



(12)发明专利申请

(10)申请公布号 CN 110741614 A

(43)申请公布日 2020.01.31

(21)申请号 201880038400.8

(22)申请日 2018.07.06

(30)优先权数据

1711016.4 2017.07.07 GB

(85)PCT国际申请进入国家阶段日

2019.12.10

(86)PCT国际申请的申请数据

PCT/EP2018/068335 2018.07.06

(87)PCT国际申请的公布数据

WO2019/008130 EN 2019.01.10

(71)申请人 古鲁洛吉克微系统公司

地址 芬兰图尔库

(72)发明人 托马斯·卡开宁 米科·萨尔博姆

(74)专利代理机构 北京英赛嘉华知识产权代理有限公司 11204

代理人 王达佐 王艳春

(51)Int.Cl.

H04L 29/06(2006.01)

H04W 12/06(2006.01)

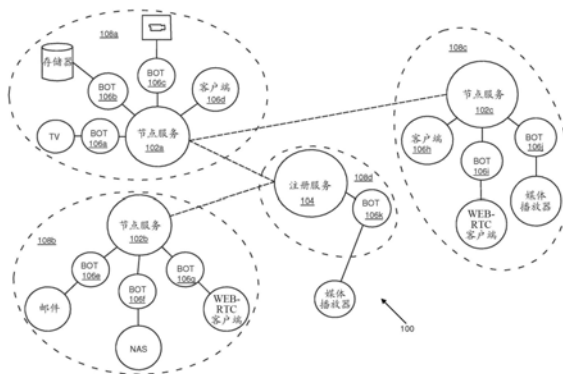
权利要求书4页 说明书17页 附图5页

(54)发明名称

数据通信系统和方法

(57)摘要

提供了用于本地网络的数据通信系统。该系统包括网络节点和与其相关联的多个网络设备。网络节点向在多个网络设备上执行的客户端或机器人程序提供网络节点服务。各个客户端或机器人程序可通信地且仅以程序化星形配置以编程方式耦接在网络节点服务周围以形成本地网络。网络节点服务验证和认证由本地网络内的客户端或机器人程序提供的本地服务。通过经由网络节点服务中继数据来实时或接近实时地在本地网络内的客户端或机器人程序之间传输数据。通过采用与源客户端或机器人程序的用户相关联的密钥存储库,在传输数据之前对该数据的信息内容进行加密。



1. 一种用于本地网络 (108a、200、300) 的数据通信系统 (100), 所述数据通信系统 (100) 包括至少一个网络节点 (102a) 以及与所述至少一个网络节点 (102a) 相关联的多个网络设备 (106a、106b、106c、106d), 其特征在于:

-所述至少一个网络节点 (102a) 配置成向在所述多个网络设备 (106a、106b、106c、106d) 上执行的多个客户端或机器人程序提供网络节点服务, 其中所述多个客户端或机器人程序中的各个客户端或机器人程序可通信地且仅以程序化星形配置以编程方式耦接在所述网络节点服务周围以形成所述本地网络 (108a、200、300), 而且其中, 所述网络节点服务配置成验证和认证由所述本地网络 (108a、200、300) 内的所述多个客户端或机器人程序提供的本地服务;

-源客户端或机器人程序配置成通过经由所述网络节点服务中继所述数据, 来实时或接近实时地将数据传输到所述本地网络 (108a、200、300) 内的一个或多个目标客户端或机器人程序; 以及

-所述源客户端或机器人程序配置成在将所述数据传输到所述一个或多个目标客户端或机器人程序之前对所述数据的信息内容进行加密, 其中所述源客户端或机器人程序配置成采用密钥存储库来加密所述数据的信息内容, 所述密钥存储库与所述源客户端或机器人程序的用户相关联。

2. 如权利要求1所述的数据通信系统 (100), 其特征在于, 所述至少一个网络节点包括至少第一网络节点 (102a) 和第二网络节点 (102b), 并且其中所述多个网络设备包括与所述第一网络节点 (102a) 相关联的第一组网络设备 (106a、106b、106c、106d) 以及与所述第二网络节点 (102b) 相关联的第二组网络设备 (106e、106f、106g), 其中,

-所述第一网络节点 (102a) 配置成向在所述第一组网络设备 (106a、106b、106c、106d) 上执行的第一组客户端或机器人程序提供第一网络节点服务, 并且所述第二网络节点 (102b) 配置成向在所述第二组网络设备 (106e、106f、106g) 上执行的第二组客户端或机器人程序提供第二网络节点服务, 其中所述第一组客户端或机器人程序中的各个客户端或机器人程序可通信地且仅以程序化星形配置以编程方式耦接在所述第一网络节点服务周围以形成第一本地网络 (108a), 并且所述第二组客户端或机器人程序中的各个客户端或机器人程序可通信地且仅以程序化星形配置以编程方式耦接在所述第二网络节点服务周围以形成第二本地网络 (108b), 而且其中, 所述第一网络节点服务和所述第二网络节点服务配置成验证和认证由它们相应的本地网络 (108a、108b) 内的所述第一组客户端或机器人程序和所述第二组客户端或机器人程序提供的本地服务;

-当给定的源客户端或机器人程序配置成将数据传输到同一本地网络内的给定的目标客户端或机器人程序时, 通过它们在所述同一本地网络内的相关网络节点服务实时或接近实时地中继将要传输的数据; 以及

-当给定的源客户端或机器人程序配置成将数据从不同的本地网络传输到给定的目标客户端或机器人程序时, 通过与所述给定的源客户端或机器人程序相关联的网络节点服务并且通过与所述给定的目标客户端或机器人程序相关联的网络节点服务, 来实时或接近实时地中继将要传输的数据。

3. 如权利要求1或2所述的数据通信系统 (100), 其特征在于, 所述源客户端或机器人程序配置成将元数据与所述数据一起传输, 其中所述元数据包括指示所述密钥存储库的唯一

标识符 (ID) 以及将要从所述密钥存储库导出的密钥材料的密钥索引的加密信息,以用于随后对所加密的信息内容进行解密。

4. 如权利要求3所述的数据通信系统 (100), 其特征在于, 所述元数据还包括组信息, 所述组信息指示所述数据待传输到的一个或多个目标客户端或机器人程序, 其中所述源客户端或机器人程序以及所述一个或多个目标客户端或机器人程序一起形成组。

5. 如权利要求3或4所述的数据通信系统 (100), 其特征在于, 所述元数据以未加密的形式进行通信。

6. 如权利要求3或4所述的数据通信系统 (100), 其特征在于, 所述元数据以加密的形式进行通信。

7. 如权利要求1至6中任一项所述的数据通信系统 (100), 其特征在于, 所述数据通信系统 (100) 配置成利用所述第一本地网络和所述第二本地网络 (108a、108b) 中存在的一个或多个数据通信网络来进行数据通信。

8. 如权利要求1至7中的任一项所述的数据通信系统 (100), 其特征在于, 所述数据通信系统 (100) 配置成利用注册服务来注册由所述第一本地网络和所述第二本地网络 (108a、108b) 的所述客户端或机器人程序提供的服务。

9. 如权利要求8所述的数据通信系统 (100), 其特征在于, 所述数据通信系统 (100) 配置成利用所述注册服务来注册由给定客户端或机器人程序提供的给定服务作为针对所述给定客户端或机器人程序的用户私有服务或公共服务。

10. 如权利要求1至9中任一项所述的数据通信系统 (100), 其特征在于, 以动态方式创建给定的本地网络 (108a、200、300)。

11. 一种经由用于本地网络 (108a、200、300) 的数据通信系统 (100) 来传输数据的方法, 所述数据通信系统 (100) 包括至少一个网络节点 (102a) 以及与所述至少一个网络节点 (102a) 相关联的多个网络设备 (106a、106b、106c、106d), 其特征在于, 所述方法包括:

