(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 103548308 B
(45)授权公告日 2017.03.22

(21)申请号 201280025187.X
(22)申请日 2012.04.26
(65)同一申请的已公布的文献号
申请公布号 CN 103548308 A
(43)申请公布日 2014.01.29
(30)优先权数据
13/114,013 2011.05.23 US
(85)PCT国际申请进入国家阶段日
2013.11.22
(86)PCT国际申请的申请数据
PCT/US2012/035281 2012.04.26
(87)PCT国际申请的公布数据
WO2012/161919 EN 2012.11.29
(73)专利权人 波音公司
地址 美国伊利诺伊州
(72)发明人 G·M·格特 A·阿亚加里
D·A·维兰 D·G·劳伦斯
(74)专利代理机构 北京纪凯知识产权代理有限公司 11245
代理人 赵蓉民
(51)Int.Cl.
H04L 12/701(2013.01)
H04L 29/06(2006.01)
H04L 29/08(2006.01)
H04W 4/04(2009.01)
H04W 12/12(2009.01)
(56)对比文件
US 2005074033 A1,2005.04.07,
US 6240074 B1,2001.05.29,
US 2002068584 A1,2002.06.06,
US 2005074033 A1,2005.04.07,
S.Kent, Network Working Group.IP Authentication Header.《IP Authentication Header ;rfc4302》.2005,
审查员 于兰

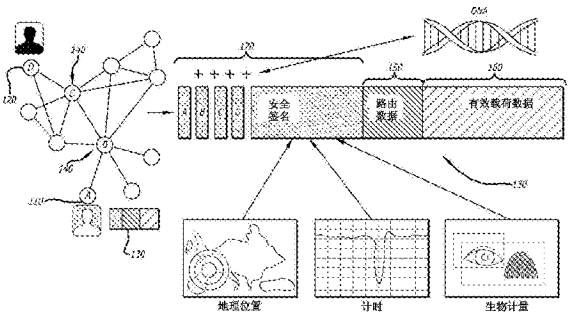
权利要求书2页 说明书11页 附图9页

(54)发明名称

针对计算机和网络安全应用在衰减环境中地理定位网络节点

(57)摘要

公开了针对计算机和网络安全应用在衰减环境中验证和/或地理定位网络节点的系统和方法。该系统涉及起始网络节点、目的地网络节点和至少一个路由器网络节点。起始网络节点被配置为通过至少一个路由器网络节点将数据包传输到目的地网络节点。数据包包含安全签名部分、路由数据部分和有效载荷数据部分。安全签名部分包含至少一个网络节点的列表，数据包从起始网络节点通过该至少一个网络节点传送到目的地网络节点。此外，安全签名部分包含列表中的至少一个网络节点的地理位置信息、标识符信息和计时信息。



CN 103548308 B

1.一种针对计算机和网络安全应用在衰减环境中验证网络节点的系统，所述系统包含：

起始网络节点；

目的地网络节点；以及

至少一个路由器网络节点；

其中所述起始网络节点和所述目的地网络节点通过所述至少一个路由器网络节点彼此相连；

其中所述起始网络节点被配置为通过所述至少一个路由器网络节点将数据包传输到所述目的地网络节点；

其中所述数据包包含安全签名部分、路由数据部分和有效载荷数据部分，以及

其中所述安全签名部分包含至少一个网络节点的列表，数据包从所述起始网络节点通过所述至少一个网络节点行进到所述目的地网络节点，并且所述安全签名部分包含所述列表中的所述至少一个网络节点的标识符信息。

2.根据权利要求1所述的系统，其中所述安全签名部分包含：

所述列表中的所述至少一个网络节点的计时信息，该计时信息表明所述数据包何时被所述至少一个网络节点接收。

3.根据权利要求1所述的系统，其中所述安全签名部分包含所述列表中的所述至少一个网络节点的地理位置信息，所述地理位置信息通过所述网络节点接收从至少一个发射源发射的合成信号而获得，

其中所述合成信号包含至少一个认证信号，以及

其中通过比较所述网络节点接收的所述合成信号的属性与所述网络节点因其位置而应当接收的所述合成信号的期望属性，从而验证所述网络节点位置。

4.根据权利要求3所述的系统，其中根据测距信息确定所述地理位置信息，所述测距信息通过由所述网络节点传输到在已验证的位置处的另一网络节点的信号以及由所述网络节点从在已验证的位置处的所述网络节点接收的信号获得。

5.根据权利要求1所述的系统，其中所述路由数据部分包含所述数据包的路由信息，

其中所述路由信息包含关于所述数据包将被发送到的所述目的地网络节点的信息。

6.根据权利要求1所述的系统，其中所述有效载荷数据部分包含被从所述起始网络节点传输到所述目的地网络节点的数据。

7.一种针对计算机和网络安全应用在衰减环境中验证网络节点的方法，所述方法包括：

起始网络节点通过至少一个路由器网络节点将数据包传输到目的地网络节点，

其中所述起始网络节点和所述目的地网络节点通过所述至少一个路由器网络节点彼此相连，

其中所述数据包包含安全签名部分、路由数据部分和有效载荷数据部分，以及

其中所述安全签名部分包含至少一个网络节点的列表，所述数据包从所述起始网络节点通过所述至少一个网络节点行进到所述目的地网络节点。

8.根据权利要求7所述的方法，其中所述安全签名部分包含所述列表中的所述至少一个网络节点的计时信息，所述计时信息表明所述数据包何时被所述至少一个网络节点接

收。

9.根据权利要求7所述的方法，其中所述安全签名部分包含所述列表中的所述至少一个网络节点的标识符信息。

10.根据权利要求9所述的方法，其中所述标识符信息是生物计量信息和比特序列识别码中的至少一个。

11.根据权利要求7所述的方法，其中所述安全签名部分包含所述列表中的所述至少一个网络节点的地理位置信息。

12.根据权利要求11所述的方法，其中通过所述网络节点接收从至少一个发射源发射的合成信号来获得地理位置信息，

其中所述合成信号包含至少一个认证信号，以及

其中通过比较所述网络节点接收的所述合成信号的属性与所述网络节点因其位置而应当接收的所述合成信号的期望的属性，从而验证所述网络节点位置。

13.根据权利要求12所述的方法，其中所述至少一个发射源是卫星、伪卫星和地面发射源中的至少一个。

14.根据权利要求11所述的方法，其中根据测距信息确定所述地理位置信息，所述测距信息通过由所述网络节点传输到已验证的位置处的另一网络节点的信号和由所述网络节点从已验证的位置处的所述网络节点接收的信号获得。

15.根据权利要求7所述的方法，其中所述路由数据部分包含所述数据包的路由信息，

其中所述路由信息包含关于所述数据包将被发送到的所述目的地网络节点的信息。

16.根据权利要求7所述的方法，其中所述有效载荷数据部分包含被从所述起始网络节点传输到所述目的地网络节点的数据。

针对计算机和网络安全应用在衰减环境中地理定位网络节点

技术领域

[0001] 本发明涉及地理定位网络节点。特别地，本发明涉及针对计算机和网络安全应用在衰减环境中地理定位网络节点。

发明内容

[0002] 本发明涉及用于针对计算机和网络安全应用在衰减环境中验证及/或地理定位网络节点的方法、系统和装置。特别地，本发明教导涉及起始网络节点和目的地网络节点的系统。该系统进一步涉及至少一个路由器网络节点。此外，该系统涉及通过至少一个路由器网络节点彼此连接的起始网络节点和目的地网络节点。而且，该系统涉及被配置以通过至少一个路由器网络节点将数据包传输到目的地网络节点的起始网络节点。另外，该系统涉及包含安全签名部分、路由数据部分和有效载荷数据部分的数据包。

[0003] 在一个实施例中，现有的基础架构能够采用所述方法，然而，考虑到互联网工程任务组(IETF)互联网协议(IP)网络协议及其在路由器中的实现，该方法需要额外的工作。对现有的已部署的基础架构来说，使用已启用硬件的相互关联的路由器网络被用于管理控制平面，标志该管理控制平面可以有效地允许对流量的具体级别将要执行的追踪和跟踪方法，同时允许正常的数据平面流量采用存在快速路径转发的标准。例如，可以将具有已知路由的具体控制平面网络管理包作为相同的对等路由器(peer router)之间的数据平面IP网络流量的特定级别而插入具有相同路由的控制平面网络管理包中。这允许利用如合适的分析学的要素形成的方案，例如用于网络属性和决策支持引擎的事件关联引擎，其可以被部署在控制平面上的现有和未来部署的基础架构上，同时与IETF RFC完全兼容。包含数据包的所列要素现在将通过控制平面数据和数据平面流来表达，并且其可以被假定为遵循当前的处理和转发机制。

[0004] 在一个或更多实施例中，安全签名部分包含数字签名。在一些实施例中，安全签名部分包含至少一个网络节点的列表，通过该网络节点，将数据包从起始网络节点传送到目的地网络节点。在至少一个实施例中，安全签名部分包含列表中的至少一个网络节点的计时信息，其表明数据包何时被该(一个或多个)网络节点接收和/或传输。在一些实施例中，安全签名部分包含列表中的至少一个网络节点的标识符信息。在一个或更多实施例中，标识符信息是生物计量信息和/或比特序列标识码。

