数据获得第三设备与第二设备之间的第三距离。最后,在阶段VERT 806中,对第一距离、受信距离和第三距离执行验证测试。当所述距离对应于第一设备、第二设备和协作设备的可行空间群集时,验证测试将第一距离接受为可靠的。测试可以基于如上面阐明的三角不等式和不一致性检查。

[0337] 在实施例中,该方法可以包括准备阶段,其中,指示第一设备充当发起设备以提供第一到达时间或第一距离。类似地,可以指示第三设备充当协作设备以提供基于第三到达时间的支持数据。准备阶段可以由单独的控制设备、计算机或服务器执行。备选地,第一设备或第三设备可以执行所述指示。

[0338] 图9示出了如上面关于图8描述的用于在经由第一设备和第二设备之间的无线通信的距离测量中充当协作设备的方法。协作设备可以位于相距第一设备的受信距离处。

[0339] 该方法在节点"开始901"处开始。在第一阶段RNGP 902中,该方法可以监测由第一和第二设备执行的测距协议。该方法通过确定测量消息到达协作设备的第三到达时间而继续阶段ARR3 903。随后,在阶段CO_IN 904中,协作侧随后例如使用无线协议或使用有线连接与第一设备通信。接下来,在阶段SUP 905中,该方法向第一设备提供支持数据。支持数据基于第三到达时间。然后,该方法在协作侧处在节点"结束906"处结束。如上面描述的,第一设备被布置为使用支持数据获得协作设备和第二设备之间的所述第三距离,并且对第一距离、受信距离和第三距离执行验证测试。

[0340] 图10a示出了具有可写部分1010的计算机可读介质1000,所述可写部分包括计算机程序1020,计算机程序1020包括用于使处理器系统在系统中执行参考图9-10所描述的以上方法的一种或多种方法的指令。计算机程序1020可以作为物理标记,或利用计算机可读介质1000的磁化被嵌入在计算机可读介质1000上。然而,也能想到任何其他适当的实施例。此外,将要意识到,尽管这里将计算机可读介质1000示为光盘,但是计算机可读介质1000可以是任何适当的计算机可读介质,诸如硬盘、固态存储器、闪速存储器等,并且可以是不可记录的或可记录的。计算机程序1020包括用于使处理器系统执行所述方法的指令。

[0341] 图10b在示意图中示出了根据参考图9-10描述的设备或服务器实施例的处理器系统1140。所述处理器系统包括一个或多个集成电路1110。附图中示意性示出了一个或多个集成电路1110的架构。电路1110包括处理单元1120,例如CPU,其用于运行计算机程序部件,以执行根据实施例的方法和/或实施其模块或单元。电路1110包括用于存储编程代码、数据等的存储器1122。存储器1122的部分可以是只读的。电路1110可以包括通信元件1126,例如天线、连接器或这两者等。电路1110可以包括用于执行在所述方法中定义的处理的部分或全部的专用集成电路1124。处理器1120、存储器1122、专用IC 1124和通信元件1126可以经由例如总线的互连1130而彼此连接。处理器系统1110可以被布置用于分别使用天线和/或连接器进行接触和/或无接触通信。

[0342] 提供了一种能从网络下载和/或存储在计算机可读介质和/或微处理器可执行介质上的计算机程序产品,其包括程序代码指令,所述程序代码指令在计算机上被运行时实施以上方法以保护位置信息,如下文进一步阐述的。

[0343] 可以使用软件来执行根据本发明的方法,所述软件包括用于使处理器系统执行各自方法的指令。软件可以仅包括由系统的特定子实体采取的那些步骤。软件可以被存储在

适当的存储介质中,诸如硬盘、软盘、存储器等。软件可以作为信号沿着线路发送或无线发送或使用例如因特网的数据网络发送。可以使软件能够被下载和/或用于在服务器上远程使用。可以使用被布置成配置例如现场可编程门阵列(FPGA)的可编程逻辑的比特流来执行根据本发明的方法,以执行所述方法。应当意识到,所述软件可以是源代码、目标代码、代码中间源和目标代码的形式,诸如部分编译的形式,或适于在根据本发明的方法的实施方式中使用的任何其他形式。涉及计算机程序产品的实施例包括与所述方法的至少一种方法的处理步骤中的每个处理步骤相对应的计算机可执行指令。这些指令可以被细分成子例程和/或被存储在可以静态或动态链接的一个或多个文件中。涉及计算机程序产品的另一实施例包括与所述系统和/或产品中的至少一种的模块中的每个模块相对应的计算机可执行指令。