- 经由所述至少一个网络节点 (102a) 来向在所述多个网络设备 (106a、106b、106c、106d) 上执行的多个客户端或机器人程序提供网络节点服务, 其中所述多个客户端或机器人程序中的各个客户端或机器人程序可通信地且仅以程序化星形配置以编程方式耦接在所述网络节点服务周围以形成所述本地网络 (108a、200、300), 而且其中, 所述网络节点服务配置成验证和认证由所述本地网络 (108a、200、300) 内的所述多个客户端或机器人程序提供的本地服务;

- 通过经由所述网络节点服务中继所述数据, 来实时或接近实时地将数据从源客户端或机器人程序传输到所述本地网络 (108a、200、300) 内的一个或多个目标客户端或机器人程序; 以及

- 在将所述数据传输到所述一个或多个目标客户端或机器人程序之前, 在所述源客户端或机器人程序处对所述数据的信息内容进行加密, 其中密钥存储库被用来加密所述数据的信息内容, 所述密钥存储库与所述源客户端或机器人程序的用户相关联。

12. 如权利要求11所述的方法, 其特征在于, 所述至少一个网络节点包括至少第一网络节点 (102a) 和第二网络节点 (102b), 并且所述多个网络设备包括与所述第一网络节点 (102a) 相关联的第一组网络设备 (106a、106b、106c、106d) 以及与所述第二网络节点 (102b) 相关联的第二组网络设备 (106e、106f、106g), 其中所述方法包括:

-经由所述第一网络节点(102a)向在所述第一组网络设备(106a、106b、106c、106d)上执行的第一组客户端或机器人程序提供第一网络节点服务,并且经由所述第二网络节点(102b)向在所述第二组网络设备(106e、106f、106g)上执行的第二组客户端或机器人程序提供第二网络节点服务,其中所述第一组客户端或机器人程序中的各个客户端或机器人程序可通信地且仅以程序化星形配置以编程方式耦接在所述第一网络节点服务周围以形成第一本地网络(108a),并且所述第二组客户端或机器人程序中的各个客户端或机器人程序可通信地且仅以程序化星形配置以编程方式耦接在所述第二网络节点服务周围以形成第二本地网络(108b),而且其中,所述第一网络节点服务和所述第二网络节点服务配置成验证和认证由它们相应的本地网络(108a、108b)内的所述第一组客户端或机器人程序和所述第二组客户端或机器人程序提供的本地服务;

-当给定的源客户端或机器人程序以及给定的目标客户端或机器人程序来自同一本地网络内时,通过它们在所述同一本地网络内的相关联网络节点服务实时或接近实时地中继将要传输的数据;以及

-当给定的源客户端或机器人程序以及给定的目标客户端或机器人程序来自不同的本地网络时,通过与所述给定的源客户端或机器人程序相关联的网络节点服务并且通过与所述给定的目标客户端或机器人程序相关联的网络节点服务来实时或接近实时地中继将要传输的数据。

13. 如权利要求11或12所述的方法,其特征在于,所述方法还包括将元数据与所述数据一起从所述源客户端或机器人程序传输到所述一个或多个目标客户端或机器人程序,其中所述元数据包括指示所述密钥存储库的唯一标识符(ID)以及将要从所述密钥存储库导出的密钥材料的密钥索引的加密信息,以用于随后对所加密的信息内容进行解密。

14. 如权利要求13所述的方法,其特征在于,所述元数据还包括组信息,所述组信息指示所述数据将被传输到的所述一个或多个目标客户端或机器人程序,其中所述源客户端或机器人程序以及所述一个或多个目标客户端或机器人程序一起形成组。

15. 如权利要求13或14所述的方法,其特征在于,所述元数据以未加密的形式进行通信。

16. 如权利要求13或14所述的方法,其特征在于,所述元数据以加密的形式进行通信。

17. 如权利要求12至16中任一项所述的方法,其特征在于,所述方法还包括利用所述第一本地网络和所述第二本地网络(108a、108b)中存在的一个或多个数据通信网络来进行数据通信。

18. 如权利要求12至17中任一项所述的方法,其特征在于,所述方法还包括利用注册服务来注册由所述第一本地网络和所述第二本地网络(108a、108b)的所述客户端或机器人程序提供的服务。

19. 如权利要求18所述的方法,其特征在于,所述方法还包括利用所述注册服务来注册由给定客户端或机器人程序提供的给定服务作为针对所述给定客户端或机器人程序的用户私有服务或公共服务。

20. 如权利要求11至19中的任一项所述的方法,其特征在于,所述方法还包括以动态方式创建给定的本地网络(108a、200、300)。

21. 一种计算机程序产品,包括其上存储有计算机可读指令的非暂时性计算机可读存

储介质,所述计算机可读指令能够由包括处理硬件的计算机化设备执行以执行如权利要求11至20中任一项所述的方法。

## 数据通信系统和方法

### 技术领域

[0001] 本公开涉及数据通信系统。此外,本公开涉及传输数据的方法。此外,本公开涉及计算机程序产品,其包括其上存储有计算机可读指令的非暂时性计算机可读存储介质,计算机可读指令可由包括处理硬件的计算机化设备执行以执行上述方法。

### 背景技术

[0002] 当代家庭和办公数据通信网络基于物理开放式本地网络中的连接设备,其中给定设备可以与其开放式本地网络之外的其他设备和服务提供商进行通信。两个物理连接的设备之间的数据通信(即,节点到节点的数据传输)由数据链路层(OSI L2)促进,该数据链路层提供两个物理连接的设备之间的链路。就这一点而言,数据链路层(OSI L2)定义协议以建立和终止两个物理连接的设备之间的连接。

[0003] 经由这种开放式本地网络提供的数据服务经常容易受到持续的攻击、窃听和其他有害的滥用行为。典型的当代方法是使用防火墙和防病毒扫描器来保护设备。然而,这种方法不能保护设备免受来自开放本地网络内部的攻击。

[0004] 另一种当代方法是为给定用户设备与给定服务器之间的数据传输提供加密连接。然而,将要传输的信息仅在传输期间被加密,并且以未加密的形式存储在两个端点,即给定的用户设备和给定的服务器。因此,不能保护信息免受可能的滥用。

[0005] 此外,当代服务是由服务提供商的数据中心生成的。这种当代实践具有若干缺点。首先,众所周知的事实是,当代数据中心在冷却方面比世界上所有航空公司消耗的能源更多,因为它们大部分时间都处于闲置状态。其次,当代数据中心产生信息并且由给定用户使用,该信息出于各种目的可用于服务提供商,例如用于基于用户配置文件的定向广告,即将此类信息出售给第三方以用于商业用途。

[0006] 此外,当代搜索引擎服务基于互联网®上存在的开放且可访问的信息,并且它们的服务为当代信息社会奠定了基础。这些搜索引擎服务行获得强大的功能,并且可能会将搜索引擎服务可访问的信息滥用于各种目的,这对于单个用户保护、公司乃至不同国家的立法都是不希望的。

[0007] 在公布的美国专利申请US 2016/0065548A1(“密钥链同步(Keychain syncing)”);发明人:Michael Brouwer、Dallas B. De Atley和Mitchell D. Adle)中,描述了一种程序,该程序在由设备的至少一个处理单元执行时,使存储在设备上的一组密钥链与一组其他设备同步。该设备和该组其他设备通过对等(P2P)网络彼此通信地耦接。程序接收对设备上存储的一组密钥链中的密钥链的修改。程序为该组其他设备中的每个设备生成更新请求,以使该设备上存储的该组密钥链与该组其他设备同步。程序通过一组独立的安全通信信道、通过P2P网络将一组更新请求传输到该组其他设备。

[0008] 在另一公布的美国专利申请US 2013/0195272A1(“用于传输或接收包含预定信息的信号的基站装置(Base station apparatus for transmitting or receiving a signal containing predetermined information)”);发明人:Makoto Nagai和Yoshihiro

