(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 110034940 B
(45)授权公告日 2021.07.20

(21)申请号 201910188008.8
(22)申请日 2014.01.23
(65)同一申请的已公布的文献号
申请公布号 CN 110034940 A
(43)申请公布日 2019.07.19
(30)优先权数据
13152725.1 2013.01.25 EP
(62)分案原申请数据
201480018193.1 2014.01.23
(73)专利权人 皇家KPN公司
地址 荷兰鹿特丹
专利权人 荷兰应用自然科学研究组织
(72)发明人 F.弗兰森 P.维尤根
S.德基伊维特 M.埃弗特斯
(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 张健 陈岚
(51)Int.Cl.
H04L 12/18(2006.01)
H04L 29/06(2006.01)
H04W 8/00(2009.01)
H04W 12/04(2021.01)
H04W 12/06(2021.01)
H04W 64/00(2009.01)
H04W 76/14(2018.01)
H04L 29/12(2006.01)
H04W 88/02(2009.01)
H04W 92/18(2009.01)

(56)对比文件
CN 101772137 A,2010.07.07
CN 101371519 A,2009.02.18
WO 2013009288 A1,2013.01.17
US 2006101280 A1,2006.05.11
KR 20120117063 A,2012.10.24
CN 1622647 A,2005.06.01
CN 101371603 A,2009.02.18
CN 102369767 A,2012.03.07
CN 102075870 A,2011.05.25

审查员 来文燕

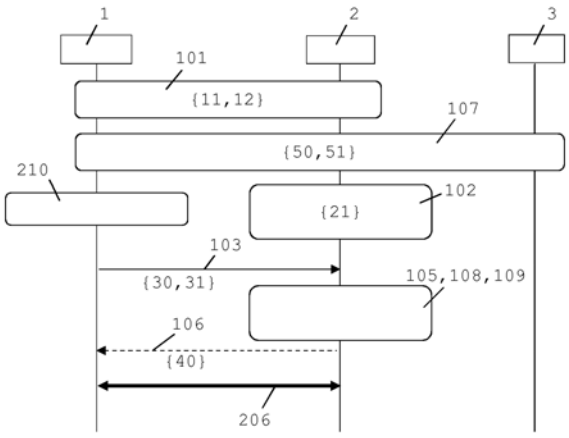
权利要求书2页 说明书13页 附图5页

(54)发明名称

3GPP LTE中的通信移动设备之间的接近发现、认证和链路建立

(57)摘要

本发明使得设备能够发现用于设备到设备模式的通信的范围内的一个或多个其它设备。该接近发现可以触发目标设备，例如以开始监听来自源设备的信号或者基于接近发现而执行任何其它动作，例如像在收费站收费。想要被发现的源设备广播包括标识符或标识符的表示的消息。该标识符可以是要联系的目标设备的标识符或源设备的标识符或其派生物或由一组对等体使用的共同安全关联。目标设备将广播标识符与已知标识符相比较以建立接近发现。



CN 110034940 B

1.一种用于源设备(1)与一个或多个目标设备(2)之间的接近发现的方法,其中源设备(1)和一个或多个目标设备(2)被配置成通信连接到网络,所述方法包括:

在源设备(1)中从网络中的服务器(3)接收(101)包括标识符(12)的第一数据(11),其中标识符(12)是唯一地标识目标设备(2)的临时广播标识符,并且其中标识符(12)可通过目标设备(2)而与源设备(1)相关联;

在目标设备(2)中从服务器(3)接收(102)包括标识符(12)的第一表示(21)的第二数据(20);

由源设备(1)广播(103)包括标识符的第二表示(31)的信号(30);

在目标设备(2)中接收(104)所述信号(30);以及

在目标设备中将标识符(12)的第一表示(21)与标识符(12)的第二表示(31)相比较(105)以获得用于建立成功的接近发现的比较结果。

2.根据权利要求1的方法,还包括从目标设备(2)向源设备(1)传送(106)取决于比较结果的确认消息(40)。

3.根据权利要求1或权利要求2的方法,其中标识符(12)、标识符(12)的第一表示(21)和标识符(12)的第二表示(31)是相同的。

4.根据权利要求1至3中任一项的方法,还包括在目标设备(2)中接收(107)包括标识符(12)的第三表示(51)的第三数据(50),其中标识符的第一表示(21)是通过第一数学函数所获得的标识符的派生物,所述第一数学函数使用标识符(12)和随机数作为输入来计算标识符的派生物,其中标识符(12)的第三表示(51)是随机数,并且其中比较步骤(105)包括:

使用与第一数学函数相同的第二数学函数来计算(108)标识符的派生物,所述第二数学函数使用标识符(12)的第二表示(31)和标识符(12)的第三表示(51)作为输入;以及

将标识符的所计算的派生物与标识符(12)的第一表示(21)相比较(109),

其中随机数为以下中的一个:

在服务器中或者在源设备(1)中所生成的随机数;

在服务器(3)中或者在源设备(1)中所生成的加盐值;

通过第三数学函数在服务器(3)中或者在源设备(1)中所获得的另外的随机数的派生物,所述第三数学函数使用另外的随机数和标识源设备(1)的源标识符作为输入来计算随机数的派生物。

5.根据权利要求1至4中任一项的方法,其中第二数据(20)还包括票据标识符(22),所述方法还包括:

在源设备(1)中从服务器(3)接收(110)包括票据标识符(22)、第一数据(11)和第四数据(13)的票据数据(10);

从目标设备(2)向服务器(3)传送(111)票据标识符(22)以获得与票据标识符(22)相关联的第四数据(13)的副本(41);以及

在目标设备(2)中从服务器(3)接收(112)第四数据(13)的副本(41),

其中确认消息(40)包括第四数据(13)的副本(41)以用于在源设备(1)中利用第四数据(13)进行验证。

6.根据权利要求1至5中任一项的方法,还包括由服务器(3)的运营商对从源设备(1)或目标设备(2)请求第一数据(11)、第二数据(20)和/或票据数据(10)进行收费。

7.根据权利要求5或权利要求6的方法,还包括:

在目标设备(2)中从源设备(1)接收(113)第一挑战数据(32);以及

在目标设备(2)中使用第四数学函数例如散列函数对第一挑战数据(32)计算(114)派生的第一挑战数据(42),

其中确认消息(40)还包括派生的第一挑战数据(42)和第二挑战数据(43),所述方法还包括:

在源设备(1)中使用与第四数学函数相同的第五数学函数对第一挑战数据(32)计算(115)派生的第一挑战数据(42),以用于与所接收的派生的第一挑战数据(42)相比较;

在源设备(1)中使用第六数学函数对第二挑战数据(43)计算(116)派生的第二挑战数据(33);

将派生的第二挑战数据(33)传送(117)给目标设备(1);

在目标设备(2)中使用与第六数学函数相同的第七数学函数对第二挑战数据(43)计算(118)派生的第二挑战数据(33),以用于与所接收的派生的第二挑战数据(33)相比较。

8.根据权利要求7的方法,其中票据数据(10)还包括加密密钥(14),其中所述方法还包括在目标设备(1)中从服务器(3)接收(119)在服务器(3)中与票据标识符(22)相关联的加密密钥(14),并且其中第四、第五、第六和第七数学函数包括使用加密密钥(14)的加密函数。

9.一种源设备(1),其被配置用于使用根据权利要求1-8中的任一项的方法来执行与一个或多个目标设备(2)的接近发现过程。

10.一种目标设备(2),其被配置用于使用根据权利要求1-8中的任一项的方法来执行与源设备(1)的接近发现过程。

11.一种网络,其包括根据权利要求9的源设备(1)和根据权利要求10的一个或多个目标设备(2)。

3GPP LTE中的通信移动设备之间的接近发现、认证和链路建立

[0001] 本申请为分案申请，其母案的发明名称为“3GPP LTE中的通信移动设备之间的接近发现、认证和链路建立”，申请日为2014年1月23日，申请号为201480018193.1。

技术领域

[0002] 本发明涉及通信设备的接近发现。更具体地，本发明涉及可以导致设立设备之间的设备到设备通信会话的设备的接近发现。

背景技术

[0003] 3GPP标准中的最近发展涉及长期演进(LTE)网络和设备。也已知为4G(即第四代)移动通信标准的LTE是针对用于移动电话和数据终端的高速数据的无线通信的标准。其是GSM/EDGE(也已知为2G或2.5G)和UMTS/HSPA(也已知为3G)的后继者，使用不同无线电接口连同核心网络改进一起增加容量和速度。最近的LTE扩展允许接着排他地在基站与移动设备之间的传统通信的、直接或者使用附近的基站作为中继站的设备到设备(D2D)通信。在LTE中，设备到设备通信也已知为LTE-Direct通信。