[0344] 将意识到,为了清晰起见,以上描述已经参考不同的功能单元和处理器描述了本发明的实施例。然而,将认识到,可以使用功能在不同功能单元或处理器之间的任意适当分布而不脱离本发明。例如,被图示为要由独立单元、处理器或控制器执行的功能可以由相同处理器或控制器执行。因此,提到特定的功能单元仅仅要被看作提到用于提供所述功能的适当手段,而不是表示严格的逻辑或物理结构或组织。本发明能够以任何适当的形式被实施,包括硬件、软件、固件或这些的任意组合。

[0345] 要指出的是,在本文中,“包括”一词不排除存在所列出的那些之外的元件或步骤,元件之前的词语“一”或“一个”不排除存在多个这样的元件,任何附图标记都不应当限制权利要求的范围,可以利用硬件和软件两者来实施本发明,并且若干“模块”或“单元”可以由同一件硬件或软件来表示,并且处理器可以完成一个或多个单元的功能,可能与硬件元件协作。此外,本发明不限于实施例,本发明体现在上文所描述的或相互不同的从属权利要求中所记载的每个新颖特征或特征组合中。

[0346] 参考文献

[0347] [36.133]3GPP TS 36.133:“Evolved Universal Terrestrial Radio Access(E-UTRA);Requirements for support of radio resource management”.

[0348] [36.211]3GPP TS 36.211:“Evolved Universal Terrestrial Radio Access(E-UTRA);Physical Channels and Modulation”.

[0349] [36.214]3GPP TS 36.214:“Evolved Universal Terrestrial Radio Access(E-UTRA);Physical layer-Measurements”.

[0350] [36.321]3GPP TS 36.321:“3rd Generation Partnership Project;Technical Specification Group Radio Access Network;Evolved Universal Terrestrial Radio Access(E-UTRA);Medium Access Control(MAC)protocol specification”.

[0351] [36.355]3GPP TS 36.355:“Evolved Universal Terrestrial Radio Access(E-UTRA);LTE Positioning Protocol(LPP)”.

[0352] [37.571-1]3GPP TS 37.571-1:“Universal Terrestrial Radio Access(UTRA) and Evolved UTRA(E-UTRA)and Evolved Packet Core(EPC);User Equipment(UE) conformance specification for UE positioning;Part 1:Conformance test specification”

[0353] [802.11]IEEE Computer Society,“IEEE Standard for Information

Technology-Telecommunications and Information Exchange Between Systems-Local and Metropolitan Area Networks-Specific requirements Part 11:Wireless LAN Medium Access Control(MAC)and Physical Layer(PHY)Specifications,"(IEEE Std.802.11-2016),December 2016

[0354] [802.1AS]Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 1AS: Timing and synchronization for time sensitive applications in bridged local area networks,Reference number ISO/IEC/IEEE 8802-1AS:2014(E)

[0355] [DH]Diffie,W.;Hellman,M.(1976),"New directions in cryptography",IEEE Transactions on Information Theory,22(6):644-654

[0356] [DPP]Device Provisioning Protocol-Technical Specification-Version 1.0,Wi-Fi Alliance,2018,https://www.wi-fi.org/file-member/device-provisioning-protocol-specification.

[0357] [NAN]Neighbor Awareness Networking-Technical Specification-Version 2.0,Wi-Fi Alliance,2017,https://www.wi-fi.org/file-member/wi-fi-nan-technical-specification.

[0358] [OTDOA]Sven Fischer,"Observed Time Difference Of Arrival(OTDOA) Positioning in 3GPP LTE",Qualcomm Technologies,Inc.,June 6,2014.