Hori)中,描述了一种存储单元,该存储单元存储对称密钥表,该对称密钥表指示可用于终端装置之间的通信的多种对称密钥。MAC帧处理单元从终端装置接收分组广播。验证单元验证包含对称密钥的对称密钥表的版本,通过该对称密钥表生成附加到接收的分组的数字签名。检测器检测已验证的对称密钥表的版本是否比存储在存储单元中的对称密钥表的版本更旧。当检测次数在单位时间内为预定次数或以上时,MAC帧处理单元生成包括存储在存储单元中的对称密钥表的分组。MAC帧处理单元随后广播生成的分组。

[0009] 在又一公布的美国专利申请US 2010/0031063A1 (“远程安全备份的系统和方法 (System for and Method of Remote Secure Backup)”);发明人:Anthony Fascenda、Emil Sturniolo、Robert Cichielo和Paul Benware)中,描述了一种安全注册模块以进行备份的方法,其中模块包括至少一个非易失性存储器和处理器。该方法包括提供模块、为模块生成备份密钥、使用导出密钥加密备份密钥、将加密的备份密钥和其他信息传输到备份中心、以及利用备份中心存储加密的备份密钥和其他信息。

[0010] 在另一公布的美国专利申请US 2009/0122984A1 (“安全移动电话 (Secure mobile telephony)”);发明人:Anthony Fascenda、Emil Sturniolo、Robert Cichielo和Paul Benware)中,描述了一种用于提供端到端加密实时电话呼叫的系统和方法,其使用商用移动电话并且无需服务提供商的合作。该系统和方法省略了对专门制造成包括端到端加密功能的移动电话的任何要求。

[0011] 在又一公布的美国专利申请US 7096355B1 (“动态编码算法和内联消息解密 (Dynamic encoding algorithms and inline message decryption)”);发明人:Maclen Marvit、Keith David Rosema、Jeffrey Ubois、David Marvit、Dean Brettle、Yair Zadik和Stuart Goodnick)中,描述了一种内联消息解密方法,其中以使得用户的客户端能够使用常规客户端工具处理编码消息并获得明文消息的形式将编码的消息提供给用户。这消除了用户的客户端知道用于编码消息的特定编码算法的需要。内联消息解密方法包括:a)原位解密;b)远程解密;以及c)数据上传。还提供了一种用于使用一组相关联的URL在网络中的节点之间交换数据的方法。鉴于上述情况,当前需要与常规数据中心相比更加安全、生态化且负担得起的数据通信系统。

## 发明内容

[0012] 本公开旨在提供改进的数据通信系统。

[0013] 此外,本公开旨在提供传输数据的改进方法。

[0014] 本公开的另一目的在于至少部分克服如前所述的现有技术的至少一些问题。

[0015] 在第一方面,本公开的实施方式提供用于本地网络的数据通信系统,该数据通信系统包括至少一个网络节点以及与至少一个网络节点相关联的多个网络设备,其特征在于:

[0016] -至少一个网络节点配置成向在多个网络设备上执行的多个客户端或机器人程序 (bot) 提供网络节点服务,其中多个客户端或机器人程序中的各个客户端或机器人程序可通信地且仅以程序化星形配置以编程方式耦接在网络节点服务周围以形成本地网络,而且其中,网络节点服务配置成验证和认证由本地网络内的多个客户端或机器人程序提供的本地服务;

[0017] -源客户端或机器人程序配置成通过经由网络节点服务中继数据,来实时或接近实时地将数据传输到本地网络内的一个或多个目标客户端或机器人程序;以及

[0018] -源客户端或机器人程序配置成在将数据传输到一个或多个目标客户端或机器人程序之前对数据的信息内容进行加密,其中源客户端或机器人程序配置成采用密钥存储库来加密数据的信息内容,该密钥存储库与源客户端或机器人程序的用户相关联。

[0019] 本公开的実施方式的优点在于,数据通信系统使得用户能够通过使用在本地网络中的有效集成的本地网络设备上执行的客户端或机器人程序来产生供自己使用的服务,同时保护由关于客户端或机器人程序的用户的服务产生的数据。

[0020] 在第二方面,本公开的實施方式提供经由用于本地网络的数据通信系统来传输数据的方法,该数据通信系统包括至少一个网络节点以及与至少一个网络节点相关联的多个网络设备,其特征在于,该方法包括:

[0021] -经由至少一个网络节点向在多个网络设备上执行的多个客户端或机器人程序提供网络节点服务,其中多个客户端或机器人程序中的各个客户端或机器人程序可通信地且仅以程序化星形配置以编程方式耦接在网络节点服务周围以形成本地网络,而且其中,网络节点服务配置成验证和认证由本地网络内的多个客户端或机器人程序提供的本地服务;

[0022] -通过经由网络节点服务中继数据,来实时或接近实时地将数据从源客户端或机器人程序传输到本地网络内的一个或多个目标客户端或机器人程序;以及

[0023] -在将数据传输到一个或多个目标客户端或机器人程序之前,在源客户端或机器人程序处对数据的信息内容进行加密,其中密钥存储库被用来加密数据的信息内容,该密钥存储库与源客户端或机器人程序的用户相关联。

[0024] 在第三方面,本公开的實施方式提供计算机程序产品,该计算机程序产品包括其上存储有计算机可读指令的非暂时性(即非瞬时性)计算机可读存储介质,这些计算机可读指令可由包括处理硬件的计算机化设备执行以执行根据前述第二方面的前述方法。

[0025] 从附图以及结合以下所附权利要求书解释的说明性實施方式的详细描述中,本公开的附加方面、优点、特征和目的将变得显而易见。

[0026] 应当理解,在不脱离由所附权利要求限定的本公开的范围的情况下,本公开的特征易于以各种组合进行组合。

## 附图说明

[0027] 当结合附图阅读时更好地理解以上发明内容及以下对说明性實施方式的详细描述。为了说明本公开,在附图中示出了本公开的示例性构造。然而,本公开不限于本文所公开的特定方法和设备。此外,本领域的技术人员将理解附图不是按比例绘制的。在任何可能之处,相同的元件已经由相同的标号指示。

[0028] 现在将参考以下各图仅以举例方式描述本公开的實施方式,在附图中:

[0029] 图1是根据本公开的實施方式的数据通讯系统的示意图;

[0030] 图2是根据本公开的實施方式的示例性本地网络的示意图;

[0031] 图3是根据本公开的實施方式的另一示例性本地网络的示意图;

[0032] 图4A和图4B是根据本公开的實施方式的客户端或机器人程序可以如何与来自不同本地网络的另一客户端或机器人程序进行通信的示意图;以及



[0033] 图5是根据本公开的实施方式在数据通信系统中定义的多个组的示意图。

[0034] 在附图中,带下划线数字用于表示带下划线数字所在的项或者带下划线数字所邻近的项。当数字不带下划线并且附有相关联箭头时,不带下划线的数字用于标识箭头所指向的一般项。

### 具体实施方式

[0035] 在以下具体实施方式中,说明了本公开的实施方式及其实现的方式。虽然描述了执行本公开的一些模式,但是本领域的技术人员将认识到,用于执行或实践本公开的其他实施方式也是可能的。

[0036] 在第一方面,本公开的实施方式提供一种用于本地网络的数据通信系统,该数据通信系统包括至少一个网络节点以及与至少一个网络节点相关联的多个网络设备,其特征在于:

[0037] -至少一个网络节点配置成向在多个网络设备上执行的多个客户端或机器人程序(bot)提供网络节点服务,其中多个客户端或机器人程序中的各个客户端或机器人程序可通信地且仅以程序化星形配置以编程方式耦接在网络节点服务周围以形成本地网络,而且其中,网络节点服务配置成验证和认证由本地网络内的多个客户端或机器人程序提供的本地服务;