[0004] 用于LTE-Direct通信的用例从3GPP技术报告TR 22.803已知。在第一用例中，Alice在开会并且想要检测她的朋友Bob的接近。Alice接通针对她的朋友Bob的直接模式发现。对此，Alice的电话将消息发送给她的移动运营商以告知她想要使用直接模式并且具体地针对Bob是可发现的。移动运营商的直接模式服务器将Alice和Bob列为一对。然后，如果网络检测到Bob和Alice靠近(例如他们位于相同的网络小区中或者通过某种其它机制)，则其通知Alice和Bob并且向他们发送信息，他们可以利用该信息可靠地标识彼此而不会泄露他们的隐私。在第二用例中，涉及公共安全服务，诸如消防队、警察和急救服务。例如，进入没有覆盖的建筑物的消防员想要能够与同事交谈。在该示例中，设备可以发现彼此并且设立安全且经认证的连接。

[0005] 当诸如电话和机器类型通信(MTC)设备之类的固定和/或移动设备处于彼此的附近时，可以在设备之间设立设备到设备通信会话，例如在LTE移动设备的情况下使用LTE-Direct或者任何其它设备到设备通信标准，例如基于IEEE 802.11、IEEE 802.16、IEEE 802.20、蓝牙、Wi-Fi或WiMax。对此，设备通常检测彼此的存在并且通知用户关于另一设备的接近。

[0006] 一般而言，网络可以协助发现设备的接近。对此，网络确定两个设备可能处于彼此的附近并且将彼此的可能接近通知给相应设备。网络可能不能够确定设备还能达到，在该情况中设备必须执行更远的接近测试，例如通过广播要由其它附近设备获得的标识符。

[0007] 可替换地，接近的发现由设备直接执行。在该情况下，设备通常广播标识符并且发现广播标识符中的其它设备。已知蓝牙设备具有这样的接近发现能力。

[0008] 在任一解决方案(网络协助的或直接的接近发现)中，相应设备的标识符由相应设备广播或以其它方式传送。通常，标识符是静态的，从而使得有可能通过简单地以规则间隔

监听广播标识符来追踪单独的设备。这样的用户隐私的破坏是高度不合期望的。

[0009] 已知接近发现解决方案的另一缺陷在于,它们被用于发现单独的设备。存在针对选择可发现性解决方案的需要,其使得能够实现单独的设备的接近发现以及设备群组的接近发现二者。用户然后将能够例如调节他/她的设备的可发现性,以使得其仅针对有限数目的设备标识自身,例如在会议中仅针对同事的设备或者在流行音乐会上仅针对朋友的设备。用于设备到设备通信的范围内的其它设备优选地不应当能够了解群组中的设备的接近。

[0010] 存在针对以下解决方案的需要:其使得能够实现尊重隐私的受控无线电网络中的设备的接近发现,允许选择可发现性,并且优选地在网络负载和必要的计算功率方面具有低的分布(profile)。

发明内容

[0011] 本发明的目的是提供以下解决方案:其使得能够实现尊重隐私的受控无线电网络中的设备的接近发现,允许选择可发现性,并且优选地在网络负载和必要的计算功率方面具有低的分布。本发明对于能够进行设备到设备通信并且想要发现针对设备到设备通信会话的附近设备的设备而言尤其有用,但并不限于此。

[0012] 根据本发明的一方面,提出一种用于源设备与一个或多个目标设备之间的接近发现的方法。该方法包括在源设备中接收包括标识符的第一数据。该方法还包括在目标设备中接收包括标识符的第一表示的第二数据。该方法还包括通过源设备广播包括标识符的第二表示的信号。该方法还包括在目标设备中接收该信号。该方法还包括在目标设备中将标识符的第一表示与标识符的第二表示相比较以获得用于建立成功的接近发现的比较结果。

[0013] 由此获得的比较结果通常指示标识符的第一表示和第二表示中的标识符是否可以匹配。如果情况如此,则可以推断接近发现成功。

[0014] 代替标识符,源设备有利地广播仅指定的目标设备或目标设备群组可以涉及源设备的标识符的派生物(derivation)。由此,目标设备能够了解到谁在广播并且例如推断源设备处于靠近范围内,例如用于设备到设备通信会话的范围内,或者基于源设备处于靠近范围内而触发任何动作,例如在收费站收费。同时,源设备的身份不是可追踪的。

[0015] 在本发明的实施例中,该方法还可以包括从目标设备向源设备传送取决于比较结果的确认消息。这有利地使得源设备能够了解到目标设备处于靠近范围内。

[0016] 在另一实施例中,标识符可以是唯一地标识目标设备的临时广播标识符,并且标识符可以通过目标设备而与源设备可关联。这有利地使得源设备能够传送对于偷听者而言看起来不会链接到源设备的标识符,从而使源设备不可追踪。目标设备能够将标识符与源设备相关联。

[0017] 在另一实施例中,源设备和一个或多个目标设备可以形成设备群组并且标识符可以标识设备群组。这有利地使得能够实现目标设备群组而不仅仅是一个目标设备的接近发现。

[0018] 在另一实施例中,标识符、标识符的第一表示和标识符的第二表示可以是相同的。

[0019] 在另一实施例中,源设备和一个或多个目标设备可以被配置成通信连接到网络,并且第一数据和第二数据可以从网络中的服务器接收。可替换地,第一数据和第二数据可

以从源设备接收。这有利地使得网络能够被包含或操作在没有网络的独立模式中。

[0020] 在本发明的另一实施例中，该方法还可以包括在目标设备中接收包括标识符的第三表示的第三数据。标识符的第一表示可以是通过第一数学函数所获得的标识符的派生物，该第一数学函数使用标识符和随机数作为输入来计算标识符的派生物。标识符的第三表示可以是随机数。比较步骤可以包括使用与第一数学函数相同的第二数学函数来计算标识符的派生物，该第二数学函数使用标识符的第二表示和标识符的第三表示作为输入。比较步骤还可以包括将标识符的所计算的派生物与标识符的第一表示相比较。随机数可以是在服务器或源设备中生成的随机数。可替换地，随机数可以是在服务器或源设备中生成的加盐值(salt)。可替换地，随机数可以是通过第三数学函数在服务器或源设备中获得的另外的随机数的派生物，该第三数学函数使用另外的随机数和标识源设备的源标识符作为输入来计算随机数的派生物。

[0021] 这有利地向所交换的标识符添加晦涩难懂的水平，从而使得更难以追踪设备。

[0022] 在另一实施例中，第二数据还可以包括票据(ticket)标识符。该方法还可以包括在源设备中从服务器接收包括票据标识符、第一数据和第四数据的票据数据。该方法还可以包括从目标设备向服务器传送票据标识符以获得与票据标识符相关联的第四数据的副本。该方法还可以包括在目标设备中从服务器接收第四数据的副本。确认消息可以包括第四数据的副本以用于在源设备中利用第四数据进行验证。

[0023] 检票(ticketing)有利地使得有可能追踪接近发现尝试。追踪可以例如用于记入接近发现尝试或者对其收费。

[0024] 在另一实施例中，该方法还可以包括由服务器的运营商对从源设备或目标设备请求第一数据、第二数据和/或票据数据进行收费。这有利地使得能够对接近发现尝试进行收费，可能地仅对成功的接近发现尝试。

[0025] 在另一实施例中，该方法还可以包括在目标设备中从源设备接收第一挑战数据。该方法还可以包括在目标设备中使用第四数学函数(例如散列函数)对第一挑战数据计算派生的第一挑战数据。确认消息还可以包括派生的第一挑战数据和第二挑战数据。该方法还可以包括在源设备中使用与第四数学函数相同的第五数学函数对第一挑战数据计算派生的第一挑战数据，以用于与所接收的派生的第一挑战数据相比较。该方法还可以包括在源设备中使用第六数学函数对第二挑战数据计算派生的第二挑战数据。该方法还可以包括将派生的第二挑战数据传送给目标设备。该方法还可以包括在目标设备中使用与第六数学函数相同的第七数学函数对第二挑战数据计算派生的第二挑战数据，以用于与所接收的派生的第二挑战数据相比较。