[0359] [OWE]Opportunistic Wireless Encryption-Technical Specification-Version 1.0,Wi-Fi Alliance,2018,https://www.wi-fi.org/file-member/opportunistic-wireless-encryption-specification.

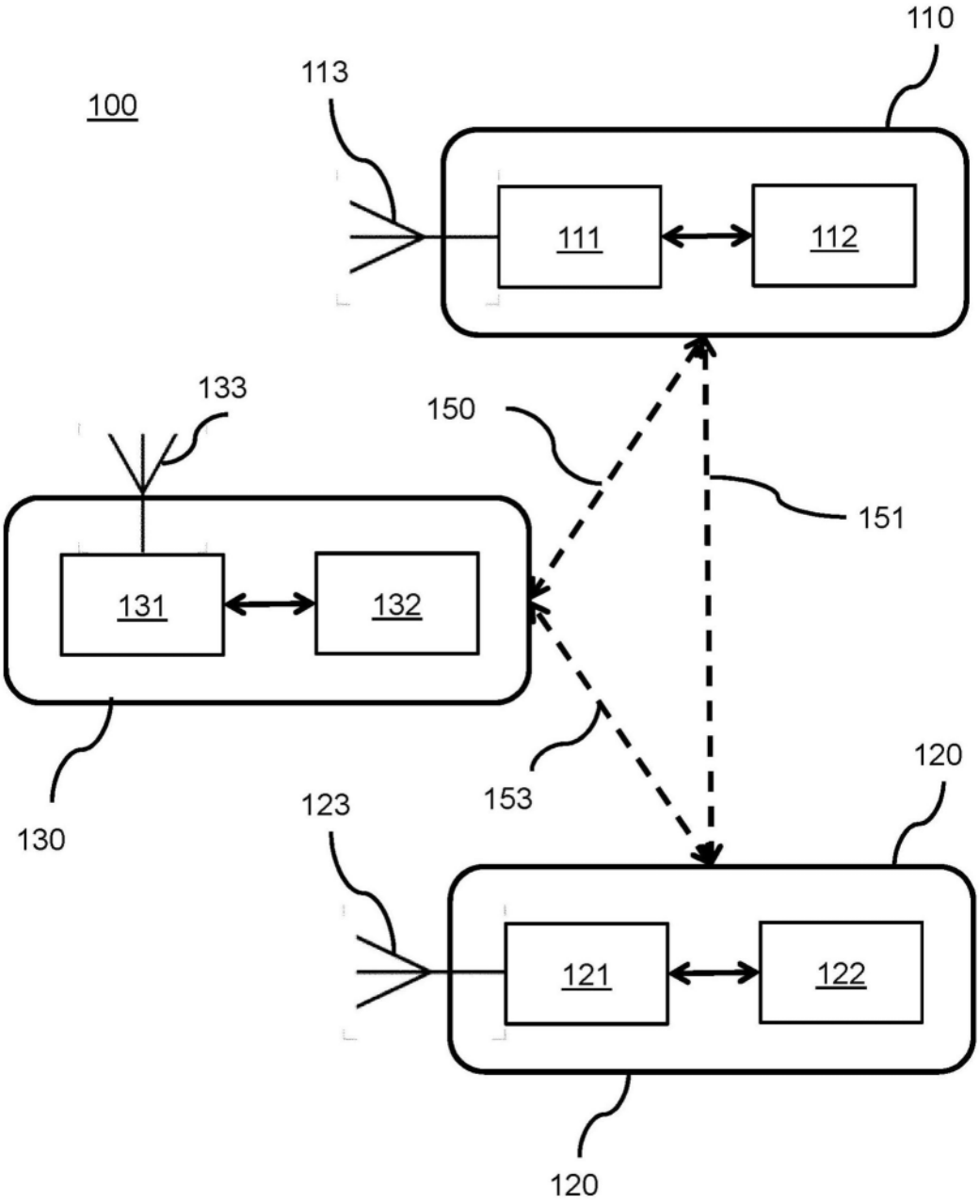

110
113
100
111
112
133
150
151
131
132
130
153
120
123
121
122
120

图1

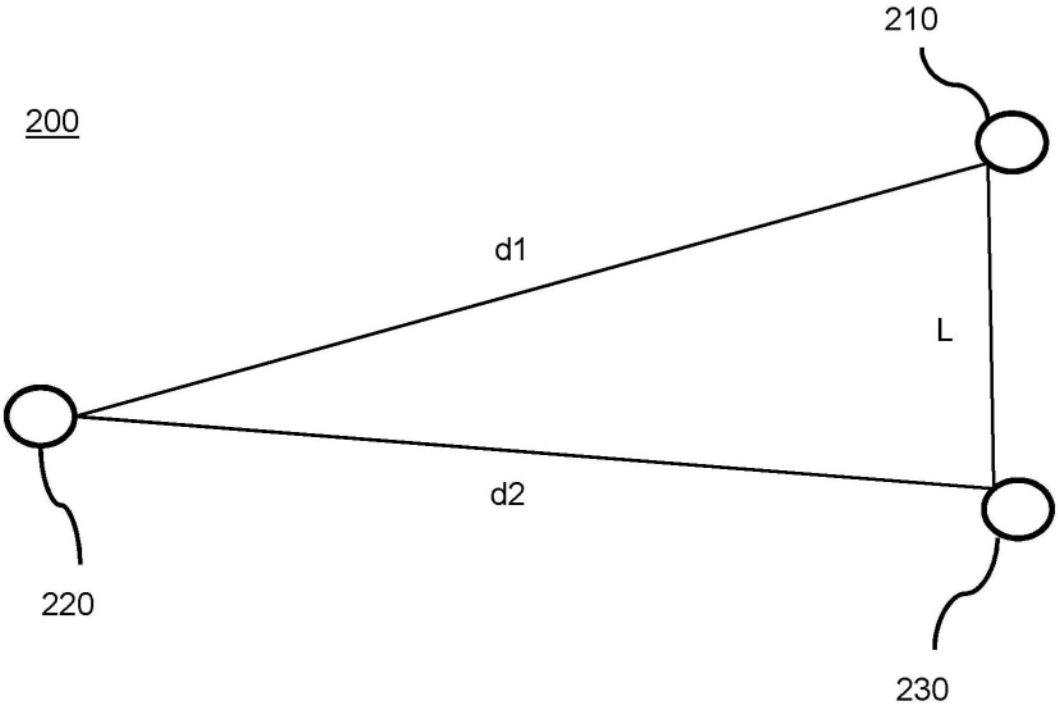