[0038] -源客户端或机器人程序配置成通过经由网络节点服务中继数据,来实时或接近实时地将数据传输到本地网络内的一个或多个目标客户端或机器人程序;以及

[0039] -源客户端或机器人程序配置成在将数据传输到一个或多个目标客户端或机器人程序之前对数据的信息内容进行加密,其中源客户端或机器人程序配置成采用密钥存储库来加密数据的信息内容,该密钥存储库与源客户端或机器人程序的用户相关联。

[0040] 可选地,至少一个网络节点包括至少第一网络节点和第二网络节点,并且多个网络设备包括与第一网络节点相关联的第一组网络设备以及与第二网络节点相关联的第二组网络设备。可选地,在这种情况下,第一网络节点配置成向在第一组网络设备上执行的第一组客户端或机器人程序提供第一网络节点服务,而第二网络节点配置成向在第二组网络设备上执行的第二组客户端或机器人程序提供第二网络节点服务。可选地,就这一点而言,第一组客户端或机器人程序中的各个客户端或机器人程序可通信地且仅以程序化星形配置以编程方式耦接在第一网络节点服务周围以形成第一本地网络,而第二组客户端或机器人程序中的各个客户端或机器人程序可通信地且仅以程序化星形配置以编程方式耦接在第二网络节点服务周围以形成第二本地网络,而且其中,第一网络节点服务和第二网络节点服务配置成验证和认证由它们相应的本地网络内的第一组客户端或机器人程序和第二组客户端或机器人程序提供的本地服务。

[0041] 可选地,当给定的源客户端或机器人程序配置成将数据传输到同一本地网络内的给定的目标客户端或机器人程序时,通过它们在同一本地网络内的相关网络节点服务实时或接近实时地中继将要传输的数据。

[0042] 可选地,当给定的源客户端或机器人程序配置成将数据从不同的本地网络传输到给定的目标客户端或机器人程序时,通过与给定的源客户端或机器人程序相关联的网络节点服务并且通过与给定的目标客户端或机器人程序相关联的网络节点服务来实时或接近

实时地中继将要传输的数据。例如,当来自第一本地网络的源客户端或机器人程序配置成将数据从第二本地网络传输到目标客户端或机器人程序时,通过第一网络节点服务和第二网络节点服务实时或接近实时地中继将要传输的数据。

[0043] “实时或接近实时地”是指在上述数据通信系统中,客户端或机器人程序可以立即或以可忽略的等待时间交换数据。这种延迟在上述数据通信系统的各种实际应用中保持最小是至关重要的。例如,当上述数据通信系统用于自动驾驶车辆和/或用于车辆监视目的、例如用于自主自动驾驶车辆的乘客安全时,这种实时或接近实时的通信是非常有益的。

[0044] 应当理解,给定的网络设备可以由给定的用户拥有、管理或租赁。贯穿本公开,术语“用户”是指使用在一个或多个网络设备上执行的一个或多个客户端或机器人程序的实体或一组实体,其中一个或多个网络设备可以由实体或一组实体拥有、管理或租赁。术语“实体”涵盖人类用户以及与人类用户相关联的用户设备。

[0045] 贯穿本公开,术语“客户端”和“机器人程序”是指当在网络设备上执行时为程序模块的用户产生本地服务的程序模块。

[0046] 此外,可选地,源客户端或机器人程序配置成采用存储在密钥存储库中的至少一种密钥材料来加密数据的信息内容。

[0047] 可选地,源客户端或机器人程序配置成将元数据与数据一起传输。可选地,就这一点而言,元数据包括指示密钥存储库的唯一标识符(ID)以及将要从密钥存储库导出的密钥材料的密钥索引的加密信息,以用于随后对加密的信息内容进行解密。应当理解,可以存在与源客户端或机器人程序的用户相关联的多个密钥存储库,多个密钥存储库专用于不同的服务提供商;在这种情况下,密钥存储库的唯一ID标识多个密钥存储库中的哪个密钥存储库将用于加密/解密目的。

[0048] 根据本公开的实施方式,源客户端或机器人程序以及一个或多个目标客户端或机器人程序被设置有密钥存储库的相同的或相互兼容的副本。可选地,密钥存储库由源客户端或机器人程序中的任一个或者一个或多个目标客户端或机器人程序来提供。可替代地,可选地,密钥存储库由受信任的第三方来提供。应当理解,即使未授权方访问了加密的信息内容,也不会造成伤害,因为未授权方无法访问相关的密钥存储库及其密钥材料。

[0049] 可选地,密钥存储库通过密钥容器或密钥生成器来实现,该密钥容器或密钥生成器能够以可再现的方式存储密钥材料和/或基于其密钥索引来生成密钥材料。“可复制”是指从给定的密钥索引可重复生成相同的密钥材料。作为示例,可以如英国专利文件GB2538052中描述地来实现密钥存储库。作为另一个示例,可以如英国专利文件GB1620553.6中描述地来实现密钥存储库。

[0050] 此外,可选地,元数据进一步包括组信息,该组信息指示数据将被传输到的一个或多个目标客户端或机器人程序。可选地,源客户端或机器人程序以及一个或多个目标客户端或机器人程序一起形成组。

[0051] 可选地,在数据通信系统内以动态方式定义多个组,其中,多个组中的给定组包括:

[0052] -来自第一本地网络的至少一个客户端或机器人程序,以及来自第二本地网络的至少一个客户端或机器人程序,或者

[0053] -来自同一本地网络的至少两个客户端或机器人程序。

[0054] 可选地,为数据通信系统的每个组分配唯一的组标签。可选地,在这种情况下,元数据的组信息包括该组的、包括源客户端或机器人程序以及一个或多个目标客户端或机器人程序的组标签。

[0055] 应当理解,“以动态方式”定义多个组意味着组可以基于个体情况和要求而变化,并且组结构可以在不同的时间点不同。

[0056] 还应当理解,元数据的前述加密信息和前述组信息使得数据通信系统能够执行到目标客户端或机器人程序的快速且可靠的数据递送。

[0057] 可选地,元数据通过一个或多个数据流进行通信。

[0058] 根据实施方式,元数据以未加密的形式通信。在这种情况下,给定的网络节点服务基于元数据将数据的加密信息内容递送(即中继)到所需方,即一个或多个目标客户端或机器人程序,而无需处理加密信息内容。换句话说,只有可能包含敏感信息的数据信息内容才被加密;给定的网络节点服务不需要解密加密的信息内容并重新对其进行加密。因此,给定的网络节点服务不会损害关于源客户端或机器人程序的用户的任何敏感信息。显然,提供给定网络节点服务的给定网络节点可以在任何种类的环境中、使用不需要具有用于保护数据的任何安全性增强的任何种类的设备来实现。

[0059] 根据另一个实施方式,元数据以加密形式进行通信。在这种情况下,需要将网络节点服务实现为具有其自己的密钥存储库以及与密钥存储库相关联的合适的安全模块(即客户端或机器人程序),以便保护密钥存储库免受未授权的访问和使用,其中安全模块(即客户端或机器人程序)配置成执行实际的加密和解密操作。这需要来自执行网络节点服务的网络节点的硬件隔离安全特征。应当理解,当期望隐藏跟踪信息时,以加密形式传输元数据特别有益,从而使得窃听第三方不可能认识到什么类型的数据流正在被传输并且利用其正在进行通讯。这潜在地提高了数据通信系统的成本效率。

[0060] 然而,应当理解,如果没有理由隐藏跟踪信息,则不需要加密元数据。

[0061] 贯穿本公开,术语“网络节点”是指配置成提供网络节点服务的物理网络节点,使得网络节点服务以编程方式集中化到在其自己的本地网络中的网络设备上执行的服务客户端或机器人程序。应当理解,本地网络的物理实施方式不需要其网络节点和网络设备以星形网络拓扑布置。换句话说,客户端或机器人程序仅以程序化星形配置以编程方式耦接在网络节点服务周围。贯穿本公开,术语“程序化星形配置”是指由网络节点服务及其关联的客户端或机器人程序形成的软件拓扑。