[0026] 这有利地以挑战-响应认证的形式向标识符的交换添加安全水平。

[0027] 在另一实施例中，票据数据还可以包括加密密钥。该方法还可以包括在目标设备中从服务器接收在服务器中与票据标识符相关联的加密密钥。第四、第五、第六和第七数学函数可以包括使用加密密钥的加密函数。

[0028] 这有利地向标识符的交换添加安全水平。

[0029] 根据本发明的一方面，提出一种源设备，其被配置用于使用上述方法的一个或多个步骤来执行与一个或多个目标设备的接近发现过程。

[0030] 根据本发明的一方面，提出一种目标设备，其被配置用于使用上述方法的一个或

多个步骤来执行与源设备的接近发现过程。

[0031] 根据本发明的一方面，提出一种网络，其包括如上文所描述的源设备和如上文所描述的一个或多个目标设备。

[0032] 在此之后，将更详细地描述本发明的实施例。然而应当领会到，这些实施例可以不解释为限制本发明的保护范围。

附图说明

[0033] 将通过参照图中所示的示例性实施例更详细地解释本发明的各方面，在各图中：

[0034] 图1-6是根据本发明的示例性实施例的接近发现过程，其被可视化为源设备、目标设备以及可选地服务器之间的时序图。

具体实施方式

[0035] 在以下描述中，词语“设备”、“终端”和“用户设备(UE)”要理解为固定或移动的最终用户或MTC设备的同义词。“对等体(peer)”要理解为在设备到设备通信中可以涉及的任何固定或移动的最终用户设备。

[0036] 在设备到设备模式的通信中，设备直接通信，即不使用固定或无线网络。设备到设备通信链路可以使用基站以用于在设备之间中继信号，但是将不使用基站的网络的另外的网络功能。对等体可以连接到接着设备到设备模式的通信的无线或固定网络。

[0037] 本发明使得设备能够发现用于设备到设备模式的通信的范围内的一个或多个其它设备。该接近发现可以触发目标设备，以例如开始监听来自源设备的信号或者基于接近发现而执行任何其它动作，例如像在收费站收费。接近发现可以导致设立源设备与目标设备之间的设备到设备通信。

[0038] 设备的身份或身份的表示被交换以使得能够实现接近发现。该标识符交换以这样的方式来完成：设备不可通过对设备的传送的监听或偷听以及获得所传送的标识符而追踪。通过不可追踪，设备的用户的隐私性增加。

[0039] 为了设立具有到网络的固定或无线连接的两个或更多设备之间的设备到设备通信会话，设备可以可选地在开始接近发现过程之前通过向网络中的服务器指示其想要是可发现的或者发现某个(某组)对等体而触发其它设备。在接近发现过程之前，网络、第三方(例如顶级提供商或任何其它第三方)或设备自身通常检测对等体在附近。

[0040] 作为接近发现过程的部分，想要被发现的源设备广播包括标识符或标识符的表示的消息。该标识符可以是要联系的目标设备的标识符或源设备的标识符或其派生物或由一组对等体使用的共同安全关联。优选地，设备不会不受阻碍地广播其自身的标识符以避免设备的可追踪性。

[0041] 标识符可以是临时广播标识符(T-BID)并且可以随时间改变。T-BID可以通过由另一方供应而改变，例如通过为设备提供新标识符的网络或者通过提供新的标识符的顶级服务，即诸如Facebook、Google+或Whatsapp之类的网络的外部方。T-BID可以借助于通过网络进行(即，不使用设备到设备模式的通信)的两个设备之间的通信会话或者诸如例如WiFi、蓝牙、NFC或摄像机和屏幕通信之类的任何其它连接的而改变，例如通过使设备交换新的临时标识符或者用于计算新的临时标识符的随机值(random)/算法。T-BID可以借助于算法而

改变，例如包括时间、在两个(或更多)设备之间已经设立设备到设备连接的次数、由诸如网络运营商或顶级服务提供商之类的第三方所提供的随机值或加盐值、和/或与加密/散列标识符同时传送的随机值。

[0042] 作为接近发现过程的部分，目标设备从广播消息提取必要信息(例如通过解密、再散列或简单地与一列已知身份相比较)。源设备以仅指定的目标设备可以了解谁在广播的方式来广播其身份。

[0043] 可选地，目标设备通过将确认消息发送给源设备而做出响应：其听到另一设备并且其可用于设备到设备通信。可选确认消息可以包含针对可以包括在初始广播中的挑战的响应。可选确认消息可以包含数据，从该数据可以建立由源设备和目标设备已知共同秘密以用于认证目的。

[0044] 在成功的接近发现之后，可以在设备之间设立设备到设备连接。

[0045] 接近发现过程可以用于设立安全的设备到设备连接。可以是合期望的是验证两个设备可以彼此认证(例如以防止中间人攻击)并且网络在如何设立连接之上具有某种控制(例如以用于对接近发现进行收费)。接近发现为此可以包括三次握手过程，其可以实现如下：

[0046] 1．源设备在与T-BID相同的广播中将随机值(挑战)发送给目标设备；

[0047] 2．目标设备计算散列(挑战||共同秘密)，其中共同秘密可以是例如随机值、加盐值或共同T-BID。目标设备生成另外的随机答复，其具有包括另外的随机值||散列(挑战||共同秘密)的消息。

[0048] 3．源设备可以验证散列(挑战||共同秘密)以及具有包括散列(另外的随机值||共同秘密)的消息的答复。

[0049] 4．目标设备可以验证散列(另外的随机值||共同秘密)并且现在源设备和目标设备二者均知晓具有相同的共同秘密并且彼此认证。

[0050] 在本发明的以下示例性实施例中，将更详细地解释上文概述的接近发现过程。

[0051] 不同种类的标识符可以用于接近发现过程中，其示例为广播标识符(BID)、临时广播标识符(T-BID)、群组特定广播标识符(G T-BID)、朋友特定(临时)广播标识符(F(T)-BID)以及安全关联(临时)广播标识符(SA(T)-BID)。广播标识符是全局唯一标识符，其通过共享介质广播以宣告某一设备的存在或者呼叫某人。设备可以广播其BID派生物或者要呼叫的“朋友”/其它设备的BID。临时广播标识符是仅用于有限量时间或使用或地理位置的广播标识符。该规则的例外是其中所谓的“一次性T-BID”从T-BID得到并且作为替代地被广播。群组特定(T-)BID是适用于群组的广播标识符。这意味着群组中的所有设备监听该BID。朋友特定(T-)BID是仅在两个朋友/设备之间共享的广播标识符。安全关联(T-)BID是适用于安全关联的广播标识符。这意味着如果两个设备共享安全关联，则它们监听相同的广播标识符。

[0052] 通常，接近检测在接近发现过程之前。在接近检测阶段中，设备接收它们靠近的信息。在接近发现过程中，接收到它们靠近的信息的一个或多个设备确定设备到设备通信是否可能。存在执行接近检测的多种方式。例如，网络可以检测并且通知两个对等体靠近。这可以是有利的，首先因为设备仅在被网络所通知的情况下必须广播标识符，这导致较低的电池耗竭以及广播信道的较低使用，并且其次因为网络可以(在相同消息中)提供标识符以

及(可选地)加密材料。附加地或可替换地,顶级服务提供商或第三方通知对等体它们靠近。附加地或可替换地,用户可以激活处于彼此附近的设备。这对于以下那些情况可以是有利的:其中不存在网络覆盖并且有人想要设立设备到设备连接。在存在网络覆盖的情况下,该方法可以仍然是有利的,例如对于尚未彼此知晓的对等体而言,例如在你遇见新人并且想要交换电话号码的情况下。

[0053] 图1-6示出了本发明的示例性实施例,其中接近发现过程被可视化为源设备1、目标设备2以及可选地网络中的服务器3之间的时序图。要指出的是,可以存在多个目标设备2。箭头指示数据流。黑点指示设备处执行的工作。括号“{}”之间的参考标记指示数据元素。虚线指示可选步骤。

[0054] 在图1中,在源设备1中接收101包含标识符12的第一数据11。第一数据11可以源自外部服务器或者源自源设备1自身。在后一情况下,源设备1生成标识符12。在目标设备2中接收102包含标识符12的第一表示21的第二数据20。第二数据20可以源自外部服务器或者源自源设备1。接下来,源设备1广播103包含标识符12的第二表示31的信号103,其在目标设备2中被接收104。目标设备2将标识符12的第一表示21与标识符12的第二表示31相比较105。由此获得的比较结果指示标识符的第一和第二表示中的标识符是否可以匹配。如果情况如此,则可以推断接近发现成功,其可以可选地在确认消息40中报告106给源设备1。