图2

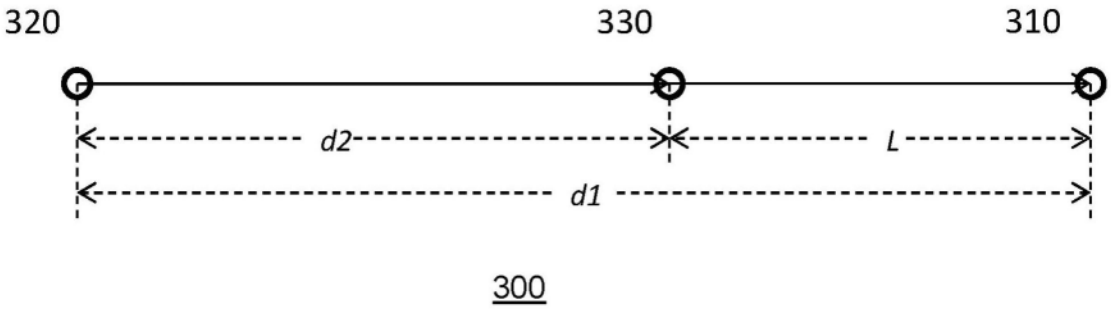


图3

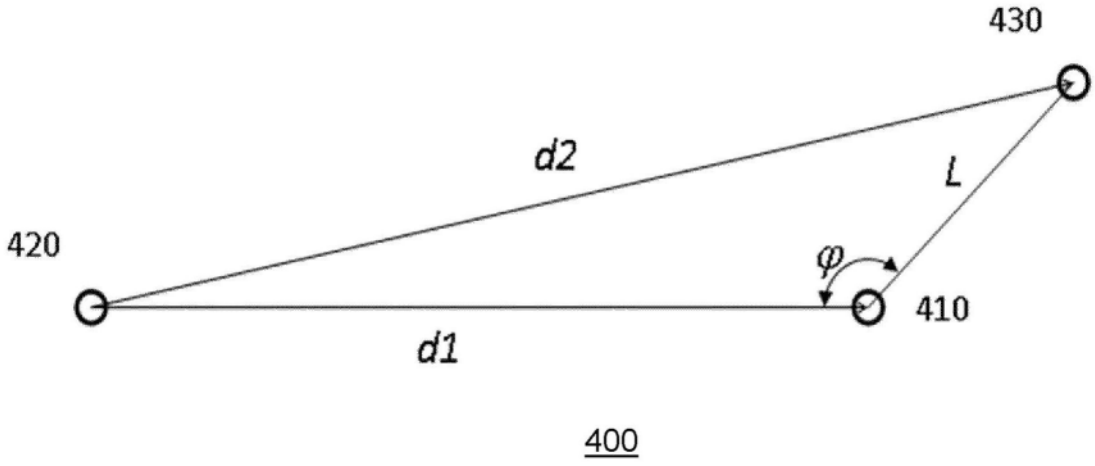


图4

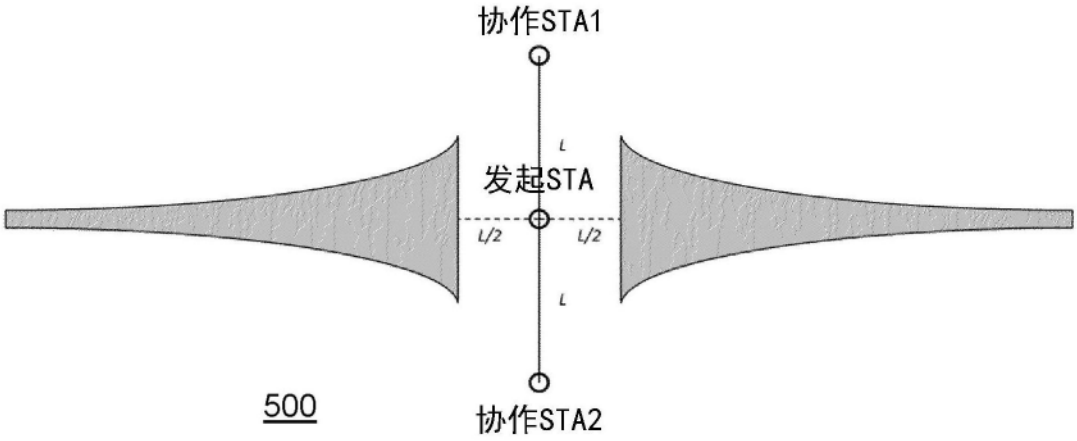


图5

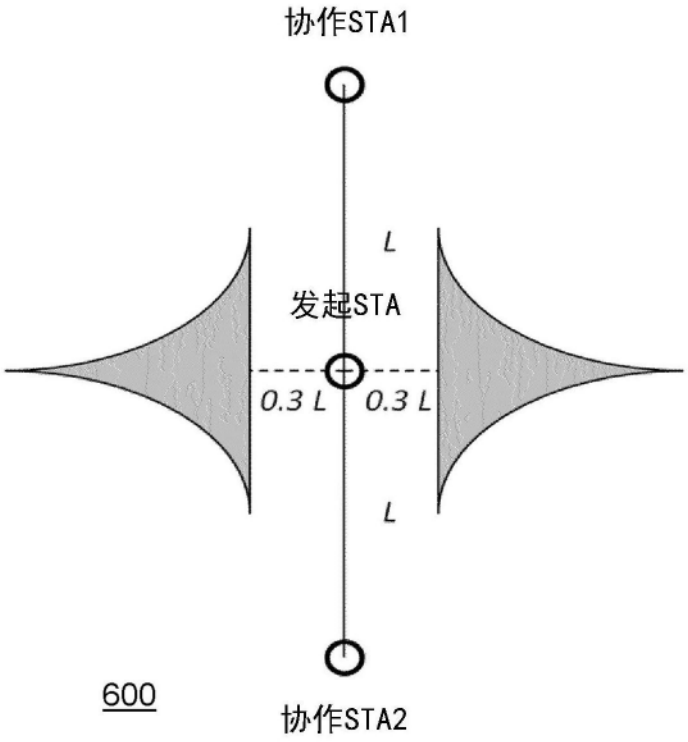