[0062] 此外,网络节点可以通过数据通信设备(例如调制解调器、集线器等)或者通过数据终端设备(例如路由器、主机等)来实现。可选地,给定的网络节点通过程序化集线器或程序化路由器来实现。

[0063] 此外或可替代地,可选地,给定的网络节点通过本地网络设备动态地实现,其中本地网络设备配置成使用以编程方式构建的星形配置与其他本地网络设备连接并通信。

[0064] 本公开的实施方式易于在广泛的系统中采用,其中网络设备可以例如是智能电话、智能手表、个人计算机(PC)、车辆的车载诊断(OBD)设备、视听设备、摄像机、电视机、数据存储设备、监控摄像机、视频会议设备、电子邮件服务器、文件系统、媒体播放器、医疗设备、地震设备、测量设备、“黑匣子”飞行记录器或数码乐器。

[0065] 应当理解,可以将给定的网络节点服务安装在固定的物理位置或物理移动物体

处。此类移动物体的示例包括但不限于无人机、车辆、其用户携带的智能电话、其用户携带的智能手表、以及其他移动或可穿戴设备。

[0066] 因此,术语“本地网络”涵盖物理(即,静态)网络以及以移动方式实现的网络。贯穿本公开,术语“本地网络”是指将通过实施应用层(OSI L7)创建的本地传输网络,该应用层与由客户端或机器人程序提供的本地服务直接交互(例如,由客户端或机器人程序提供的软件应用),而无需任何外部传输网络。值得注意的是,通常需要外部传输网络在两个或多个本地传输网络之间传输数据。

[0067] 可选地,数据通信系统的本地网络经由在其网络节点上执行的网络节点服务而相互互连,以形成网状网络(参见[https://en.wikipedia.org/wiki/Mesh\\_networking](https://en.wikipedia.org/wiki/Mesh_networking))。已经结合图1示出一个这种网状网络。可选地,出于网格计算目的而形成网状网络(参见[https://en.wikipedia.org/wiki/Grid\\_computing](https://en.wikipedia.org/wiki/Grid_computing))。应当理解,仅在需要时才使用在数据通信系统的网络设备上执行的不同客户端或机器人程序,并且它们可以通过互连(例如,通过网格计算)共享以组合大量的计算资源。因此,数据通信系统能够提供对常规数据中心更安全、更生态和更负担得起的替代方案。此外,可以使用移动或可穿戴设备来实现数据通信系统的给定本地网络,以基于动态移动的网格网络通过各种客户端或机器人程序来提供所需服务。

[0068] 应当理解,给定的网络设备配置成执行给定的客户端或机器人程序,以向在一个或多个其他网络设备上执行的一个或多个客户端或机器人程序提供所需服务。应当理解,两个给定网络设备之间的实际数据通信由在两个给定的网络设备上执行的客户端(参见[https://en.wikipedia.org/wiki/Client\\_\(computing\)](https://en.wikipedia.org/wiki/Client_(computing)))或机器人程序(参见[https://en.wikipedia.org/wiki/Software\\_agent](https://en.wikipedia.org/wiki/Software_agent))执行。可选地,默认情况下,给定的客户端或机器人程序永久连接到由其关联的网络节点提供的网络节点服务。因此,提供了一种解决方案,该解决方案使得能够在网络设备的本地网络中提供本地服务,从而替代了由常规数据中心当前提供的服务。

[0069] 应当理解,给定的机器人程序能够向给定的机器人程序的用户和所需的第三方提供来自可能不受保护的网络设备以及在其上执行的软件的保护服务。换句话说,由于数据以加密形式存储在两个端点处,即,执行源客户端或机器人程序的网络设备以及执行一个或多个目标客户端或机器人程序的一个或多个网络设备,因此根据本公开的实施方式的数据通信系统提供了改进的保护。

[0070] 根据本公开的实施方式,服务由连接至由其对应的网络节点提供的网络节点服务的客户端或机器人程序以编程方式提供。这使得可以在硬件独立的跨平台软件解决方案上产生此类服务。换句话说,可以在具有不同目标平台的网络设备(例如x86/x64/AArch64等)上执行给定服务的相同功能。

[0071] 在本公开的实施方式中,给定的网络节点服务配置成仅处理两个给定的客户端或机器人程序之间的兼容连接。可选地,就这一点而言,给定的网络节点服务配置成在本地和远程支持广泛的互不相同的应用程序和服务,例如:

[0072] -类似FaaS的云计算种类的执行模型(参见[https://en.wikipedia.org/wiki/Serverless\\_computing](https://en.wikipedia.org/wiki/Serverless_computing));

[0073] -类似PaaS的应用程序平台,用于管理和运行应用程序,而没有相关联的用于开发

和执行它们的典型基础架构(参见[https://en.wikipedia.org/wiki/Platform\\_as\\_a\\_service](https://en.wikipedia.org/wiki/Platform_as_a_service));以及

[0074] -集中托管的类似SaaS的软件交付模型(参见[https://en.wikipedia.org/wiki/Software\\_as\\_a\\_service](https://en.wikipedia.org/wiki/Software_as_a_service))。

[0075] 为了支持各种互不相同的应用程序和服务,客户端或机器人程序配置成为数据通信系统的用户执行某些功能,无论用户是否具有接口。

[0076] 可选地,就这一点而言,机器人程序被实现为软件代理,该软件代理配置成以代理关系来代理用户、程序或服务。可选地,此类软件代理被定义成三种类型的机器人程序:协议机器人程序、客户端机器人程序和服务器机器人程序,它们是为了不同的目的而定义的,从而为第三方服务提供商提供有效的应用程序编程接口(API),以根据本公开的实施方式开发并且可选地基于数据通信系统将其服务货币化。应当理解,这些类型的机器人程序提供了接口,该接口使得来自私有或公共网络的不同设备和服务能够与数据通信系统的网络设备建立受保护的连接。“受保护的连接”是指由设备和服务产生的数据使用加密来进行保护,并且通过本地网络的网络节点服务经由中继来传递。因此,保护数据免受本地网络内部和外部引起的传统形式的攻击。此外,传统形式的攻击不可能窃听数据的加密信息内容。

[0077] 可选地,协议机器人程序配置成转换不同的通信和命令协议以支持由数据通信系统的网络设备提供的服务。作为示例,给定的协议机器人程序可以配置成在不同的目标平台上连接不同类型的媒体播放器,以支持由产生视听内容的网络设备提供的服务(例如监控摄像机、电视、回放视频等等)。换句话说,给定的协议机器人程序可以配置成根据目标设备调整传输数据的信息内容及其内容格式。例如,可以如英国专利文件GB2514543中描述地进行这种调整。无论目标设备的内置生态系统软件如何,都可以使用由此类机器人程序提供的服务来根据目标设备的给定平台调整信息内容。

[0078] 可选地,协议机器人程序是媒体播放器机器人程序,其配置成根据与其相关联的媒体播放器来翻译视听信息。媒体播放器可以在本地设备或远程连接设备上执行,其中媒体播放器机器人程序被耦接到媒体播放器。可选地,在这种情况下,媒体播放器机器人程序配置成在传递视频和音频之前,将视频和音频调整成与连接设备的媒体播放器兼容的格式。连接设备的媒体播放器随后渲染从机器人程序接收的视频和音频。可选地,就这一点而言,媒体播放器机器人程序配置成识别并理解连接设备的媒体播放器的技术要求,从而将视频和音频调整成从传输协议的角度以及从视频格式和音频格式的角度与连接设备兼容的格式。作为示例,用户的移动电话的媒体播放器可以使用由媒体播放器机器人程序提供的服务来在世界上随时随地访问TV或摄像机视频馈送。