[0055] 图2示出了基于票据且网络协助的实施例,其有利地使得能够通过检测票据的使用而由网络运营商对接近发现进行收费。

[0056] 在接近发现之前,源设备1通知201网络中或第三方处的服务器3其想要发现一个或多个目标设备2。网络或第三方可以知晓这些前述目标设备2中的哪些是可发现的或者能够发现并且将这些列出为对等体,例如因为设备具有网络或第三方处的订阅并且被追踪,或者因为设备通知了网络或第三方。

[0057] 服务器3为源设备1提供以票据数据10的形式的票据,其中将标识符12给予源设备1以广播103来达到其对等体2的每一个。网络3还通知源设备1的对等体2关于它们应当监听的标识符21。标识符21可以与标识符12或者标识符12的第一表示21相同。

[0058] 网络可以可选地在票据10中包括源设备1可以用来安全地设立到其对等体2之一的连接的安全关联14,例如加密密钥。类似地,网络3可能已经将安全关联14发送给目标设备2,但是从收费的角度来看,可能合期望的是一旦目标设备2请求整个票据就发送它。原因在于,在该情况下,网络可以确定成功的发现,这意味着其允许收费。可替换地,当网络3检测到两个对等体1,2靠近时,网络可以发送密钥14。在该情况下,网络3涉及接近检测或者连接的设立。这对于密钥新鲜性是有利的。此外,网络3不必针对为对等体的所有设备保持利用密钥进行登记。

[0059] 网络3可以在要接近检测时发送标识符12和/或标识符12的派生物21。

[0060] 对于其对等体2的每一个,源设备1现在具有包含以下信息的票据10:票据标识符22;可选地,要在可选的挑战响应系统中使用的共同秘密或随机值;标识符12,21,诸如第一设备1可以用来达到目标设备2的T-BID;可选地,另外的标识符13,诸如目标设备2可以在其响应中使用以达到第一设备1的T-BID。另外的标识符13在示例性实施例中还已知为第四数据。

[0061] 可选地,可以从其得到其它密钥的主加密密钥或者一组密钥(密码密钥和完整性

保护密钥)可以包括在票据数据10中。

[0062] 对等体1,2的每一个现在在存储器中具有以下信息:T-BID 12,21(或其表示)以监听源设备1并且与其相关;可选地相同的共同秘密或随机值;票据标识符22;可选地可以从其得到其它密钥的主加密密钥或者一组密钥(密码密钥和完整性保护密钥)。

[0063] 在某一随后时间点,网络或第三方/顶级提供商可以检测源设备和目标设备在附近(并且彼此仍然可发现,即没有用户改变它们的设置)。网络或第三方通知第一设备它们靠近。

[0064] 此处基于票据的系统的优点变得明显:不必是网络进行接近检测,这意味着一旦网络已经发布包括密钥14的票据10,则其可以将密钥14仅提供给目标设备2并且对源设备1开账单。

[0065] 第一设备1广播103包含早前接收的临时广播标识符的信号30或其第二表示31,其由目标设备2所接收104。

[0066] 可选地,该机制可以扩展有挑战响应系统。在该情况下,标识符31的广播103可以连同挑战32(在示例性实施例中也被称为第一挑战数据32)一起进行,目标设备2可以向其提供正确回答。

[0067] 在目标设备2接收到广播之后,其可选地使用确认消息106来向目标设备1回答它得到了消息。可选地,如上文所述的,目标设备2在接收到广播消息103时从网络检索完整票据(包括密钥)。可选地,目标设备2计算114其对挑战32的回答,可选地对其进行加密并且向第一设备1进行答复106。

[0068] 针对挑战32的回答106可以具有散列形式(挑战32||共同秘密)。在接收时,源设备1可以进行相同计算并且验证115回答是相同的。对答复也进行加密的优点在于,答复不易受散列函数上的强力或彩虹攻击。尽管在不加密的情况下解决方案仍然是安全的。

[0069] 目标设备2还可以在其答复中包括挑战43(在示例性实施例中也被称为第二挑战数据43)。这可以是由目标设备2生成的另一随机值。

[0070] 源设备可选地计算116散列(挑战43||共同秘密)并且利用该派生的第二挑战数据值33来答复117目标设备2,其继而可以验证源设备1具有正确计算的散列(挑战43||共同秘密)。基于现在均具有的安全关联,可以可选地设立安全且经认证的连接202。

[0071] 单个票据10可以多次使用,然而建议将使用限制为低次数以避免追踪广播T-BID。这意味着在T-BID的不成功广播(例如不能够达到对等体)之后,新票据10也可能必须被发行。

[0072] 可想到有人想要在不可追踪的情况下重复使用相同票据。对此除了图2之外,还可以使用图4和图6中所呈现的解决方案以及下文针对群组寻址所描述的解决方案。

[0073] 在图3和图4中所示出的网络协助的实施例中,标识符被预加载在对等体1,2中,并且将源设备1和(多个)目标设备2是对等体预先通知给网络。

[0074] 参照图2,在接近发现之前,源设备1将其想要发现一个或多个目标设备2通知给网络3。网络3知晓这些前述目标设备2中的哪些是可发现的或者能够发现并且将它们列出为对。网络因而可以检测到源设备1和目标设备2在附近并且通知它们。

[0075] 接近发现之前的这些步骤由框203指示。

[0076] 在某一指定间隔处(例如在夜晚或任何其它时间间隔期间),将可以用于针对设备

1,2的每一个的接近发现中的一组T-BID 12,21(或其它标识符12,21)给予101,102对等体1,2。对此在第一数据11中从网络在源设备1中接收101标识符12,并且在第二数据中从网络在(多个)目标设备2中接收102在该示例中可以与标识符12相同的标识符21。该示例中的T-BID12,21为对等体特定的T-BID。同样,对等体1,2被提供101,102以另一设备将使用的T-BID 12,21。可选地,对等体1,2还接收101,102通用T-BID 12,21(Gen T-BID),其可以用于设备群组的可发现性。该Gen T-BID 12,21还分发给每一成对设备。每一对等体1,2现在具有可能看起来像以下表格那样的登记(registry)(该示例对于源设备1有效):

[0077]

	广播	接收	
	T-BID	Gen T-BID	T-BID
通用 T-BID	a		
用于第一目标设备的 T-BID	b	f	j
用于第二目标设备的 T-BID	c	g	k
用于第三目标设备的 T-BID	d	h	m
用于第四目标设备的 T-BID	e	i	n

[0078] 在源设备1想要使用通用T-BID 31(即“a”)联系任何具体的目标设备2或对于任何人可发现的情况下,在表格的广播侧上的是将在信号30中从源设备1被广播103并且在目标设备2中被接收104的T-BID 31(即“b”,“c”,“d”和“e”)。在表格的接收侧上的是源设备1应当在对等体发现的情况下监听的广播。因此,如果源设备1想要达到第一目标设备2,则其应当广播103“b”。可替换地,如果源设备1想要对于具有其通用T-BID的任何人是可发现的,则其广播103“a”。在接收侧上,源设备1应当监听最后两列。如果最后一列中的任何值(“j”,“k”,“m”,“n”)被广播,则其可以推断105其对等体2之一在附近并且正尝试达到源设备1。如果中间列中的任何值(“f”,“g”,“h”,“i”)被广播,则源设备1知晓其对等体2之一在附近并且它们广播它们的通用T-BID以仅使得知晓它们存在。

[0079] 要理解,存储登记的方式是任意的。表格格式仅是示例,可以使用对值进行存储的任何其它形式。标识符12,21被呈现为字母表的字母。要理解,标识符可以具有任何长度的任何二进制值、十进制值、十六进制值、字值、双字值、字符串值等。

[0080] 图3的实施例允许简单地广播Gen T-BID 31或数个具体T-BID 31而不具有关于谁在附近的先前知识。这在对等体1,2当前不处于网络覆盖或控制之下的情况下也将工作,例如当其(可能临时)操作在自组网(ad-hoc)模式中时。