协作STA1
L
发起STA
0.3 L
0.3 L
L
600
协作STA2

图6

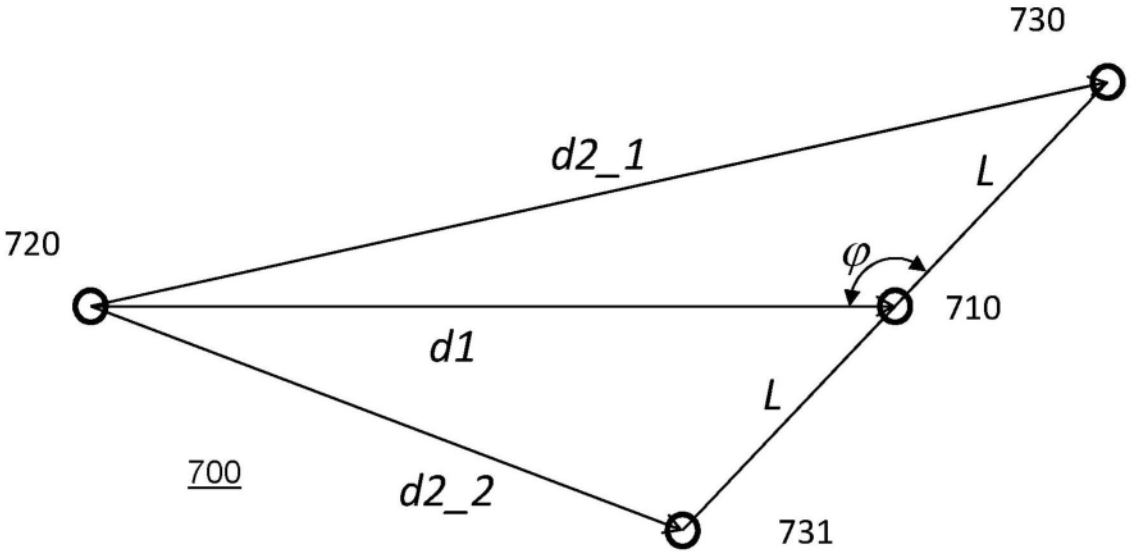

730
d2_1
L
720
φ
710
d1
L
700
d2_2
731

图7