[0079] 可选地,客户端机器人程序配置成充当用户的应用程序以提供不同类型的特征。作为示例,给定的客户端机器人程序可以配置成提供视频记录和回放的特征,其中给定的用户被提供图形用户界面(GUI)以选择视频。作为另一个示例,给定的客户端机器人程序可以配置成基于人工智能(AI)来提供护士或医生的特征,以潜在地帮助用户。

[0080] 可选地,服务器机器人程序配置成充当服务器以提供期望服务。作为示例,给定的服务器机器人程序可以配置成根据给定用户的个人需求来提供电子邮件服务。作为另一个示例,给定的服务器机器人程序可以配置成托管公司的用户数据库,以支持现有信息系统上的不同类型的登录界面。

[0081] 可选地,服务器机器人程序是配置成充当根据用户的个人需求提供电子邮件服务的电子邮件服务器的电子邮件机器人程序。可选地,电子邮件机器人程序配置成启用各种功能,例如安全的电子邮件和垃圾邮件防护。

[0082] 此外,应当理解,可以在同一物理设备或单独的物理设备中实现给定的网络节点服务和给定的客户端或机器人程序。技术上适用于实现给定网络节点服务和给定客户端或机器人程序的目标软件平台的示例包括但不限于**Unix<sup>®</sup>**、**Linux<sup>®</sup>**、**Windows<sup>®</sup>**、**OS**

**X<sup>®</sup>**、**Android<sup>®</sup>**和**iOS<sup>®</sup>**。值得注意的是,给定目标软件平台上的选定生态系统定义了有效实施方式的要求以及编程语言和工具的要求。因此,根据本公开的实施方式的数据通信系统有利地设计成在Gurulogic微系统的**Starwindow<sup>®</sup>**生态系统中工作,该生态系统提供了**Starwindow<sup>®</sup>**框架应用程序编程接口(API)以支持高级开发环境来允许在数据通信系统中使用第三方服务。此外,**Starwindow<sup>®</sup>**生态系统是基于多层架构构建的,其中除针对给定目标平台的服务以外的所有其他事物都是基于硬件独立的软件解决方案构建的。

[0083] 可选地,给定的网络节点是通过采用异步网络库(IOLoop)技术通过低功耗中央处理器(CPU)来实现的。即使使用低功耗CPU,也可以通过编程方式传递网络节点服务。通过使用IOLoop技术,将给定的网络节点配置成在一个线程中处理与网络节点服务的所有连接。与在一个或多个CPU内核中执行的为每个连接提供专用线程的常规已知方法相比,这实现了显著更有成本效益的输入/输出(I/O)通信和技术上更快的实施方案。作为示例,用于移动通信设备的当代通信技术被设计成以最小的能耗工作;因此,将IOLoop技术用于新的目的提供了如参考本公开的实施方式描述的高度有成本效益的解决方案。

[0084] 此外,如前所述,给定的网络节点服务配置成验证和认证由客户端或机器人程序在其自己的本地网络内提供的本地服务。可选地,就这一点而言,给定的网络节点服务配置成在客户端或机器人程序加入本地网络时,利用接受的凭证对由这些客户端或机器人程序提供的本地服务进行认证。

[0085] 此外或可替代地,可选地,认证请求由注册服务来验证和认证。可选地,就这一点而言,数据通信系统配置成利用注册服务来注册由第一本地网络和第二本地网络的客户端或机器人程序提供的服务。

[0086] 可选地,每个客户端或机器人程序具有其自己的密钥存储库,该密钥存储库存储使用该客户端或机器人程序的用户的凭证。取决于需要验证的认证请求,凭证用于登录服务并且认证用户。可选地,用户的凭证(存储在密钥存储库中)用于加密将要通信的数据和/或执行后续解密。

[0087] 作为示例,可以如英国专利文件GB2554082中描述地来实现认证。作为另一示例,可以使用摘要认证技术来实现认证。应当理解,认证是按照通用数据保护条例(GDPR)实施的。

[0088] 此外,可选地,注册服务用于注册服务及其客户端或机器人程序的连接地址。

[0089] 可选地,数据通信系统配置成利用注册服务来注册由给定客户端或机器人程序提供的给定服务作为针对给定客户端或机器人程序的用户的私有服务或公共服务。可选地,在给定的本地服务经过验证和认证之后,给定的本地服务被注册为给定的客户端或机器人程序的用户的私有服务或公共服务。

[0090] 应当理解,这种注册使得给定用户更容易维护和配置针对给定用户注册的所有服务。作为示例,第三方服务提供商可以构建其自己的服务并且利用注册服务来注册这些服务;在这种情况下,第三方服务提供商是这些服务的用户,并且将这些服务提供给各个远程用户。可选地,注册服务配置成为给定用户提供用户界面,该用户界面允许给定用户在成功登录后查看给定用户的本地网络中可用的所有服务,并且启用或禁用某些服务以供使用。

[0091] 可选地,注册服务由数据通信系统中定义的“超节点”提供为集中后端服务。可选地,从第一网络节点和第二网络节点中选择提供注册服务的节点。可替代地,可选地,超节点由第三方提供。

[0092] 应当注意,超节点以静态方式工作,而网络节点是动态的。

[0093] 可选地,数据通信系统配置成以硬件独立的方式起作用,其中在由给定用户拥有、管理或租赁的网络设备中产生安全服务。可选地,就这一点而言,由这些服务产生的所有数据针对给定用户,即,使用与给定用户相关联的密钥存储库进行保护。

[0094] 可选地,在给定的网络设备中,由在给定的网络设备上执行的客户端或机器人程序提供的给定服务与和客户端或机器人程序的用户相关联的密钥存储库集成,使得仅允许与密钥存储库集成的服务访问密钥存储库并使用在其中存储或生成的密钥材料。可选地,一旦与密钥存储库集成,该服务就在受到给定网络设备的内核的保护的情况下由在给定的网络设备上执行的客户端或机器人程序提供。

[0095] 可选地,通过使用一种或多种内容加密方法来加密数据的信息内容。可选地,通过使用例如高级加密标准(AES)的对称加密块密码算法(参见[https://en.wikipedia.org/wiki/Block\\_cipher](https://en.wikipedia.org/wiki/Block_cipher))的形式来实现内容加密。可替代地,可选地,通过使用例如ChaCha算法的流密码算法(参见[https://en.wikipedia.org/wiki/Stream\\_cipher](https://en.wikipedia.org/wiki/Stream_cipher))来实现内容加密。这种内容加密使得数据通信系统能够可靠地运行并且以使得数据的内容关于其合法所有者受到保护的方式来处理其中产生的数据。

[0096] 应当理解,在一些情况下,用户可以是应当针对其保护数据的一组用户或设备。在这种情况下,即使该组通常由该组的一个成员管理,其他组成员也能够根据预定义的组规则访问由该组产生的数据并向该组产生数据。可选地,就这一点而言,为特定目的定义组,其中允许组成员以安全的方式存储和访问未指定的数据。作为示例,该组可以是电话组,其中组成员可以存储和访问在属于该组成员的多个电话之间交换的数据。作为另一个示例,该组可以是摄像机组,其中组成员可以存储和访问由多个摄像机捕获的图像数据。作为又一示例,该组可以是协商组,其中组成员可以彼此协商。

[0097] 可选地,根据给定用户的认证,至少一个服务与一个或多个注册用户远程共享。应当理解,数据通信系统允许给定用户使用本地资源(即,网络设备)产生自己的服务,并且与远程用户共享这些服务而不损害安全性。

[0098] 此外,可选地,给定用户被设置有用户界面,该用户界面允许给定用户控制由至少一项服务产生的数据被泄露给第三方并且随后用于各种目的(例如促销、定向广告等等)的程度。因此,例如,搜索引擎无法在没有来自给定用户的许可的情况下访问给定用户的受保护的数据并使用它。这使得能够实现更安全的信息社会。

[0099] 此外,可选地,在数据通信系统中,以动态方式创建给定的本地网络。可选地,就这一点而言,通过实现应用程序层(OSI L7),将给定的本地网络动态地创建为程序化本地网