[0005] 在至少一个实施例中，安全签名部分包含列表中的至少一个网络节点的地理定位信息。在一个或更多实施例中，通过网络节点接收从至少一个发射源发射的合成信号来获得地理定位信息。所述合成信号包含至少一个认证信号。通过比较网络节点接收的合成信号的属性和该网络节点由于其位置而应当接收的合成信号的期望属性，来验证网络节点位置。在一些实施例中，至少一个发射源是卫星、伪卫星和/或地面发射源。在至少一个实施例中，卫星是近地轨道(LEO)卫星、中地轨道(MEO)卫星或同步地球轨道(GEO)卫星。

[0006] 在至少一个实施例中，可以使用安全网络服务器来周期性地验证已启用的参与路由器的位置，从而代替被附加到每个数据包的地理定位数据。具有已启用设备的终端用户

可以通过周期性地与安全网络服务器进行校验来验证路由路径，以确保路由器的位置在该路径中。由于每个路由器可以具有其自己的密钥，只要密钥没有受损，则该密钥可以代替向每个数据包添加地理定位数据来使用或与其结合使用。

[0007] 在一个或更多实施例中，所公开的系统采用铱LEO卫星星座，其中星座中的每个卫星都具有发射四十八(48)个点波束的天线阵型，该48个点波束具有不同的点波束图案。在至少一个实施例中，至少一个认证信号可以从星座中的至少一个铱卫星发射。可以使用铱卫星的四十八(48)个点波束来将本地化的认证信号传输到位于或靠近地球表面的网络节点。与这些认证信号相关联的所广播的消息脉冲串内容包含伪随机噪声(PRN)数据。由于给定的消息脉冲串可以在具体的时间出现在具体的卫星点波束内，因此可以使用包含PRN和独特的波束参数(例如，时间、卫星标识符(ID)、时间偏置、轨道数据等)的消息脉冲串内容来认证网络节点的位置。应当注意，当采用如上所描述的一个铱LEO卫星时，发射信号功率足够强以允许该信号穿透到室内环境中。这允许对认证技术的许多室内应用使用所公开的系统。

[0008] 在一个或更多实施例中，根据该测距信息确定地理位置信息，该测距信息由所述网络节点传输到已验证的位置处的另一网络节点的信号和所述网络节点从已验证的位置处的所述网络节点接收的信号获得。在至少一个实施例中，所公开的系统利用网络级的原理为每服务质量(QoS)流基础上的互联网IP流量测距。在至少一个实施例中，路由数据部分包含数据包的路由信息，其中路由信息包含关于数据包将被发送到的目的地网络节点的信息。在一个或更多实施例中，有效载荷数据部分包括被从起始网络节点传输到目的地网络节点的数据。

[0009] 在至少一个实施例中，用于针对计算机和网络安全应用在衰减环境中验证和/或地理定位网络节点的方法涉及起始网络节点通过至少一个路由器网络节点将数据包传输到目的地网络节点。起始网络节点和目的地网络节点通过至少一个路由器网络节点彼此连接。数据包包括安全签名部分、路由数据部分和有效载荷数据部分。

[0010] 在一个或更多实施例中，用于计算机和网络安全应用的网络节点设备涉及接收器和处理器。接收器能够从信号源接收信号。处理器能够将关于所述信号的信息作为安全签名附加到通过网络节点设备被路由的数据包上。

[0011] 在至少一个实施例中，用于计算机和网络安全应用的认证系统涉及网络节点设备和处理设备。网络节点设备包含能够从信号源接收信号的接收器和能够将关于所述信号的信息作为安全签名附加到通过网络节点设备路由的数据包上的处理器。处理设备能够比较通过网络节点设备被路由的数据包的安全签名和该网络节点设备所接收的关于所述信号的已知信息，从而认证网络节点设备。

[0012] 在一个或更多实施例中，网络节点设备的认证至少部分地包含确定该网络节点设备是否物理地位于其预期的地理位置中。在至少一个实施例中，在数据被授权通过之前，认证网络节点设备。在一些实施例中，处理设备是蜂窝电话、个人数字助理(PDA)、个人计算机、计算机节点、互联网协议(IP)节点、服务器、Wi-Fi节点和/或系绳/接触式节点或自由/非接触式节点。

[0013] 此外，本发明涉及用于利用保护点波束来认证网络节点的位置的方法、系统和装置。特别地，本发明教导用于基于传输的认证系统的方法来验证网络节点的地理位置信息。

在一个或更多实施例中，所公开的方法涉及从至少一个发射源发射认证信号和至少一个保护信号。该方法进一步涉及从至少一个接收源接收至少一个合成信号。至少一个合成信号包含认证信号和/或至少一个保护信号。另外，该方法进一步涉及通过评估至少一个网络节点从至少一个接收源接收的至少一个合成信号，而通过至少一个认证器设备来认证该网络节点。在至少一个实施例中，至少一个网络节点被实体和/或用户使用。

[0014] 在一个或更多实施例中，从相同的发射源发射认证信号和至少一个保护信号。在至少一个实施例中，从不同的发射源发射认证信号和至少一个保护信号。在一些实施例中，在相同的频率上发射认证信号和至少一个保护信号。在可替换的实施例中，在不同频率上发射认证信号和至少一个保护信号。

[0015] 在至少一个实施例中，通过至少一个保护信号传输的数据可以被用于合法的目的。在一个或更多实施例中，至少一个保护信号至少部分地包含认证信号。在各种实施例中，保护信号可以包含认证信号和/或数据，其可以是合法的或错误的。在一些实施例中，通过至少一个保护信号传输的数据包含本地化信息和/或区域性信息。

[0016] 在一个或更多实施例中，通过保护信号传输的数据能够被位于该信号的重叠区域内的网络节点接收。在一些实施例中，数据通过至少两个异相的二进制相移键控(BPSK)信号传输，其中异相的BPSK信号看起来是至少一个四进制相移键控(QPSK)信号。在至少一个实施例中，至少一个保护信号的比特流的调制的变化在逐比特基础上修改比特流中比特的广播功率。在一些实施例中，当发射至少两个保护信号时，保护信号的相对功率是变化的，使得比起定位为更远离认证信号的保护信号，定位为更接近认证信号的保护信号具有更高的功率。

[0017] 此外，本发明教导了基于传输的认证系统，从而验证网络节点的地理位置信息。在一个或更多实施例中，所公开的系统包括至少一个发射器、至少一个接收器和至少一个认证器设备。在一个或更多实施例中，至少一个发射器发射认证信号和至少一个保护信号；并且至少一个接收器接收至少一个合成信号。至少一个合成信号包含认证信号和/或至少一个保护信号。在至少一个实施例中，至少一个认证器设备通过评估至少一个网络节点从至少一个接收器接收的至少一个合成信号来认证该至少一个网络节点。应当注意，在一个或更多实施例中，所述系统还包括计算机定位门户(cyber locate portal)。该计算机定位门户是网络与将额外的安全等级添加到所述系统的认证器设备之间的安全接口。在这些实施例中，通过计算机定位门户将合成信号发送到认证器设备以进行认证。

[0018] 在一个或更多实施例中，认证数据被加密以避免被拦截和重复使用。此外，可以用签名对数据进行标记，通过比较数据的签名与具体的门户设备的签名，可以用该签名来确认数据来源于所述具体的门户设备。每个计算机定位门户设备可以具有用于加密的独特的密钥，并且可以具有用于标记样本数据的额外的密钥。优选为只有认证服务器和门户设备知道这些密钥。

[0019] 在至少一个实施例中，至少一个接收器和至少一个发射器被合并在至少一个收发器中。在一些实施例中，从相同的发射器发射认证信号和至少一个保护信号。在至少一个实施例中，从不同的发射器发射认证信号和至少一个保护信号。在一个或更多实施例中，至少一个认证器设备包含服务器和/或处理器。在一些实施例中，在相同的频率上发射认证信号和至少一个保护信号。

[0020] 在至少一个实施例中，至少一个认证器设备操作主机网络的至少部分。在一个或更多实施例中，所公开的系统进一步包含作为至少一个网络节点和至少一个认证器设备之间的中介操作的主机网络。在一些实施例中，在蜂窝电话、个人数字助理(PDA)、个人计算机、计算机节点、互联网协议(IP)节点、服务器、Wi-Fi节点和/或系绳/接触式节点或自由/非接触式节点中采用至少一个接收器。

[0021] 在一些实施例中，接收器也可以包含计算机定位门户设备的功能。在一些实施例中，将接收器和计算机定位门户设备结合在蜂窝电话或PDA中。注意，如果蜂窝电话或PDA包含计算机定位门户设备，则理想地，可以由不是蜂窝电话或PDA的操作系统的一部分的硬件和/或固件执行信号处理、加密和签名功能。例如，可选地，加密和签名密钥以及未加密的样本数据不可被蜂窝电话或PDA操作系统访问。

[0022] 在一个或更多实施例中，在至少一个卫星和/或至少一个伪卫星中采用至少一个发射器。在一些实施例中，至少一个卫星是近地轨道(LEO)卫星、中地轨道(MEO)卫星和/或同步地球轨道(GEO)卫星。在一个或更多实施例中，至少一个网络节点是固定的和/或移动的。在至少一个实施例中，至少一个认证器设备是对等设备。