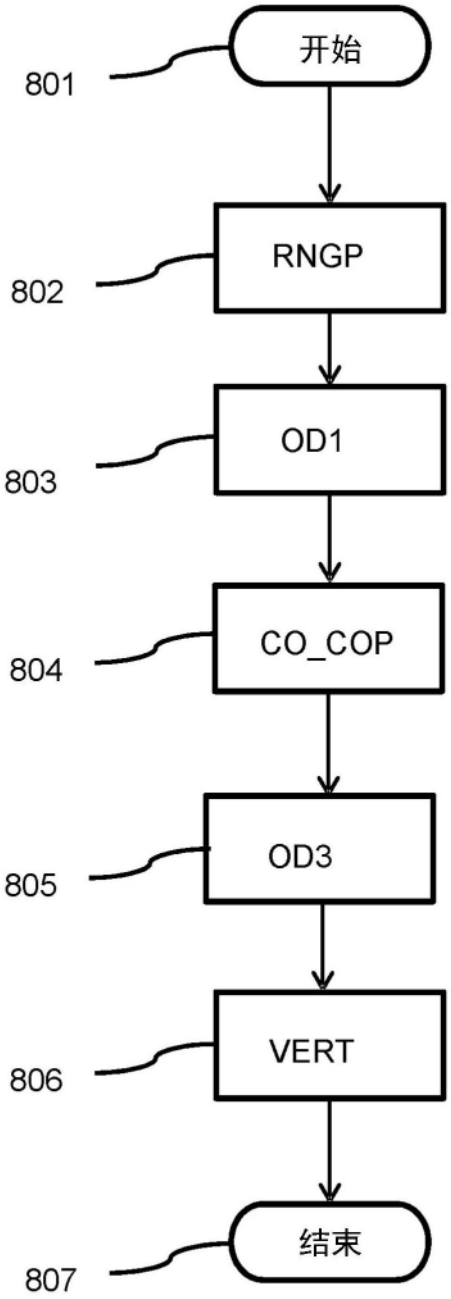


图8

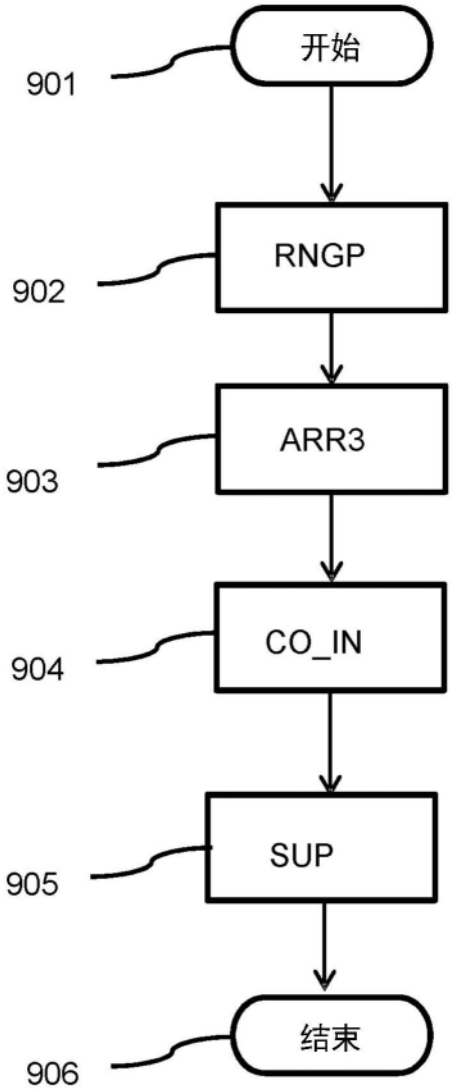


图9

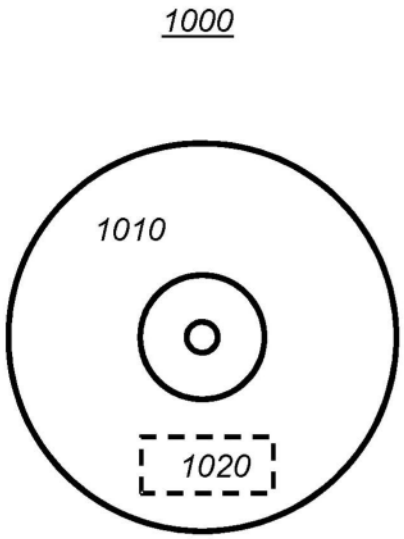


图10a

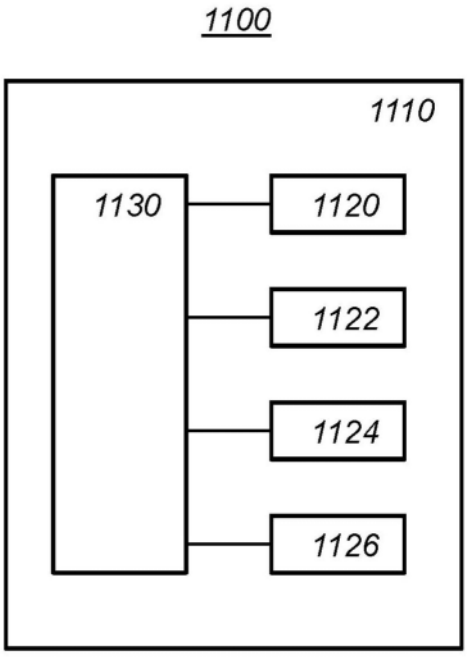


图10b