[0081] 如果安全关联在设备到设备连接206的时间点不是已知的并且期望这样的安全关联204,则网络3可以可选地向设备1,2提供加密密钥14,优选地通过安全线路。有利地,然后还将发现已经工作通知205给网络,这有利地使得能够收费。

[0082] 可以合期望的是具有改变通用BID 12,21或对等体特定T-BID 12,21的机制。例如,一旦T-BID 31已经广播103(并且独立于设备到设备会话206是否成功设立),则可能的是,恶意用户将保存该T-BID并且在将来保持寻找它。如果在任何时间点相同T-BID被再次广播,则恶意用户可以推断特定设备在附近。因此可选地可能的是,源设备1要求101a网络3更新其T-BID 12。网络3然后分配新T-BID 12并且将新T-BID 12,21通知101b,102a给对等体1,2。

[0083] 可能的是,网络在每次T-BID 12,21被用于广播中时重新分配T-BID 12,21并且将它们重新分发101b,102a给所有对等体1,2。

[0084] 接着BID和对等体特定T-BID,网络可以可选地提供具体T-BID以用于仅针对具体朋友/设备群组是可发现的。亲密用户群组特定的T-BID(GUG T-BID)因而可以针对较大群组而被限定。这样的CUG T-BID标识符优选地还提供给群组中的每一人。这对于静态的那些群组是有利的,诸如例如同事或公共安全服务,诸如警察和消防队。

[0085] 对等体特定的T-BID可以可选地在设备到设备连接期间刷新而不涉及或通知网络。这提供增加的隐私程度(网络甚至不知晓标识符12,21)并且其缓解网络生成T-BID的任务。

[0086] 在图4的实施例中,标识符12被预加载并且是静态的。然而,广播T-BID 31可以改变,例如通过网络3(在广播发生之前),其为源设备1和目标设备2提供随机值51,源设备1使用该随机值51来计算103a标识符的派生物,例如通过对标识符12进行加密或散列,并且目标设备2可以使用该随机值51来解密和验证109标识符。

[0087] 图4的实施例在快速改变群组的情况下是特别有利的,其中群组成员具有彼此的标识符,但是并非全部得到相同的随机值。

[0088] 在以下参照图4的第一示例中,在接近发现之前,对等体1,2被分配207称为p_i的T-BID(p_1用于源设备1,p_2用于第一目标设备2,p_3用于第二目标设备2等)。

[0089] 运营商3从源设备1接收其想要发现第一、第二、第三和第四目标设备2的消息101c。运营商3检测到第一、第二、第三和第四目标设备2靠近。第五和第六目标设备也可以靠近,但是不在源设备1的列表中。第五和第六目标设备因此不是要发现的。

[0090] 运营商3采用长度为p_i^2的随机数x,并且针对第一目标设备2计算:对于p_2,$x_2=x \bmod p_2$;并且对于第三目标设备2同样如此(不用于第二和第四目标设备,因为它们在该示例中未靠近)。可替换地,源设备1为运营商3提供随机数x。

[0091] 运营商3将102b x发送给源设备1。运营商3将102 x_2发送给第一目标设备2,并且将x_4发送给第三目标设备2。在本文中,x_2和x_4是标识符12的表示21。

[0092] 源设备1广播103随机值x 31,并且能达到的所有对等体2(希望地包括第一目标设备2和第三目标设备2)可以验证109 $x_i= =x \bmod p_i$是否成立。值x 31现在用作标识符的第二表示,因为其可以用于在目标设备2中验证身份。

[0093] 第一和第三目标设备2可以做出响应106:接收到消息,并且设备可以设立设备到设备通信会话,可能地使用从服务器3接收到的安全关联。

[0094] 第五和第六目标设备也将接收到随机值x 31,但是其信息非常有限(它们不接收到来自运营商3的x_i值)以至于不能查明谁在呼叫或者以至于不能使用它来追踪和跟踪。

[0095] 可能的是源设备1针对下一广播103重新使用r 31的经修改版本。这在第一设备1知晓目标设备2的p_i的值的情况下是可能的。如果其知晓,则其可以使用二者的(多个)最小公倍数(LCM)来获得针对其$x_i= =x \bmod p_i$仍然成立的新x,即x'=x+k LCM(p_2,p_3等)。在本文中,k不应当采取素数并且优选地采取素数的倍数以便防止放弃关于所使用的标识符的LCM的太多信息。该解决方案的益处在于,对于目标设备而言没有任何改变,其答复仍然相同。

[0096] 在以下参照图4的第二示例中,在接近发现之前,对等体1,2被分配207称为p_i的T-BID(p_1用于源设备1,p_2用于第一目标设备2,p_3用于第二目标设备2等)。将彼此的身份通知给对等体1,2,例如因此源设备1知晓第一目标设备2的T-BID,并且第二目标设备2知晓源设备1的T-BID。

[0097] 运营商3从源设备1接收其想要发现第一、第二、第三和第四目标设备2的消息101c。运营商3检测到第一、第二和第四目标设备2靠近。第五和第六目标设备也可能靠近，但是不在源设备1的列表中。第五和第六目标设备因此不是要发现的。

[0098] 运营商3采用随机数r，并且对于第二和第四目标设备2计算x=散列(T-BID$_{源设备1}$||r)以及再次x_i=x mod p_i。可替换地，源设备1为运营商3提供随机数r。

[0099] 运营商3将随机值r发送102b给源设备1。运营商3将(x_2,r)发送102给第一目标设备2，并且将(x_4,r)发送给第三目标设备2。在本文中，x_2和x_4是标识符12的表示21。

[0100] 源设备1广播103 x 31，并且能达到的所有对等体2(希望地包括第一目标设备2和第三目标设备2)可以验证109 x_i= =x mod p_i是否成立。值x 31现在用作标识符的第二表示，因为其可以用于在目标设备2中验证身份。

[0101] 第一和第三目标设备2可以做出响应106：接收到消息，并且通过返回在目标设备2中所计算108的散列(p_i||r)证明其可靠性。

[0102] 如之前实施例中那样，网络3可以涉及交换加密密钥14，从而提供附加安全性并且使得能够对成功的接近检测进行收费。

[0103] 图4的示例还适于以下情况：一个设备1,2想要发现仅另一个设备1,2。网络3然后仅通知这些特定对等体。

[0104] 描述了以下示例性实施例独立的接近发现过程，其中设备1,2自身决定广播什么以用于可发现性。网络3或第三方仍然可以涉及通知设备1,2关于可能的接近，例如涉及接近检测。在独立的接近发现过程中，假定之前在任何时刻已经存在联系或者已经通过其它方式交换标识符，诸如使用源设备1和目标设备2中的近场芯片(例如通过将设备1,2保持在一起并且做出摇晃手势而触发)、扫描另一设备屏幕上的条形码或标签、用户输入标识符、使用wifi、使用诸如Facebook之类的第三方应用、或者任何其它方式。

[0105] 图5示出了基于具有自动忘记选项的逆散列堆叠的独立接近发现过程。图5的示例在具有极有可能再次遇见的许多对等体1,2的环境中尤其有用。对等体1,2自身决定广播103什么并且如何加密广播信号中的标识符12的第二表示31或者使其模糊。被广播的T-BID的表示31可以随时间改变，以使得追踪和跟踪变得非常困难。

[0106] 处于设备到设备通信会话中的源设备1和目标设备2二者可以生成101随机T-BID 12和加盐值51。两个设备1,2使用将前一散列和加盐值51采取为输入的任何散列函数来递归地计算第n散列21。第一散列然后被计算为散列$_1$=散列(T-BID,加盐值)，并且随后的所有散列被计算为散列(前一散列,加盐值)。为了计算第n散列21，可以例如使用以下代码：

[0107]
```
hash1=hash(T-BID,salt);
i=2;while i<=n do {
  hashi=hash(hashi-1,salt);
}
```

[0108] 在本文中，T-BID 12是标识符12，并且T-BID的第n散列是标识符12的第一表示21，并且加盐值为标识符12的第三表示51。

[0109] 设备1,2在步骤102和107中交换其第n散列和加盐值。

[0110] 在该阶段，源设备1和目标设备2具有足够信息来在后一阶段联系彼此而不必联系网络3或任何其它第三方。

[0111] 在下一次它们靠近时(由框209所描绘的),源设备1可以将T-BID的第n-1散列31广播为T-BID的第二表示 31。目标设备2然后可以计算108散列(散列$_{n-1}$,加盐值)=前一散列。知晓散列函数的偷听者将不知晓加盐值51并且因此不能查明谁正被呼叫。