[0023] 在一个或更多实施例中，用于基于传输的认证系统的方法涉及从至少一个发射源发射多个认证信号。该方法进一步涉及从至少一个接收源接收包括至少两个认证信号的合成信号。此外，该方法涉及通过比较(一个或多个)网络节点从(一个或多个)接收源位置接收的合成信号的属性与该(一个或多个)网络节点应当从(一个或多个)接收源位置接收的合成信号的期望属性，而通过至少一个认证器设备认证至少一个网络节点。

[0024] 在一个或更多实施例中，用于基于传输的认证系统的系统和方法包括从至少一个发射源发射点波束中的多个认证信号，其中每个点波束包含一个认证信号。在至少一个实施例中，在来自铱卫星星座的至少一个LEO卫星中采用(一个或多个)发射源。在一些实施例中，在相同频率上发射认证信号。该方法进一步包括从至少一个接收源接收包括至少两个认证信号的合成信号。此外，该方法包括通过比较(一个或多个)网络节点从(一个或多个)接收源位置接收的合成信号的属性与该(一个或多个)网络节点应当从(一个或多个)接收源位置接收的合成信号的期望属性，从而认证至少一个网络节点。

[0025] 在至少一个实施例中，从相同的发射源发射认证信号。在可替换的实施例中，从不同的发射源发射认证信号。在一些实施例中，至少一个卫星和/或至少一个伪卫星采用(一个或多个)发射源。在一个或更多实施例中，在相同的频率上并且同时发射认证信号，并且每个认证信号具有不同于其它认证信号的调制。在至少一个实施例中，不同的调制是不同的伪随机数字调制序列。在一些实施例中，不同的伪随机数字调制序列是不同的BPSK码序列。

[0026] 在一个或更多实施例中，所比较的属性是信号功率、多普勒位移、到达时间和/或信号调制。特别地，所接收的信号调制是多个认证信号的组合，并且该合成的组合调制具有将随接收源的位置而改变的特性。在一些实施例中，所公开的系统和方法涉及包括但不限于自组织网络、对等(peer-to-peer)网络和/或点对点(ad hoc)网络等网络的网络安全。

[0027] 特征、功能和优势能够在本发明的各实施例中独立地实现，或者可以在其它实施例中组合实现。

附图说明

[0028] 考虑到下列说明、所附权利要求以及附图将更好地理解本发明的这些和其它特征、方面和优势，其中：

[0029] 图1说明了用于针对计算机和网络安全应用在衰减环境中地理定位网络节点的公开的系统的实施例。

[0030] 图2说明了通过基于传输的认证系统以及通过使用测距信息而验证的三个网络节点的位置。

[0031] 图3说明了采用卫星来发射认证波束和多个保护波束的基于传输的认证系统的实施例。

[0032] 图4A说明了具有位于三个重叠的点波束之内和附近的不同位置处的四个网络节点的基于传输的认证系统的实施例。

[0033] 图4B说明了通过图4A的三个点波束传输的信号的图形的实施例。

[0034] 图4C说明了图4A的四个网络节点的位置处的三个点波束的信号强度的阵列的实施例。

[0035] 图4D说明了图4A的三个点波束的比特的阵列的实施例。

[0036] 图4E说明了由图4A的四个网络节点接收的合成信号序列的阵列的实施例。

[0037] 图4F说明了描述由图4A的四个网络节点接收的合成信号的图形的实施例。

[0038] 图5说明了利用保护波束传输作为辅助任务的一部分的基于传输的认证系统的实施例。

[0039] 图6说明了采用异相的二进制相移键控(BPSK)保护波束传输的基于传输的认证系统的实施例。

[0040] 图7说明了具有能够在闭塞或拥挤的环境中执行的网络节点的所公开的系统的实施例。

具体实施方式

[0041] 本文所公开的方法和装置为地理定位网络节点提供了操作系统。具体地，该系统涉及针对计算机和网络安全应用在衰减的环境中地理定位网络节点，例如用于网络节点的认证和/或授权。特别地，本发明教导了用附加的认证数据标记传输的数据包的参与网络节点或网络链中的其它结点。该认证数据具有具体的数据包结构，该数据包结构包含独特的数据，例如安全签名数据、路由数据和/或有效载荷数据。安全签名数据包含关于网络链中的参与网络节点的位置的信息，并且其也可以包含关于网络链中的参与网络节点的位置是否已经被验证的信息。

[0042] 目前，随着电子系统在日常商业和社交任务中更加根深蒂固，计算机安全变得越来越重要。许多以前管理的商业处理已经被扩展到在线电子数据处理，这使不断发展的信息和计算安全高级技术成为必须的要求，从而保护这些每天使用的系统。使用从社会安全号(social security number)到国家基础设施相关信息的信息的重要文件和其它数据被存储在网络化的系统中，如果该系统被未授权方访问，则该系统将具有从妨害行为到灾难性的社会基础设施损坏的不同程度的社会影响。在对电子系统的依赖增加的同时，国家也

已经看到了恐怖行为和计算机黑客的显著增加，因此要求社会致力于改进方法来保护我们网络化的计算机系统。

[0043] 计算机攻击和网络渗透都在变得非常普遍。这些频繁发生的事件已经由商业和军事环境中的外部威胁将网络渗透的危害的讨论带至最前沿。目前的访问控制方法主要是基于静态密码，或者是以使用基于公共密钥基础设施(PKI)的密码和智能标志证书为基础的认证。由于系统攻击通常通过冒充终端用户进行，因此机构关注于用户认证方法以减少网络数据拦截的网络漏洞已经成为一种趋势。这些方法对复杂的攻击仍然是脆弱的，因此形成了对访问控制的新范式的需求，该新范式的优势在于通过添加地理空间位置/环境(例如用户位置)的认证的正常的三个维度(你知道什么、你具备什么、你是谁)之外的额外的维度/信息，从而提供额外和正交的保护层，其提供了来自映射到逻辑网络和信息管理视图的综合物理地理位置的位置和环境感知之间的加强的相关性。

[0044] 此外，现有的计算机攻击经常被匿名所掩盖的事实已经产生了另外令人担忧的问题。发起者进行小的侵入/攻击以更好地了解系统的漏洞，以便于日后的开发并为以后的更具破坏性的攻击奠定基础，更大的攻击通常被发起者的这些尝试所阻止。到目前为止，许多大规模的计算机攻击不仅使攻击的受害者仍在从遗留的损害中恢复，而且这些受害者也不能阻止通过报复的任何进一步的破坏，或否则，由于不具有对攻击的发起者的清晰的追踪性，并且因此这些受害者往往缺乏响应的权限。如果攻击动机不清楚，则受害者更不可能辨别攻击是单纯的破坏行为、有目的的盗窃还是危害国家安全的更阴险的手段。这样，帮助拒绝恶意用户的网络访问和/或提供可追踪的数据来帮助识别发起者的任何系统将具有极大的用途，以减少和减轻拒绝服务(DoS)和网络数据拦截攻击。

[0045] 本发明总体涉及从计算机安全中受益的网络化系统。更具体地，本发明的系统的优势在于至少一个自地理定位的网络节点，从而采用签名包结构，该签名包结构可允许数据包被及时追溯到定义的点处的具体的网络节点。该签名包结构能够被用来提高参与网络中的计算机安全。作为示例，签名包结构可以包括要素，如有效载荷数据、路由数据和/或安全数据。安全数据可以被定义为地理定位数据、生物计量数据和/或计时数据。在至少一个实施例中，当签名包结构被用于计算机安全应用时，其可以被统称为计算机安全签名。例如，通过连接可以将文件从一个用户传输给另一用户，所述文件例如通过互联网传输的邮件。网络链中的参与网络节点或其它类型的结点可以用附加的认证数据标记数据，该认证数据可以包含签名包结构的要素(例如，有效载荷数据、路由数据和/或安全数据)。当数据包移动到网络链中的下一个结点时，该网络结点可以对其进行认证。当用已知的网络节点位置验证了通过地理位置数据表示的物理位置时，可以发生认证。

[0046] 本发明可以被用来提供到网络化系统的访问，也可以被用来限制到这个系统的访问。在至少一个实施例中，可以设想，优势在于这种形式的计算机安全的网络会需要这样的计算机安全签名数据，从而接受数据包。通过这种方式，可以在恶意用户进入系统前将其识别，因为签名几乎是无法假冒的，或者中间人或其它相似的攻击被识别为与签名数据不符。在至少一个实施例中，所述系统可以包含现有的追溯方法，例如限制节点跳转的次数(即，数字计数器生存时间(TTL))。在计算机安全方面，本发明可以引入范式转移(即互联网3.0)，这可以使得能够支持签名包数据结构的众多硬件和/或软件采用本发明。

[0047] 本发明的系统可以适用于包含有线和/或无线网络节点的网络化系统。在至少一

个实施例中，至少一个网络节点使用至少一个卫星来地理定位。在一个示例中，自地理定位的网络节点可以使用能够提供在室内可被接收的信号的近地轨道(LEO)星座。该系统可以或不可以与全球定位系统(GPS)或用来定位、导航和/或计时的任何其它系统结合使用。此外，本发明的系统可以采用生物测定学，以便通过用户/节点固有的一些东西来验证用户/节点，所述系统也可以采用与所描述的方法结合使用时将提高系统的整体安全性的任何其它的验证方法。