络,该应用程序层与经由在连接的网络设备上执行的客户端或机器人程序可用的本地服务直接交互。就这一点而言,由给定本地网络的网络节点提供的网络节点服务注册由在给定本地网络的连接的网络设备上执行的客户端或机器人程序提供的所有本地服务。更可选地,由不再连接或不可用的网络设备提供的服务被自动地从给定的本地网络中删除,而通过新连接的网络设备可用的新服务会被自动添加到给定的本地网络中。换句话说,可以将服务添加到给定的本地网络或从中将其删除。

[0100] 可选地,在网络设备上执行的客户端或机器人程序存在于动态网络环境中,其中客户端或机器人程序配置成在局域网(LAN)中查找集中式网络节点服务,而无需使用一个或多个发现协议进行预先配置。此类发现协议的示例包括但不限于服务位置协议(SLP;参见[https://en.wikipedia.org/wiki/Service\\_Location\\_Protocol](https://en.wikipedia.org/wiki/Service_Location_Protocol))和苹果公司的Bonjour协议(参见[https://en.wikipedia.org/wiki/Bonjour\\_\(software\)](https://en.wikipedia.org/wiki/Bonjour_(software)))。

[0101] 可替代地,可选地,以静态方式创建给定的本地网络。就这一点而言,可选地,客户端或机器人程序被静态寻址以连接到给定的网络节点服务。在静态网络环境中(例如,在同一网络设备内或者在受控的公司网络中)产生服务的情况下,这是特别有益的。

[0102] 此外,根据本公开的实施方式,定义了用于在数据通信系统中实现数据通信的通信协议,并且该通信协议在数据通信系统的网络设备上执行的客户端或机器人程序之间互相同意。可选地,就这一点而言,给定的网络节点服务配置成创建具有程序化星形配置的本地网络,并且与具有程序化星形配置的另一本地网络的至少一个其他网络节点服务互连。客户端或机器人程序通过其关联的网络节点服务经由中继彼此通信。因此,数据通信系统以通过编程方式构建的星形配置的形式来实施。值得注意的是,合适的内容加密方法有益地集成到通信协议中,以便以安全的方式处理在数据通信系统内产生的数据。

[0103] 根据本公开的实施方式,第一本地网络的客户端或机器人程序不直接与第二本地网络的客户端或机器人程序连接,而是通过第一网络节点服务和第二网络节点服务来中继数据。然而,应当理解,如果第二网络节点服务的连接地址是已知的并且可用于连接,则第一本地网络的客户端或机器人程序可以直接连接到第二网络节点服务,以将数据中继到第二本地网络的客户端或机器人程序。这将稍后结合图4A和图4B进行说明。

[0104] 可选地,数据通信系统配置成利用第一本地网络和第二本地网络中存在的一个或多个数据通信网络来进行数据通信。应当理解,以通信协议对于数据通信系统的所有客户端或机器人程序是实用且有效的方式来定义通信协议,因为该通信协议必须利用物理网络(例如有线以太网、无线Wi-Fi®网络、无线Li-Fi或无线蓝牙®连接)来基于分组数据的通信执行实际的数据传输任务。物理网络利用OSI模型的一个或多个上层。可选地,就这一点而言,将通过在现有网络层(OSI L3)上实现传输层(OSI L4)来创建物理网络。换句话说,物理网络利用基于L4层的接口。作为示例,出于家庭、办公室和工厂的工作目的,使用现有的有线或无线数据通信网络是有效的。这种数据通信网络通常采用互联网®协议(IP)。

[0105] 应当理解,为了支持应用层(OSI L7),需要支持传输层(OSI L4)、会话层(OSI L5)和表示层(OSI L6)。

[0106] 此外,可选地,在数据通信系统中,使用低能量通信技术(例如,蓝牙低功耗(BLE))或者通过利用某些专用的基于频率的通信技术来实现数据通信。这潜在地使参与这种低能耗数据通信的网络设备具有持久的电池寿命。



[0107] 可选地,通信协议在默认情况下技术上基于合适的分组数据通信协议。作为示例,通信协议可以基于互联网协议,例如传输控制协议/互联网协议(TCP/IP)。使用在私有和公共网络中广泛使用的通信协议是有利的,以便能够处理防火墙和防病毒服务的已知问题。

[0108] 应当理解,在数据通信系统内发生的数据通信对于物理网络基础设施是透明的。换句话说,可以使用有线或无线通信技术,只要它们能够适应相互同意的通信协议即可。作为示例,TCP/IP可以与**Wi-Fi®**和**蓝牙®**一起使用。

[0109] 如上所述,给定的网络节点服务尝试使用物理上可用的通信协议直接连接到其他网络节点服务。可选地,当使用互联网协议(IP)时,基于IPv4或IPv6连接地址使用直接连接。

[0110] 可选地,当无法建立直接连接时,例如在不同的局域网(LAN)中远程存在其他网络节点服务的情况下,给定的网络节点服务配置成采用基于NAT会话穿越应用程序(Session Traversal Utilities)的打孔技术(STUN;参见<https://en.wikipedia.org/wiki/STUN>)以遍历位于不同网络地址中的端点。然而,一些公司防火墙可能因为不允许使用用户数据报协议(UDP)而阻止基于STUN的技术。可选地,在这种情况下,给定的网络节点服务配置成采用基于中继穿越绕行NAT(Traversal Using Relays around NAT)的技术(TURN;参见<https://en.wikipedia.org/wiki/TURN>)。这将提供网络节点服务之间的连接性,但是将通过集中可用的服务路由所有通信。作为示例,可以通过由数据通信系统的超节点提供的前述注册服务来实现集中可用的服务。

[0111] 可选地,给定的网络节点服务配置成采用交互式连接建立(ICE;参见[https://en.wikipedia.org/wiki/Interactive\\_Connectivity\\_Establishment](https://en.wikipedia.org/wiki/Interactive_Connectivity_Establishment))以便连接到其他网络节点服务。应当理解,ICE技术结合了STUN和TURN技术。

[0112] 此外或可替代地,可选地,为了支持网络节点服务之间的直接连接,采用通用即插即用(UPnP;参见[https://en.wikipedia.org/wiki/Universal\\_Plug\\_and\\_Play](https://en.wikipedia.org/wiki/Universal_Plug_and_Play))联网协议以允许自动配置本地网络设备,例如路由器和防火墙,以打开网络节点服务之间的直接通信访问。然而,在这种情况下,正确实施认证以避免任何安全问题很重要。

[0113] 根据本公开的实施方式,与其中经由远程数据中心提供服务的常规数据通信系统相比,数据通信系统提供了经济高效且容错的解决方案,以用于为本地网络的网络设备中的给定用户提供服务。换句话说,与服务相关联的计算任务被卸载到本地网络,从而节省了能源利用。因此,以全面且更具成本效益的方式、即以更本地的方式为给定用户提供服务。因此,根据本公开的实施方式的数据通信系统不仅能够满足当今的需求,而且能够满足未来的需求,其中用户可以使用在本地网络中的高效集成的本地网络设备上执行的客户端或机器人程序来产生供自己使用的服务。此外,由服务生成的数据相对于客户端或机器人程序的给定用户受到保护。

[0114] 与基于物理上开放的本地网络中的连接设备的常规数据通信网络对比,根据本公开的实施方式的数据通信系统配置成在给定用户的本地网络中提供具有增加的数据保护功能的服务。由服务产生的数据使用内置的安全服务模块(即客户端或机器人程序)为给定用户进行保护,并且通过本地网络的网络节点服务经由中继来传递。因此,保护数据免受本地网络内部和外部引起的传统形式的攻击。此外,传统形式的攻击不可能窃听数据的加密信息内容。