[0112] 可选地,附近的设备1,2可以在接近发现过程之前的接近检测过程中由网络3通知关于它们的接近。那样,可以避免针对持续监视广播信号的需要和相关的电池耗竭。

[0113] 因为两个设备1,2具有许多散列,所以它们可以决定针对例如每一天或者它们每一次靠近时使用不同散列。如果它们然后广播103 T-BID的第二表示31作为散列,则它们可以例如在广播信号30中包括指示它们广播了哪个散列的计数器值k。值k可以例如指示第(n-k)散列(第n减k散列)作为标识符的第二表示31被包括在广播信号30中。

[0114] 可选地,通过定时器给出k,例如基于自最后的设备到设备通信会话起经过的天数或小时数。这可以用于引入满期(expiry)方法,其将使散列堆叠在时间上减少并且最终打破两个设备1,2的“对等性”。如果设备1,2例如在其最初安全关联已经满期之后再次遇见,则它们将必须再次经历最初的接近发现过程。

[0115] 如果目标设备2必须在每一个到来的散列化T-BID 31之上计算108散列,则图5的示例性实施例可以在计算上变为高强度的。这可以通过依赖于网络3指示何时监听广播来减小。可替换地,这可以通过串联数个广播散列(因此将n-k添加给广播)来减小。以该方式,目标设备2可以检查其是否期望来自其对等体之一的第(n-k)散列并且然后决定针对到来的广播计算108(多个)(递归)散列。

[0116] 图5的接近发现过程有利地工作,即便当不存在网络覆盖(不必涉及网络)时。此外,其具有可以用于收费或订阅目的的在某一时间之后忘记对等体的机制,并且允许减少所有到来的广播103上的计算递归散列的计算负载的机制。

[0117] 作为图5的示例的变形,可能的是设备1,2自身决定使用什么随机值来加密标识符12。当标识符已经被交换(例如在接近检测过程之前或由网络提供)时,网络或第三方不必涉及建立设备到设备通信会话。该可替换过程可以如下工作。

[0118] 首先,源设备1计算随机值51并且计算散列(R||T-BID),R为随机值51,T-BID为标识符12。T-BID可以例如为对等体特定的T-BID(例如b或j,如图2的示例的表格中所示),这意味着它可以指定谁在呼叫或谁被呼叫。T-BID可以例如是安全关联T-BID(SA-T-BID),如果已经指定一个的话。

[0119] 接下来,源设备1广播R||散列(R||T-BID)。接收广播的(多个)目标设备2针对其存储器(可能地包括其自身)中的T-BID计算函数散列(R||T-BID)并且确定它们是否匹配。如果找到匹配,则可以得出的结论取决于什么T-BID被广播。如果源设备1广播表示其自身身份的T-BID,则可以由目标设备2推断源设备1能达到。如果源设备1广播表示目标设备2的身份的T-BID,则仅作为被呼叫方的目标设备2将找到与其自身身份的匹配。恶意用户仍然可以查明目标设备2正被呼叫,但是不能查明谁在呼叫。如果源设备1广播来自共同安全关联的T-BID(其可以包括源设备1和/或(多个)目标设备2的T-BID和/或T-SA-BID),则目标设备2可以确定其正被呼叫。

[0120] 图5的该变形的优点在于,源设备1自身可以确定如何使其自身被知晓并且提供高程度的隐私性,而允许网络发现谁在广播。后者针对例如收费原因或合法拦截而是有利的。另外的优点在于,不需要涉及网络并且过程因而在没有网络覆盖的情况下也工作。

[0121] 图6的示例示出混合型解决方案，其中网络或第三方提供要用于散列函数中的加盐值。图6的示例是图4和图5的示例的变形，并且在许多对等体1,2极可能再次遇见的情况下尤其有利。对等体1,2保留诸如标识符12之类的关于彼此的信息，它们可以在随后的会话中使用该信息来标识彼此或者找到下一T-BID。

[0122] 在图6的示例中，处于设备到设备会话中的两个设备1,2均生成随机T-BID。它们通知101彼此所选的T-BID 12。在预限定的时刻(例如每晚或预限定的时间间隔)，网络3(或任何其它第三方)将加盐值51分发107给设备1,2。可选地或可替换地，网络3(或第三方)可以在检测到两个设备1,2靠近并且想要交谈的时候提供107加盐值。(多个)目标设备2通过针对所有T-BID 12计算散列(T-BID,加盐值)而获得102设备1,2的已知T-BID 12的第一表示21，即如在通知步骤101中所接收到的。源设备通过计算由源设备1使用的T-BID 31的第二表示31而针对其自身的T-BID 12执行相同计算210。T-BID的第二表示31被广播103并且在(多个)目标设备2中被接收。(多个)目标设备2将所计算的T-BID的第一表示21与所接收的T-BID 12的第二表示31相比较105,108，并且验证109是否找到匹配。

[0123] 图6的示例的优点在于，其在计算上比依赖于快速改变参数(诸如接收随机值)以及在每次接收到随机值时计算散列的示例的强度更低。其仍然为标识符12的广播1提供充足的隐私性。

[0124] 图1-6示出了本发明的示例性实施例的不同示例。本发明不限于所示出的示例。在一个示例中示出的步骤可以例如用于其它示例中，尽管未示出。该示例为标识符的散列化、利用票据、附加的挑战-响应验证、以及使用加密密钥14对数据加密。所示出的其它步骤可以是可选的，诸如确认消息的传送106以及设备到设备通信会话206的建立。

[0125] 在一些示例中，散列函数用于计算标识符12的派生物21,31。要理解，可以替代地使用使用随机值51来创建派生物21,31的任何其它数学函数。随机值51可以例如是在服务器3中或源设备1中所生成的随机数或其派生物、在服务器3中或源设备1中所生成的加盐值。

[0126] 标识符12可以用于群组寻址。例如，T-BID可以用于指示设备1,2的某一群组正被呼叫。属于群组的设备1,2接收表示该群组的标识符12。为了发现其它设备，设备计算标识符12的派生物，例如取决于当前日期和/或时间或者任何其它随机值51，其可以由设备1,2共同已知而不交换随机值51。标识符的第二派生物31因而可以被计算为x=散列(日期||群组标识符)。源设备1广播103 x，并且群组的(多个)目标设备2接收x并通过执行相同计算散列(日期||群组标识符)来计算标识符的第一派生物21。如果第一派生物21与第三派生物31匹配，则接近发现成功。

[0127] 一般而言，如果随机值51是时变参数，则随机值51可以被选择成使得缓慢地改变，例如在随机值51为当前日期的情况下每天一次。在该情况下，散列(日期||群组标识符)或散列(日期||标识符)的计算可以每天仅计算一次。一旦完成该计算，则仅必须做出比较109。在图5和图6的示例中，这可能有利地导致必须执行较少的计算，原因在于其它设备的散列每天仅计算一次。

[0128] 本发明的一个实施例可以实现为用于供计算机系统使用的程序产品。程序产品的(多个)程序限定实施例的功能(包括本文所描述的方法)并且可以包含在各种非暂时性计算机可读存储介质上。说明性的计算机可读存储介质包括但不限于：(i)在其上永久地存储

信息的不可写存储介质(例如计算机内的只读存储器设备,诸如由CD-ROM驱动器可读的CD-ROM盘、ROM芯片或任何类型的固态非易失性半导体存储器);以及(ii)在其上存储可变更信息的可写存储介质(例如闪速存储器、磁盘驱动器或硬盘驱动器内的软盘、或者任何类型的固态随机存取半导体存储器)。