[0048] 本发明的系统具有四个主要特征。所述系统的第一个主要特征是教导了具有很多应用的自地理定位网络设备(例如，自地理定位服务器、路由器、个人计算设备、蜂窝电话和/或电视)，包括一般的计算机安全和认证，但是其也可以被用在其它应用(例如游戏)中。

[0049] 所公开的系统的第二个主要特征是其教导了实现认证和计算机安全的数据包结构。数据包结构使装置能够将该数据包追溯到作为被数据包用来到达其目的地位置的一系列结点的一部分的网络节点。该签名包结构能够被用来提高参与网络中的计算机安全。作为示例，签名数据包结构可以包含要素，如有效载荷数据、路由数据和/或安全数据。安全数据可以被定义为地理位置数据、生物计量数据和/或计时数据。在至少一个实施例中，如果该签名包结构被用于计算机安全应用，则其可以被统称为计算机安全签名。

[0050] 所公开的系统的第三个主要特征是其教导了独特的签名包结构的要素。网络链中的参与网络节点或其它类型的结点可以用附加的认证数据标记数据，该认证数据可以包含签名包结构的要素(即，有效载荷数据、路由数据和/或安全数据)。在追踪性方面，参与网络节点类似于来自指纹的接触DNA那样产生作用，因为数据包所使用的每个路由器为签名提供了一些可追踪的数据。当数据包移动到网络链中的下一个结点时，该结点将积累例如小比特序列，并且每个后续的结点可以对其进行认证。该小比特序列的积累能够导致在统计上引人注目的网络路径的指纹。通过比较到签名数据包的预期的网络路径(以及其相应的独特的附加数据)的网络延迟与预期的网络延迟可接受范围，可以进行认证。此外，可以对其它网络参数进行监控，以验证没有进行中间人(MITM)攻击。在一个实施例中，如果怀疑有MITM攻击，则可以将网络配置为基于网络的策略进行响应。

[0051] 所公开的系统的第四个主要特征是所述系统采用至少一个LEO卫星的使用来传输信号到网络节点。由于在接收器处LEO卫星信号的较高的接收功率，因此所述LEO卫星信号能够穿透到室内环境中。正因为如此，该特征允许将所公开的系统用于认证技术的许多室内应用。

[0052] 此外，应当注意，所公开的系统能够被用于期望确认、追踪、监控和/或追踪“节点”的位置的各种应用。另外，该系统可以为信用卡的现有跟踪方法提供额外的用途，特别是因为支付选项目前正被更多地集成到个人便携设备中，如蜂窝电话。不仅信用卡用户的位置能够被监控，而且对于试图从用户那里取回被偷的信用卡的情况，还可以潜在地追踪用户以对其重定位。而且，应当注意，该特征可以与用来玩游戏(例如用于地理藏宝(geo-caching))的个人计算设备结合使用。

[0053] 在下列描述中，对很多细节进行阐述以提供系统的更透彻的描述。然而，对本领域的一个技术人员来说显而易见的是，所公开的系统可以脱离这些具体的细节而实现。在其它例子中，没有对公知的特征进行详细的描述，以免不必要地模糊所述系统。

[0054] 图1说明了用于针对计算机和网络安全应用在衰减环境中地理定位网络节点的所

公开的系统100的实施例。在该图中，位于起始网络节点（节点A）110处的用户希望将数据包130传输给位于目的地网络节点（节点D）120处的用户。起始网络节点（节点A）110和目的地网络节点（节点D）120通过多个路由器网络节点140（其包括节点B140和节点C140）彼此连接。起始网络节点（节点A）110被示为经由路由器网络节点即节点B140和节点C140将数据包130传输到目的地网络节点（节点D）120。

[0055] 数据包130包含安全签名部分170、路由数据部分150和有效载荷数据部分160。数据包130的路由数据部分150包含数据包130的路由信息。该路由信息包含关于数据包130被发送到的目的地网络节点（例如，目的地网络节点（节点D）120的地址）的信息。数据包130的有效载荷数据部分160包含起始网络节点（节点A）110处的用户想要发送给目的地网络节点（节点D）120处的用户的数据和/或信息。安全签名部分应当不能从一个包中复制并粘贴到另一包中，否则将危害发明的实质，因为产生似乎遵循与第一个数据包相同的路由的另一数据包将是可能的。在不同的实施例中，安全签名部分可以有不同的应用。在一个实施例中，安全签名可以是有效载荷数据的函数。例如，安全签名能够包含是数字签名的组分，该数字签名可以是有效载荷数据的函数。可以沿着所述路由积累这些数字签名，或者可以将其验证为是来自最后的参与路由器的数字签名，并在每一跳中用新的数字签名对其进行替换。

[0056] 数据包130的安全签名部分170包含数据包130从起始网络节点（节点A）110行进到目的地网络节点（节点D）120所经过的所有网络节点的列表。如该示例中所示，安全签名部分170中的网络节点的列表包含节点A110、节点B140、节点C140和节点D120。随着数据包130行进经过节点的网络，每次数据包130行进经过网络节点，该特定的网络节点就被添加到网络节点的列表中。这样，安全签名170发展成数据包130的独特的密钥标识符，很像特定生物体的具体的DNA序列。

[0057] 在一个或更多实施例中，安全签名部分170也包含列表中至少一个网络节点的计时信息。该计时信息表明数据包130何时被（一个或多个）网络节点接收和/或传输。另外，在至少一个实施例中，数据包130的安全签名部分170包含列表中至少一个网络节点的标识符信息。可以用于所公开的系统的标识符信息的类型包括但不限于各种类型的生物计量信息和/或每个网络节点的独特的比特序列标识码。

[0058] 此外，数据包130的安全签名部分170包含列表中至少一个网络节点的地理位置信息。该地理位置信息包括网络节点的具体物理位置，并且其也可以包括关于网络节点的位置是否被验证的指示。在至少一个实施例中，通过网络节点接收从至少一个发射源发射的至少一个认证信号来验证该网络节点的地理位置信息。在图3、图4、图5和图6的描述中论述了如何通过使用（一个或多个）认证信号来验证网络节点的位置的详细描述。在一些实施例中，从传输到已验证位置处的网络节点的信号和从已验证位置处的网络节点发射的信号中获得测距信息，通过利用该测距信息验证网络节点的地理位置信息。在图2的描述中描述了如何获得测距信息的详细描述。

[0059] 图2说明了被基于传输的认证系统200和测距信息的使用所验证的三个网络节点210、220、230的位置。在该图中，网络节点210、220是位于已验证的位置处的路由器网络节点。通过使用采用卫星240来传输至少一个认证信号的基于传输的认证系统200来验证这些网络节点210、220的位置。参考图3、图4、图5和图6的论述，得到如何操作基于传输的认证系

统200的详细描述。在该图中，网络节点230的位置没有被基于传输的认证系统200验证，因为网络节点230没有卫星240接入。然而，能够利用通过往返时间延迟(即，ping延迟)的使用得到的测距信息来验证网络节点230的位置，往返时间延迟通过传输信号到已验证位置处的网络节点210、220和从该节点发射信号来获得。

[0060] 用于为该示例获得测距信息的过程如下。首先，在t1a时刻，网络节点230传输信号(R31)到网络节点210。在t3a时刻，网络节点210接收信号(R31)，并且在t3b时刻传输返回信号(R13)到网络节点230。在t1b时刻，网络节点230接收返回信号(R13)。网络节点210接收信号(R31)和用信号(R13)进行回复之间的延迟(即t3b-t3a)是已知的。这样，往返延迟(乘以光速并除以2)给出网络节点210和网络节点230之间的距离。然后，该距离信息能够被用来验证网络节点230的位置。使用相似的计算方法来计算网络节点230和网络节点220之间的距离。相关的网络距离公式为：

[0061] $R13=c[(t3a-t1a)+(t1b-t3b)]/2$

[0062] $R23=c[(t3a-t2a)+(t2b-t3b)]/2$,

[0063] 其中t等于时间，而c等于光速。

[0064] 图3说明了采用卫星310的基于传输的认证系统300的实施例，卫星310发射包含认证波束320(其也可以被称为“波束零”)和一个或更多保护波束330的重叠的点波束340。合法的网络节点360被示为位于认证波束320之内。欺骗性网络节点350试图模拟合法的网络节点360的位置。

[0065] 随着时间的推移，保护波束330和波束零320内的每个位置都接收到来自每个波束340的独特的认证信号。波束340重叠的区域内的位置接收复合认证信号。欺骗性网络节点350没有位于合法的网络节点360的位置，并且因此，欺骗性网络节点350将不能接收合法的网络节点360因其位置应当收到的特定的认证信号320。除非网络节点位于其合法位置，否则该网络节点将无法接收正确的认证信号，并且这样，认证器设备不能验证该网络节点的位置。

[0066] 在一个或更多实施例中，在点波束340中传输的数据可以包括可被用来区分一个波束中的数据与其它波束中的数据的认证密钥和/或其他伪随机代码段。所公开的系统和方法可以使用其它相区别的波束特性和/或数据特性来区分波束340之间的数据。在至少一个实施例中，可以用比发射波束零320更高的功率来发射保护波束330。这将使来自保护波束330的信号屏蔽波束零320认证信号。

[0067] 图4A至图4F描述了使用被一个或更多网络节点从多个重叠的点波束中接收的信号来认证一个或更多网络节点的位置和身份的实施例。基本概念是根据网络节点在重叠的点波束图案中所处的位置，每个网络节点将从多个点波束传输的信号组合中接收不同的复合信号。特别地，图4A示出了具有例如四个网络节点(即A、B、C和D)的公开的基于传输的认证系统，该四个网络节点被置于三个重叠的点波束(即波束1、波束2和波束3)内和附近的不同位置处。这样，该图说明了照明网络节点A、B和C的位置的重叠的点波束。网络节点D的位置被示为刚好在波束图案外部。

[0068] 图4B说明了示出由图4A的三个点波束传输的示例性信号(1、2和3)的图形400。特别地，该图示出了被每个点波束(波束1、波束2和波束3)传输并被用来验证网络节点的位置的信号的示例性集合。三条曲线(由图形400上的1、2和3表示)示出了从每个点波束传输的

信号随时间的比特序列。这三个比特序列仅用来说明概念。因此，也可以采用许多其它类型的数据和调制形式。信号图案也可以周期性地变化，以提供对避免欺骗性的网络节点和/或用户的额外的保护，并且提供移动的网络节点何时处于特定位置的独特的时间。此外，在正常的传输期间，可以将被用来认证网络节点的这些信号与短期的正常信号分开发送，或可替换地，可以将这些信号嵌入到正常信号中。

[0069] 图4C示出了图4A的四个网络节点(A、B、C和D)的位置处的三个点波束(波束1、波束2和波束3)的信号强度的阵列410。特别地，接收的信号波束(sbr)阵列410示出了由阵列410的列中的每个网络节点(A、B、C和D)从阵列410的行中的接收的信号波束(波束1、波束2和波束3)接收的信号强度。例如，B位置处的网络节点从波束2接收大部分信号，与分别来自波束1和波束3的信号强度2和1.5相比，其具有信号强度11。网络节点的接收的信号的特性和/或属性可以是被用来验证该网络节点的位置的签名。

[0070] 图4D描述了图4A的三个点波束(波束1、波束2和波束3)的比特的阵列420。在该图中，比特阵列420示出了由三个阵列行中的每个波束(波束1、波束2和波束3)传输的信号序列，作为时间的函数，其由阵列420的十六(16)列表示。这里，为说明概念，所传输的信号是二进制的。然而，在可替换的实施例中，可以采用其它信号模式。

[0071] 图4E说明了被图4A的四个网络节点(A、B、C和D)接收的合成信号序列的阵列430。该图示出了被位置A、B、C和D处的网络节点从多个重叠的波束中接收的复合信号的合成序列。合成信号(rx)=gx(sbr^T)x(bits)，其中g等于每个网络节点接收器的增益。在该示例中，选择增益(g)等于0.7(即g=0.7)。接收阵列(rx^T)430的十六(16)行表示时间步长，而四(4)列对应于不同位置(A、B、C和D)的网络节点。应当注意，在该示例中，位置D处的网络节点不接收信号，因为该位置在波束图案外部。

[0072] 图4F示出了描述被图4A的四个网络节点(A、B、C和D)接收的合成信号的图形440。四条曲线(由A、B、C和D表示)示出被位置A、B、C和D处的网络节点接收的合成信号的时间序列。四个合成复合信号分别为四个网络节点(A、B、C和D)提供独特的网络节点位置识别。

[0073] 图5示出了利用保护波束传输作为辅助任务的一部分的基于传输的认证系统500的实施例。在该实施例中，使用至少一个保护波束作为卫星510的辅助任务的一部分来传输合法数据。例如，可以利用保护波束来广播原始信息，例如在保护波束足迹中有效的不同的GPS网络修正。然而，应当注意，对更高的安全性来说，这不是优选的实施例，因为比起更随机的信号，该原始信息更可能被欺骗设备确定。作为另一示例，可以用保护波束来传输与主要任务(即认证信号)相关和/或与辅助任务相关的数据。

[0074] 如图5所示，可以在脉冲串中传输认证信号。可以在脉冲串、波束零或交替波束(包括波束零和保护波束)中随机发送认证信号，以便认证信号的计时表明网络节点的位置。这样，如果网络节点接收多个脉冲串，则该网络节点位于波束零之内或波束重叠的区域之内。

[0075] 在可替代的实施例中，可以将认证信号嵌入到正常的数据传输中，从而最小化认证信号对卫星发射功率和/或带宽的影响。可以采用不影响正常的接收但是可被具体处理检测的各种方式(例如，时间、频率、极化偏移等)将认证信号嵌入到数据传输中。

[0076] 在一个或更多实施例中，可以通过在逐位基础上改变广播功率来将认证信号嵌入到正常的数据传输中。对这些实施例来说，保护波束比特调制在逐位基础上改变传输的比特的广播功率。这防止欺骗设备试图观察本地保护波束中的比特，并防止欺骗设备处理数

据以移除这些比特。

[0077] 例如，欺骗设备进行一系列测量(m)：

[0078] 95 105 105 -105 105 -105 95 -105 -95 -95

[0079] 该欺骗设备可能推测保护信号(g)为sign(m)：

[0080] 1 1 1 -1 1 -1 1 -1 -1 -1

[0081] 并且，该欺骗设备尝试访问的信号为sign(m-sign(m)*100)：

[0082] -1 1 1 -1 1 -1 -1 -1 1 1

[0083] 如果不是固定的功率信号，则对保护波束广播功率进行调制，使得其接收到的信号的组分为：

[0084] 107 97 91 -93 99 -91 93 -107 -107 -101

[0085] 然后，欺骗设备将接收到的信号为：

[0086] 102 102 96 -98 104 -96 88 -112 -102 -96

[0087] 对欺骗设备来说，尝试从测量的集合中计算出认证信号将是非常困难的。

[0088] 此外，应当注意，该相同的想法的延伸将是在保护带信号上添加小的随机四相相移键控(QPSK)信号。对于这种情况，仍然可以利用保护信号来传输有用的信息。

[0089] 图6示出了采用异相的二进制相移键控(BPSK)保护波束传输的基于传输的认证系统600。具体地，在该图中，保护波束利用相邻的重叠波束之间的异相BPSK信号来传输认证信号。于是，重叠区域中的信号将是QPSK信号。然后，通过分析网络节点接收的信号相位和信号类型能够确定波束内的网络节点的独特的位置。

[0090] 在可替换的实施例中，可以使用辅助信号源来提供额外的屏蔽传输。例如，第二卫星可以为第一卫星的外部波束广播保护波束。

[0091] 图7说明了具有能够在闭塞或拥挤的环境中执行的网络节点710的公开的系统700的实施例。特别地，图7示出了从两个卫星706、704和蜂窝信号塔708接收RF信号709、705、707的网络节点710。在一个示例中，RF信号709、705、707被下变频、取样、有选择地加密，并被附加到经过网络节点710路由的安全增强数据包。在另一示例中，从RF信号709、705、707提取数据。对提取的数据进行任选的加密，并将其附加到通过网络节点710路由的安全增强数据包。可以由公开的系统采用的各种类型的RF信号源的示例包括但不限于：LEO卫星(例如，铱卫星)、GPS卫星(例如，传输GNSS信号)以及蜂窝信号塔。

[0092] 虽然本文公开了某些说明性实施例和方法，但是根据上述公开，对本领域技术人员来说显而易见的是，能够在不脱离本发明的实质精神和范围的情况下对这些实施例和方法做出各种变化和修改。存在本领域公开的许多其它示例，每个示例仅在细节方面区别于其它示例。因此，所公开的领域旨在应当仅被由所附权利要求和适用的法律的规则和原理要求的范围所限定。