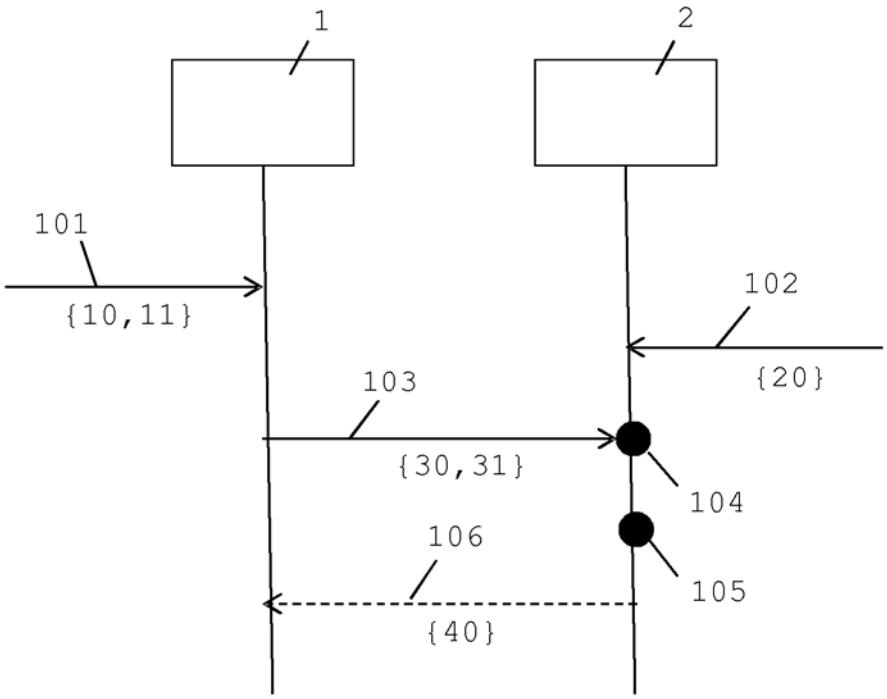


图 1

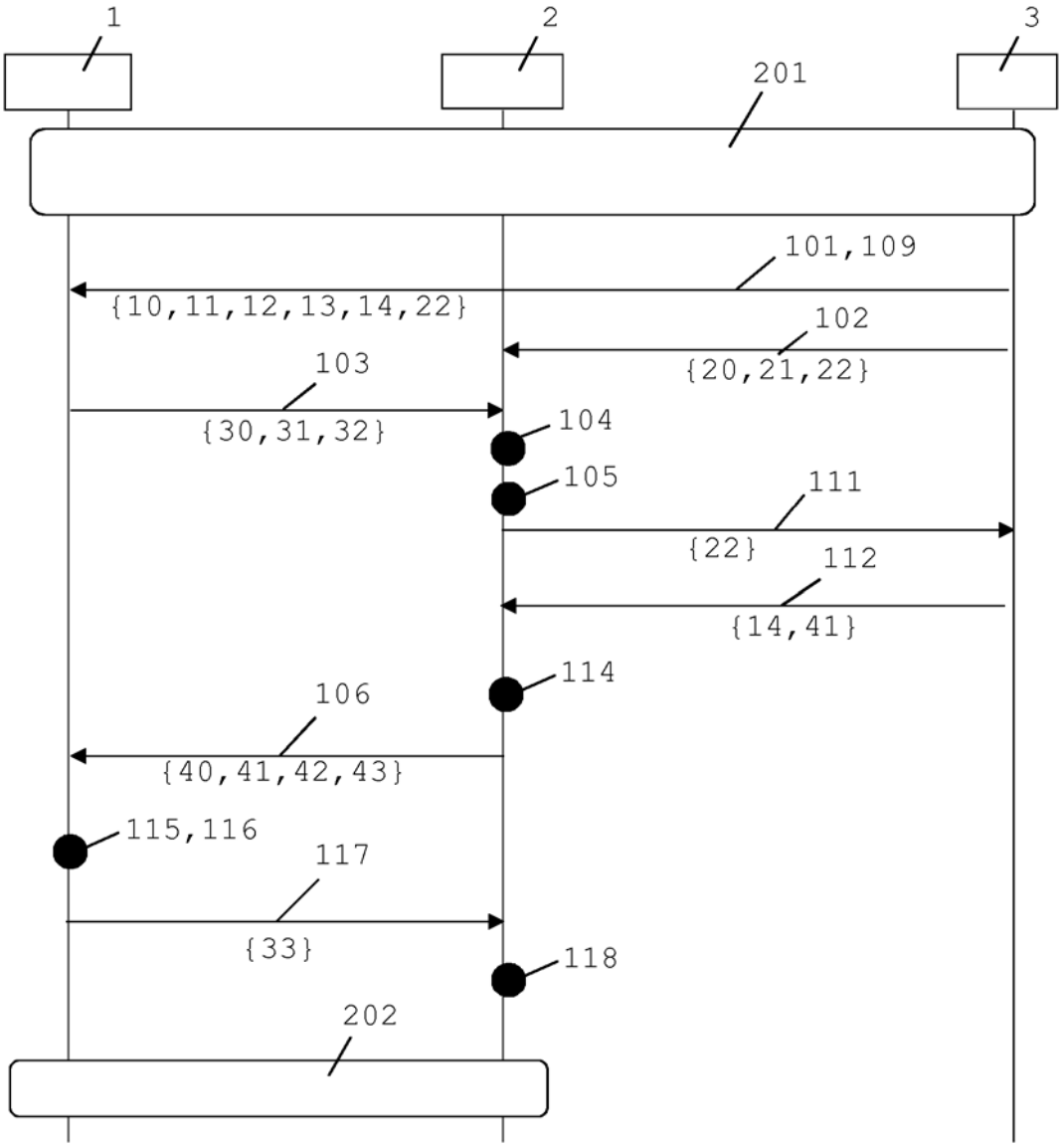

1
2
3
201
101,109
{10,11,12,13,14,22}
102
{20,21,22}
103
{30,31,32}
104
105
111
{22}
112
{14,41}
114
106
{40,41,42,43}
115,116
117
{33}
118
202