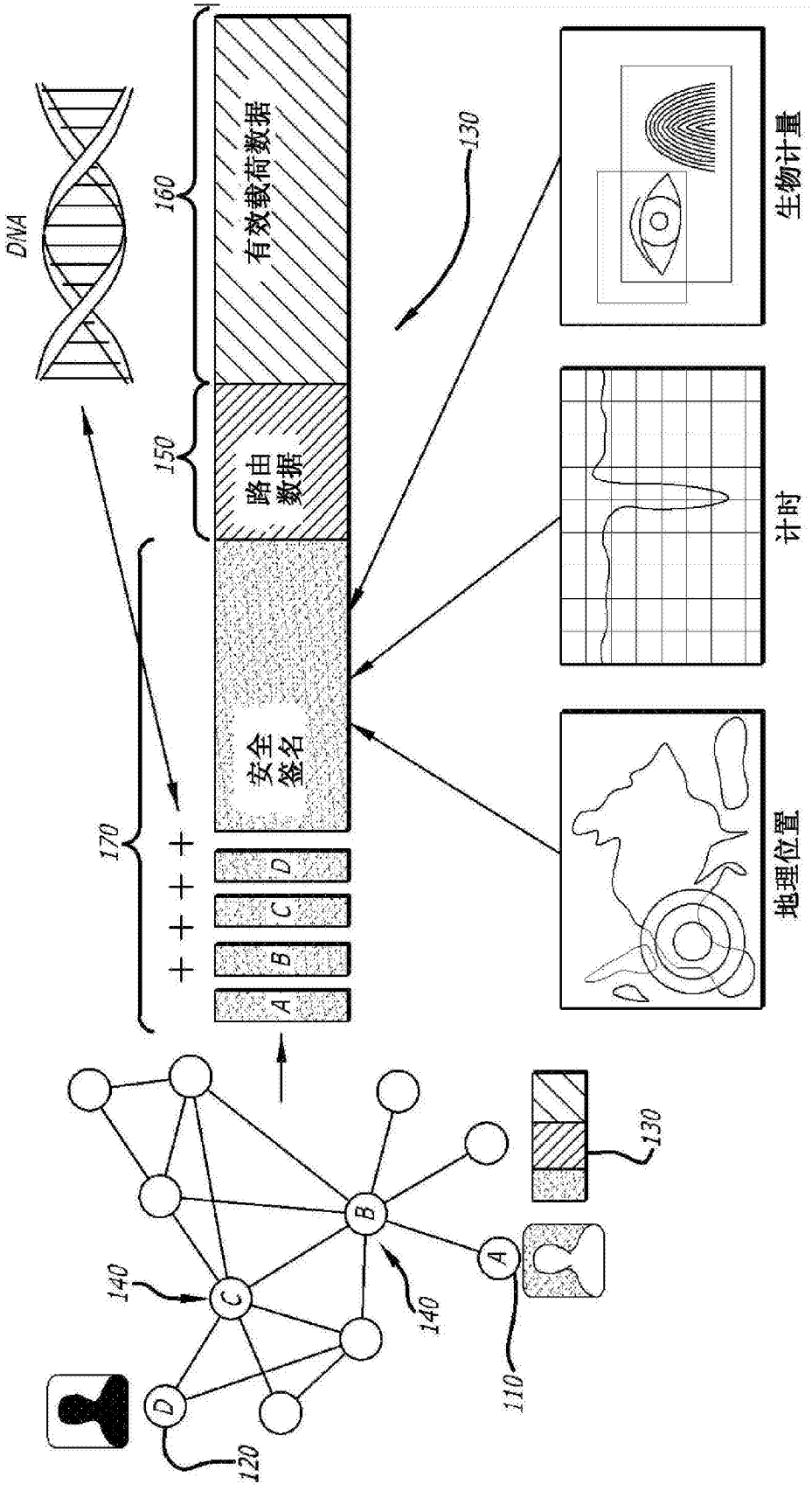

DNA
160
有效载荷数据
150
路由数据
130
安全签名
170
A
B
C
D
生物计量
计时
地理位置
130
140
140
110
120

图1

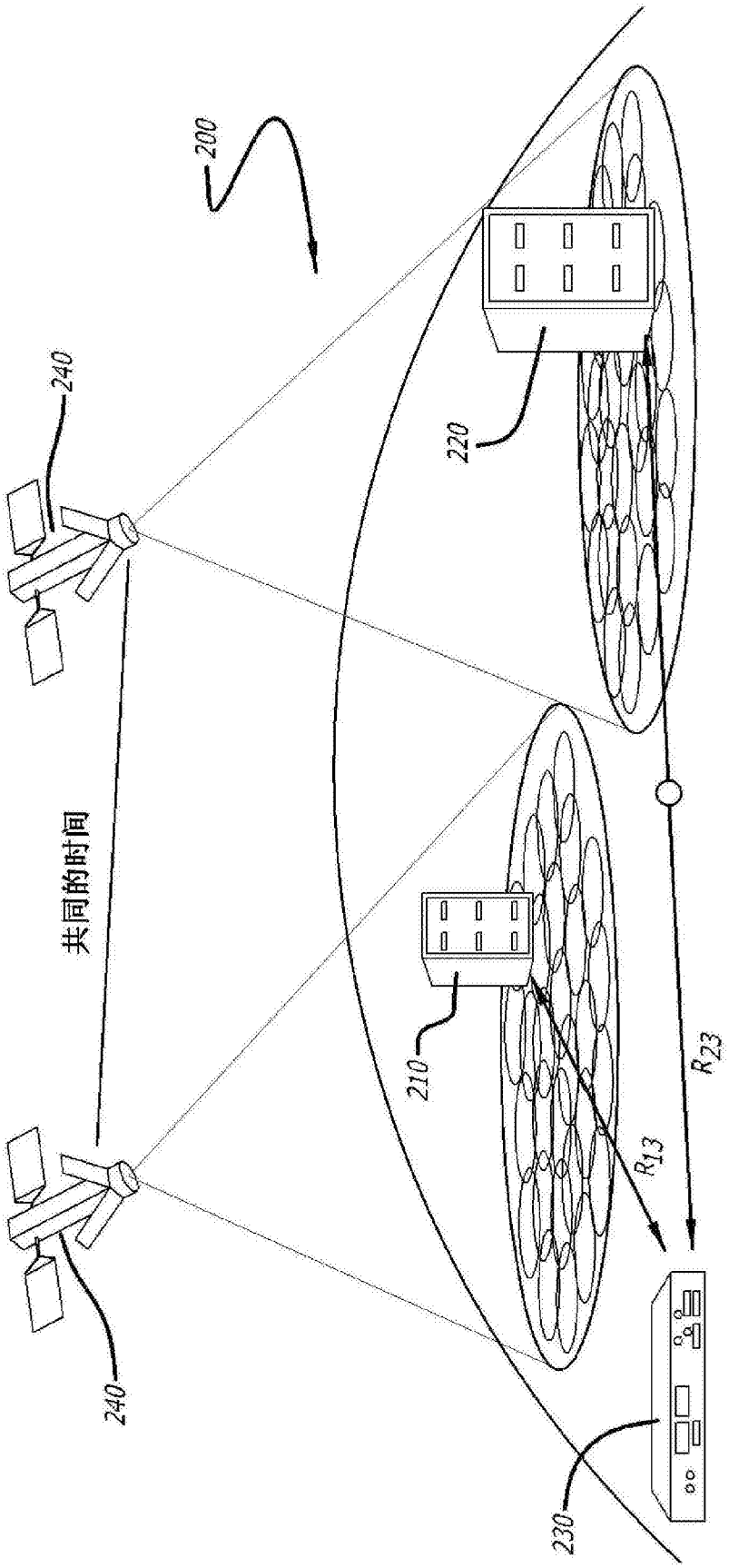


图2

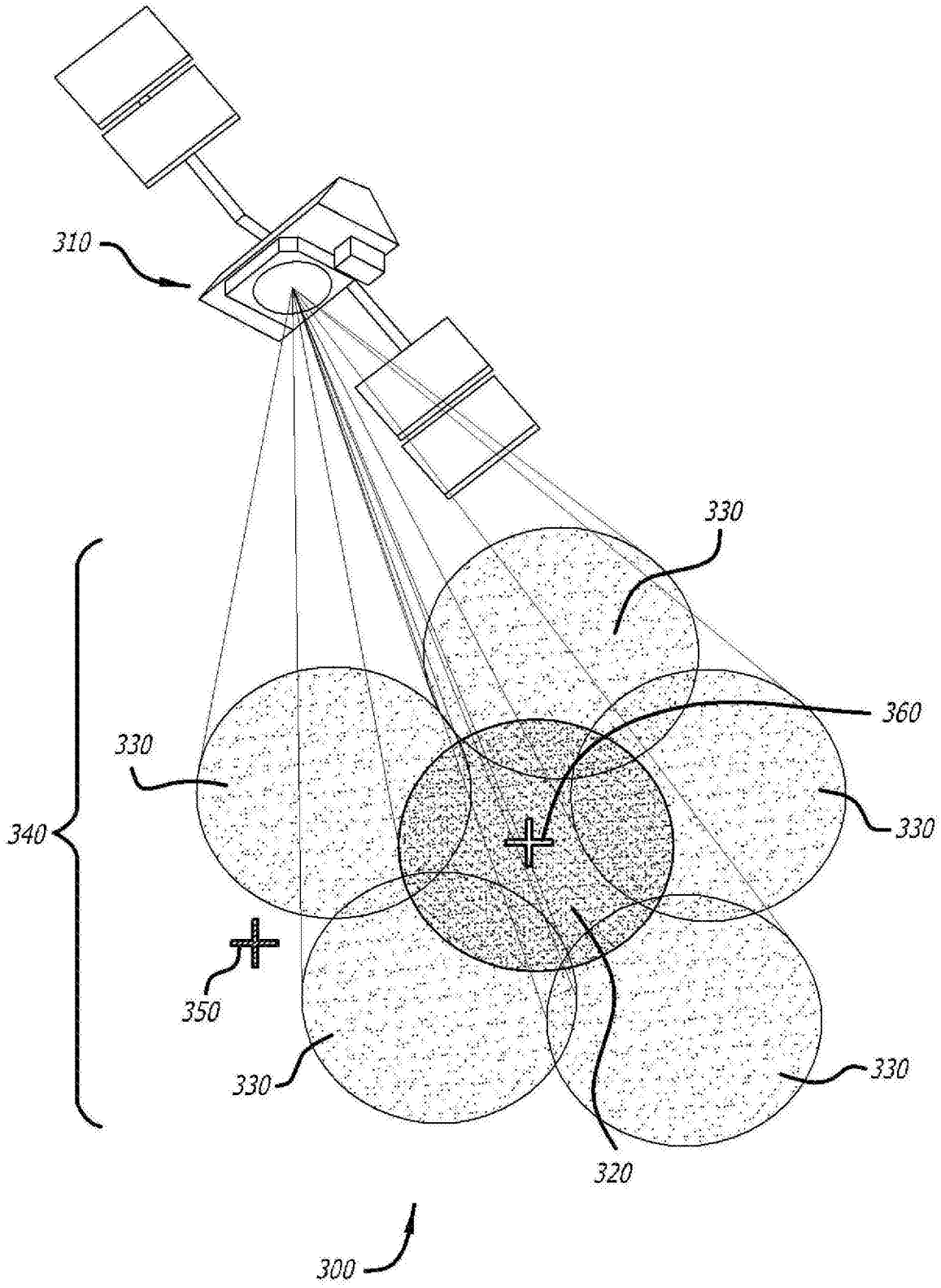


图3

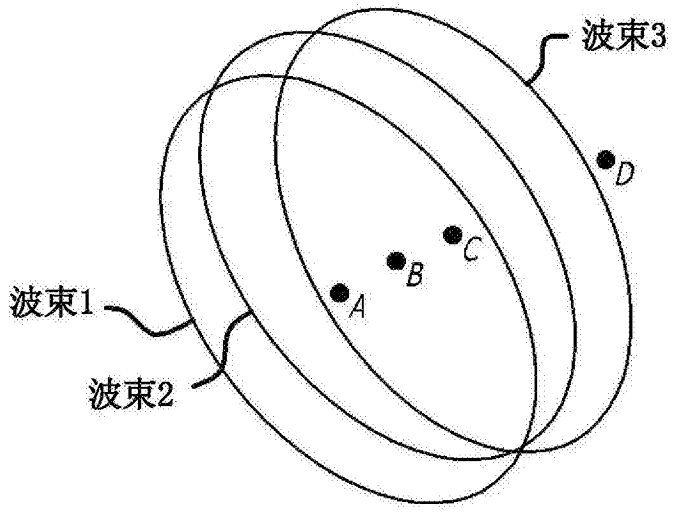


图4A

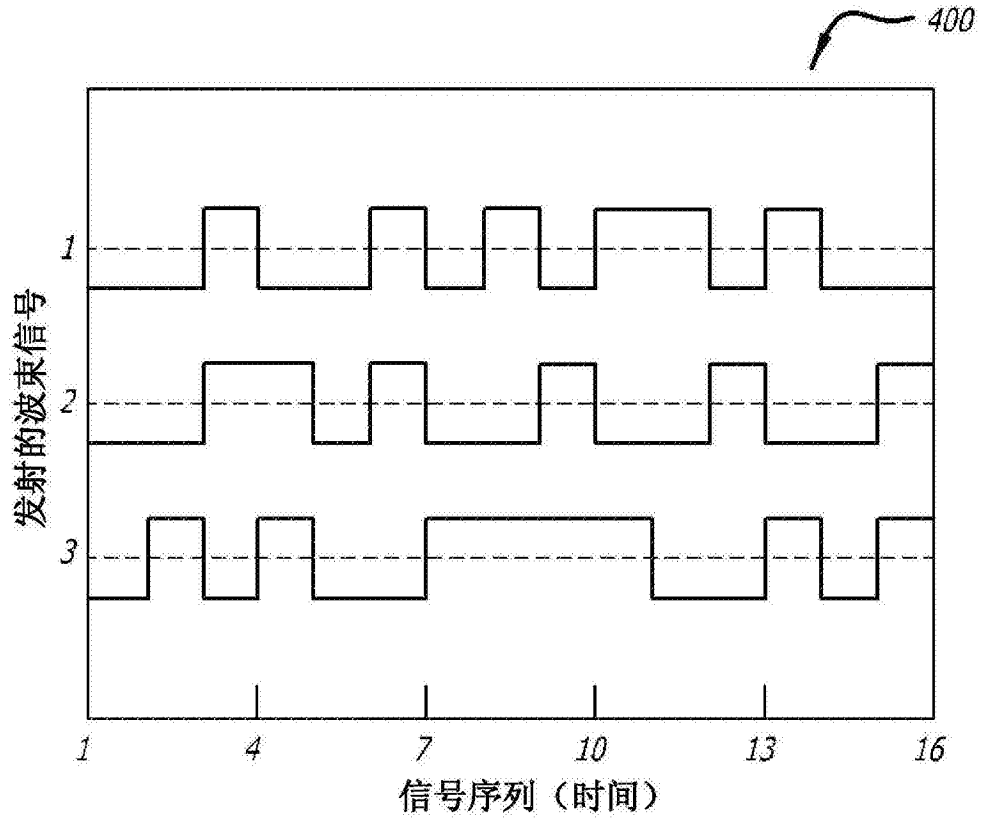


图4B

410

	A	B	C	D	
sbr=	10	2	.5	0	波束1
	3	11	2.5	0	波束2
	.2	1.5	12	0	波束3

图4C

420

时间

比特 =

-1	-1	1	-1	-1	1	-1	1	-1	1	1	-1	1	-1	-1	-1	波束1
-1	-1	1	1	-1	1	-1	-1	1	-1	-1	1	-1	-1	1	-1	波束2
-1	1	-1	1	-1	-1	1	1	1	1	-1	-1	1	-1	1	-1	波束3

图4D

430

rx^T =

	A	B	C	D
1	-9.24	-10.15	-10.5	0
2	-8.96	-8.05	6.3	0
3	8.96	8.05	-6.3	0
4	-4.76	7.35	9.8	0
5	-9.24	-10.15	-10.5	0
6	8.96	8.05	-6.3	0
7	-8.96	-8.05	6.3	0
8	5.04	-5.25	7	0
9	-4.76	7.35	9.8	0
10	5.04	-5.25	7	0
11	4.76	-7.35	-9.8	0
12	-5.04	5.25	-7	0
13	5.04	-5.25	7	0
14	-9.24	-10.15	-10.5	0
15	-4.76	7.35	9.8	0
16	-9.24	-10.15	-10.5	0

时间

图4E

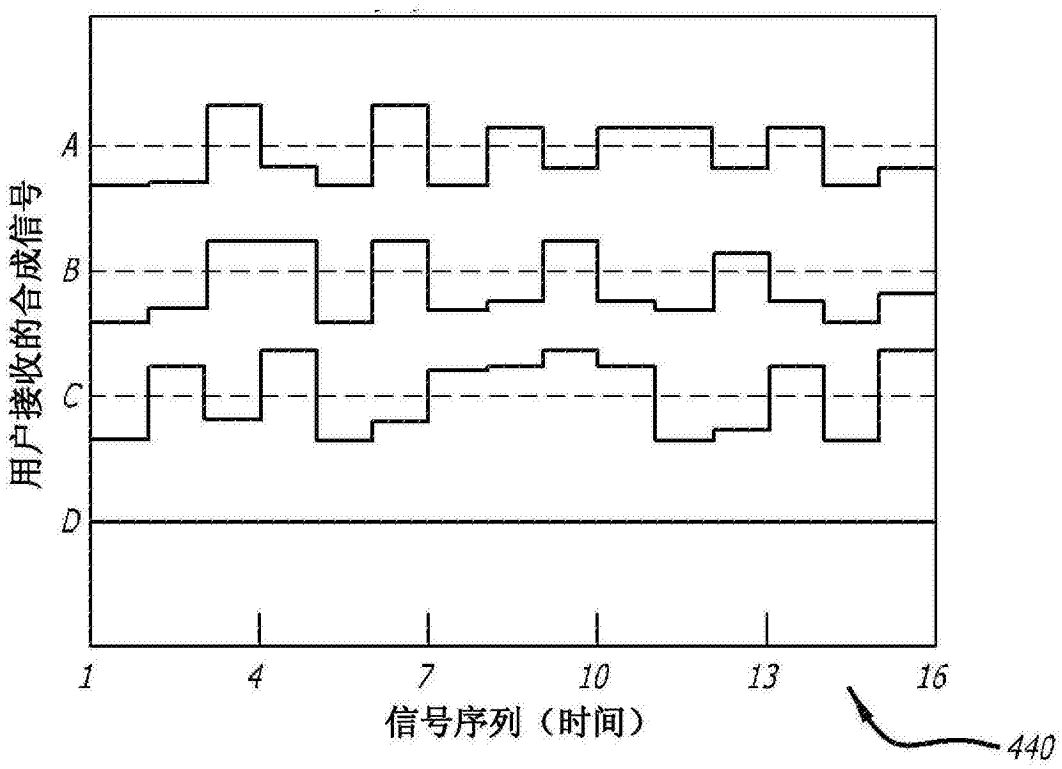


图4F

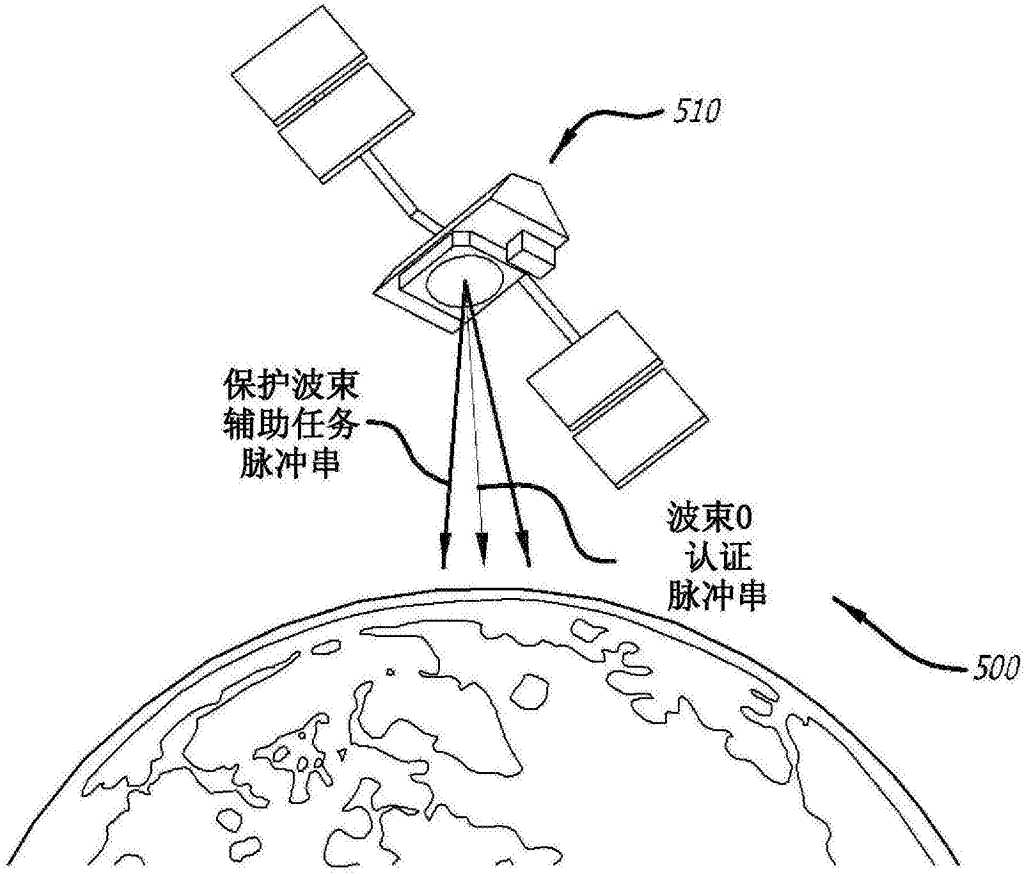


图5

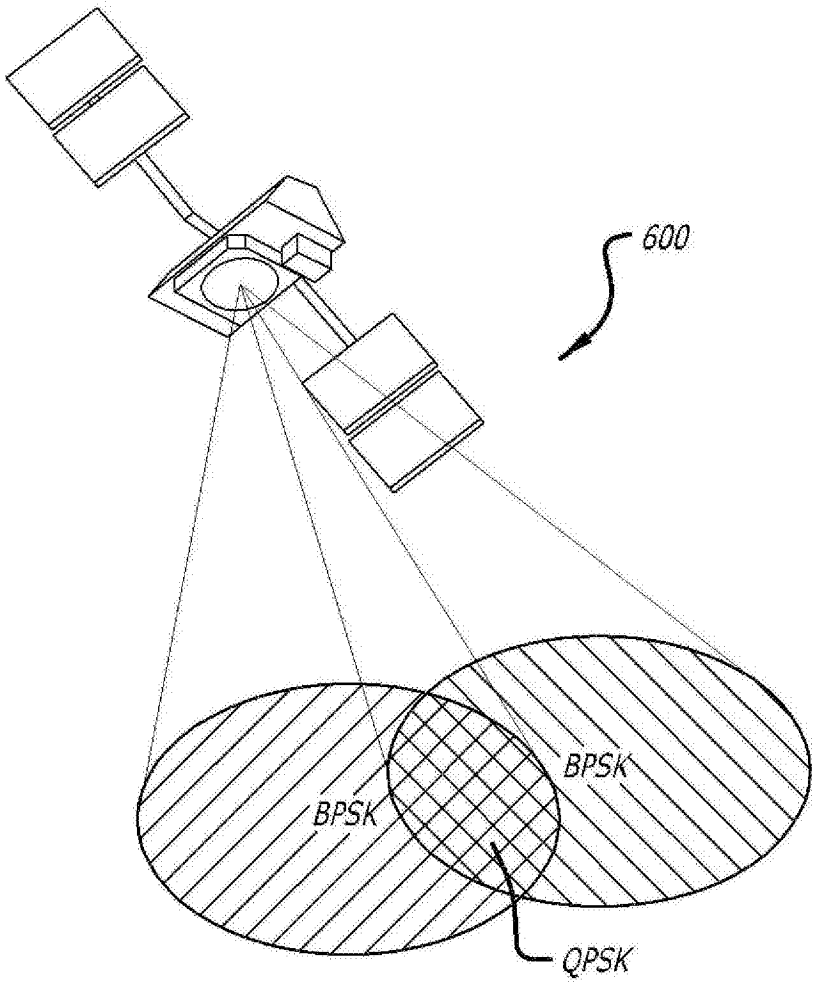


图6

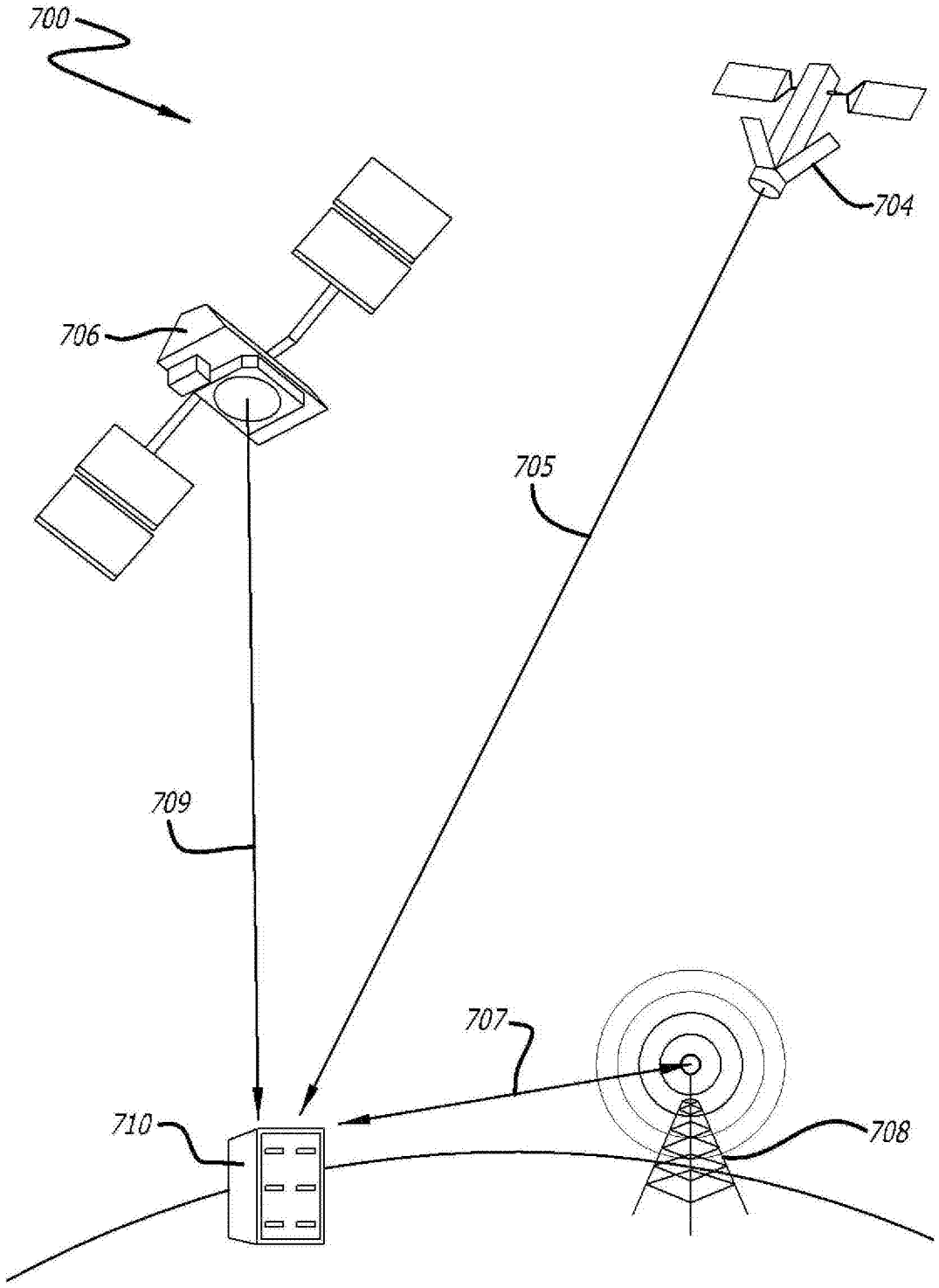


图7