图 2

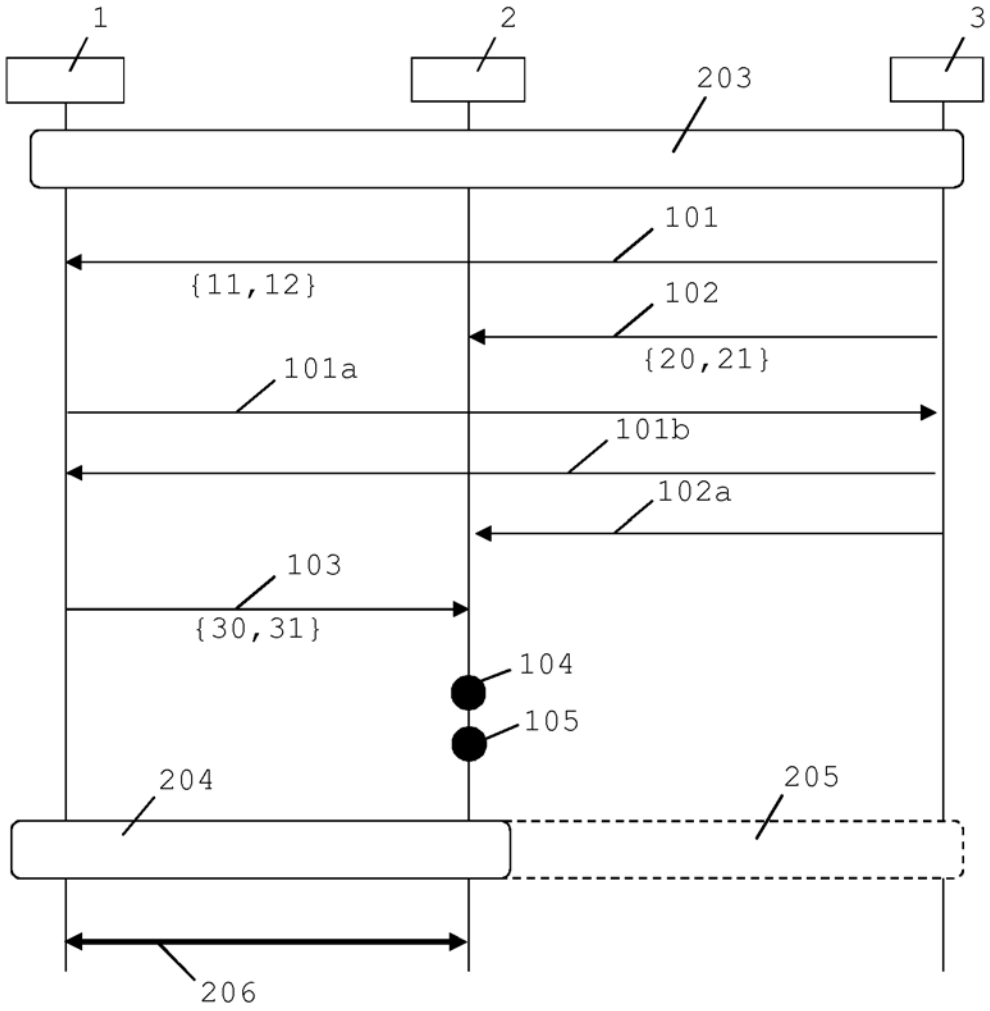

1
2
3
203
101
{11,12}
102
{20,21}
101a
101b
102a
103
{30,31}
104
105
204
205
206

图 3

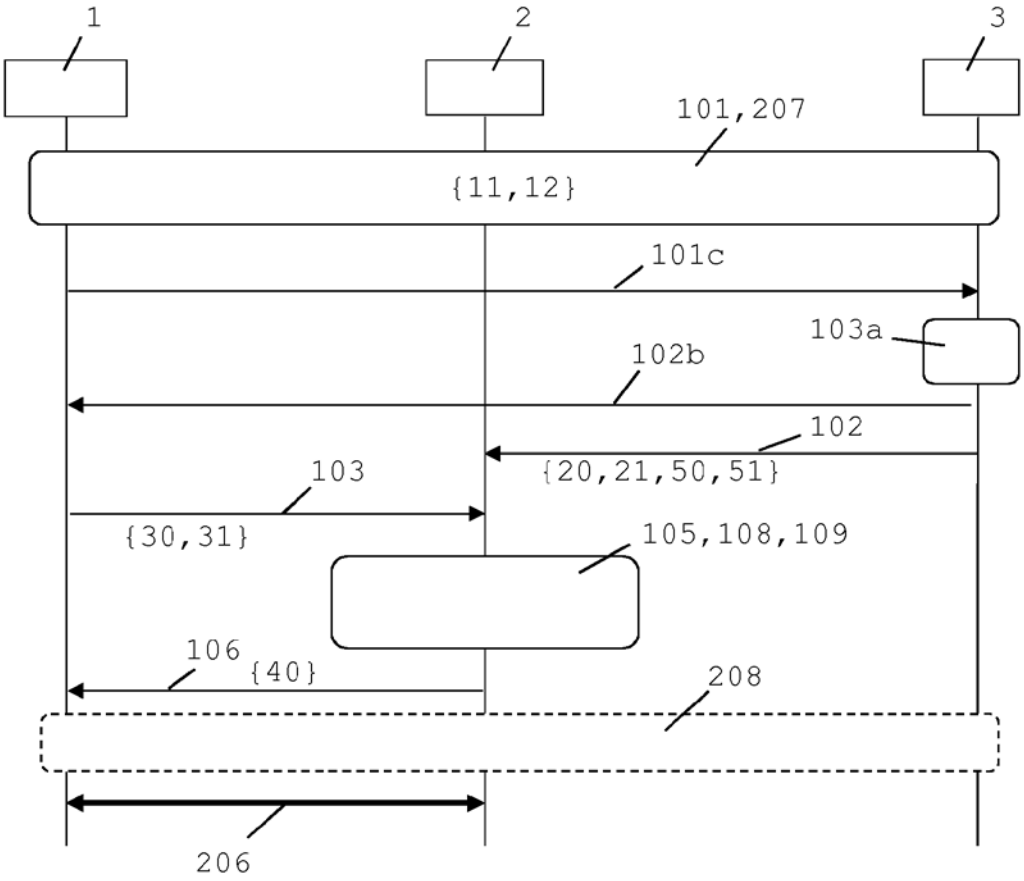

1
2
3
101,207
{11,12}
101c
103a
102b
102
{20,21,50,51}
103
{30,31}
105,108,109
106
{40}
208
206

图 4

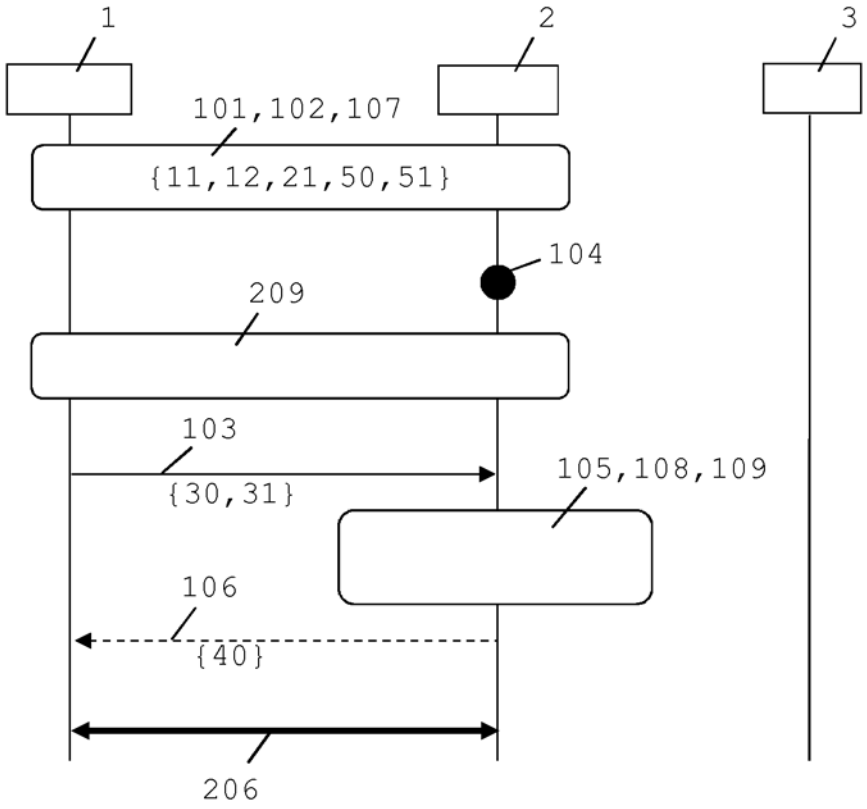

1
2
3
101,102,107
{11,12,21,50,51}
104
209
103
{30,31}
105,108,109
106
{40}
206

图 5

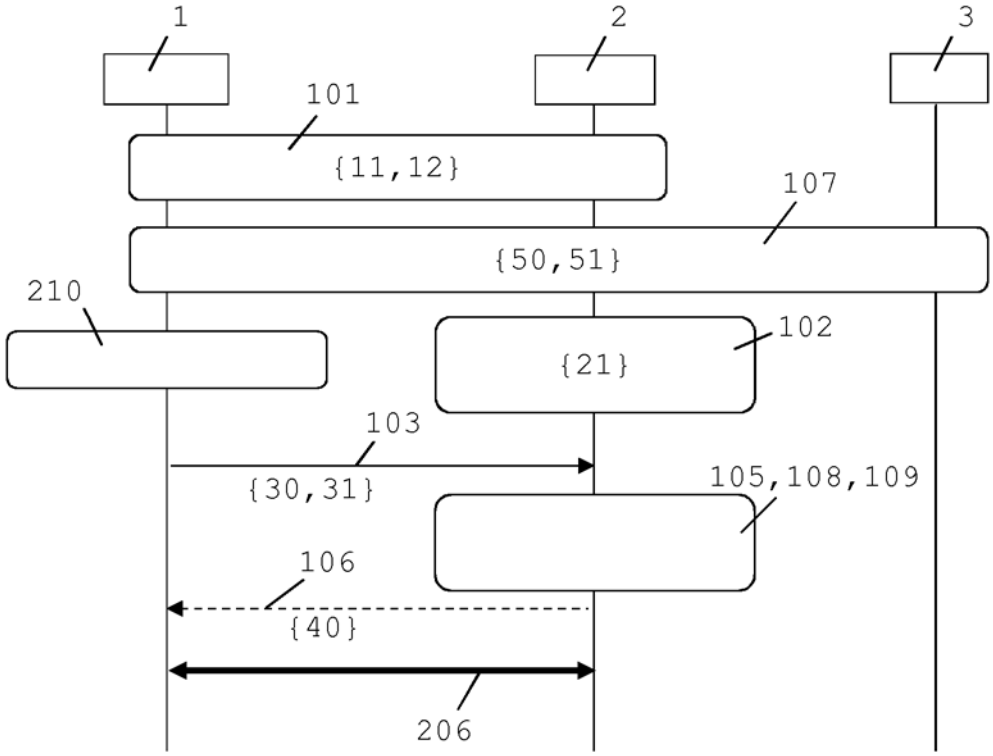

1
2
3
101
{11,12}
107
{50,51}
210
102
{21}
103
{30,31}
105,108,109
106
{40}
206

图 6