[0115] 此外,上述数据通信系统使得用户能够将服务注册为公共或私人服务,并且与远程用户共享公共服务。换句话说,数据通信系统使得用户能够关于允许在哪里共享由给定服务产生的数据以及出于何种目的作出决定。因此,搜索引擎和其他第三方无法在没有来自用户的许可的情况下访问用户的受保护数据并使用它。这使得能够实现更安全的信息社会。

[0116] 在第二方面,本公开的实施方式提供一种经由用于本地网络的数据通信系统来传输数据的方法,数据通信系统包括至少一个网络节点以及与该至少一个网络节点相关联的多个网络设备,其特征在于,该方法包括:

[0117] -经由至少一个网络节点向在多个网络设备上执行的多个客户端或机器人程序提供网络节点服务,其中多个客户端或机器人程序中的各个客户端或机器人程序可通信地且仅以程序化星形配置以编程方式耦接在网络节点服务周围,从而形成本地网络,而且其中,网络节点服务配置成验证和认证由本地网络内的多个客户端或机器人程序提供的本地服务;

[0118] -通过经由网络节点服务中继数据来实时或接近实时地,将数据从源客户端或机器人程序传输到本地网络内的一个或多个目标客户端或机器人程序;以及

[0119] -在将数据传输到一个或多个目标客户端或机器人程序之前,在源客户端或机器人程序处对数据的信息内容进行加密,其中密钥存储库被用来加密数据的信息内容,密钥存储库与源客户端或机器人程序的用户相关联。

[0120] 以上公开的各种实施方式和变型经必要修正适用于该方法。

[0121] 可选地,至少一个网络节点包括至少第一网络节点和第二网络节点,并且多个网络设备包括与第一网络节点相关联的第一组网络设备以及与第二网络节点相关联的第二组网络设备。可选地,在这种情况下,该方法包括:经由第一网络节点向在第一组网络设备上执行的第一组客户端或机器人程序提供第一网络节点服务,并且经由第二网络节点向在第二组网络设备上执行的第二组客户端或机器人程序提供第二网络节点服务。可选地,就这一点而言,第一组客户端或机器人程序中的各个客户端或机器人程序可通信地且仅以程序化星形配置以编程方式耦接在第一网络节点服务周围以形成第一本地网络,而第二组客户端或机器人程序中的各个客户端或机器人程序可通信地且仅以程序化星形配置以编程方式耦接在第二网络节点服务周围以形成第二本地网络,而且其中,第一网络节点服务和第二网络节点服务配置成验证和认证由它们相应的本地网络内的第一组客户端或机器人程序和第二组客户端或机器人程序提供的本地服务。

[0122] 可选地,当给定的源客户端或机器人程序以及给定的目标客户端或机器人程序来自同一本地网络内时,该方法包括:通过它们在同一本地网络内的相关网络节点服务实时或接近实时地中继将要传输的数据。

[0123] 可选地,当给定的源客户端或机器人程序以及给定的目标客户端或机器人程序来自不同的本地网络时,该方法包括:通过与给定的源客户端或机器人程序相关联的网络节点服务并且通过与给定的目标客户端或机器人程序相关联的网络节点服务,来实时或接近实时地中继将要传输的数据。

[0124] 可选地,该方法还包括将元数据与数据一起从源客户端或机器人程序传输到一个或多个目标客户端或机器人程序,其中元数据包括指示密钥存储库的唯一ID以及将从密

钥存储库导出的密钥材料的密钥索引的加密信息,以用于随后对加密的信息内容进行解密。

[0125] 可选地,元数据还包括组信息,该组信息指示数据将被传输到的一个或多个目标客户端或机器人程序,其中源客户端或机器人程序以及一个或多个目标客户端或机器人程序一起形成组。

[0126] 可选地,元数据以未加密的形式进行通信。可替代地,可选地,元数据以加密形式进行通信。

[0127] 可选地,该方法还包括利用第一本地网络和第二本地网络中存在的一个或多个数据通信网络来进行数据通信。

[0128] 可选地,该方法还包括利用注册服务来注册由第一本地网络和第二本地网络的客户端或机器人程序提供的服务。可选地,如前所述,该方法还包括利用注册服务来注册由给定客户端或机器人程序提供的给定服务作为针对给定客户端或机器人程序的用户的私有服务或公共服务。

[0129] 可选地,如前所述,该方法还包括以动态方式创建给定的本地网络。

[0130] 在第三方面,本公开的实施方式提供一种计算机程序产品,该计算机程序产品包括其上存储有计算机可读指令的非暂时性计算机可读存储介质,这些计算机可读指令可由包括处理硬件的计算机化设备执行以执行前述第二方面的方法。

[0131] 接下来,将参考附图描述本公开的实施方式。

[0132] 图1是根据本公开的实施方式的数据通讯系统100的示意图。数据通信系统100包括多个网络节点102a、102b和102c、超节点104、以及多个网络设备106a、106b、106c、106d、106e、106f、106g、106h、106i、106j和106k(为方便起见以下统称为网络设备106)。网络节点102a、102b和102c配置成提供网络节点服务,而超节点104配置成提供注册服务。客户端在网络设备106d和106h上执行,而机器人程序在网络设备106a、106b、106c、106e、106f、106g、106i、106j和106k上执行。在图1中,网络设备106代表各种设备,例如电视机(TV)机、数据存储设备、监控摄像机、电子邮件服务器、文件系统、媒体播放器或者任何其他远程连接的设备。

[0133] 参考图1,在网络设备106a、106b和106c上执行的机器人程序以及在网络设备106d上执行的客户端可通信地耦接在由网络节点102a提供的网络节点服务周围,以形成本地网络108a。在网络设备106e、106f和106g上执行的机器人程序可通信地耦接在由网络节点102b提供的网络节点服务周围,以形成本地网络108b。在网络设备106h上执行的客户端以及在网络设备106i和106j上执行的机器人程序可通信地耦接在由网络节点102c提供的网络节点服务周围,以形成本地网络108c。在网络设备106k上执行的机器人程序可通信地耦接到由超节点104提供的注册服务,以形成本地网络108d。

[0134] 参考图1,由网络节点102a提供的网络节点服务连接到由网络节点102c提供的网络节点服务和由超节点104提供的注册服务,而由网络节点102b提供的网络节点服务连接到由超节点104提供的注册服务,从而形成网状网络。

[0135] 作为第一示例,在网络设备106a上执行的机器人程序是协议机器人程序,其可以配置成将电视(TV)机连接到由提供视听内容的网络设备提供的服务。此类服务的示例是Android TV API。

[0136] 作为第二示例,在网络设备106b上执行的机器人程序是可以配置成在与其相关联的数据存储设备处存储收集的统计数据的存储器机器人程序。这种统计数据可以被传输到不同服务或者从不同服务接收。统计数据的示例是TV和摄像机图像。

[0137] 作为第三示例,在网络设备106c上执行的机器人是协议机器人程序,其可以配置成连接不同目标平台上的不同类型的媒体播放器以支持由一个或多个监控摄像机提供的服务。

[0138] 作为第四示例,在网络设备106e上执行的机器人程序是服务器机器人程序,其可以配置成充当根据用户的个人需求提供电子邮件服务的电子邮件服务器。这种机器人程序可以启用各种功能,例如安全的电子邮件和垃圾邮件防护。

[0139] 作为第五示例,在网络设备106f上执行的机器人程序是服务器机器人程序,其可以配置成管理其文件系统。

[0140] 作为第六示例,在网络设备106g和106i上执行的机器人程序是协议机器人程序,其可以配置成根据远程连接设备的目标平台来翻译信息。

[0141] 作为第七示例,在网络设备106j和106k上执行的机器人程序是协议机器人程序,其可以配置成根据与其相关联的媒体播放器来翻译视听信息。这种媒体播放器可能正在本地设备或远程连接设备上执行。

[0142] 参考图1,在网络设备106k上执行的机器人程序被耦接到远程连接设备的媒体播放器。机器人程序配置成在传递视频和音频之前,将视频和音频调整成与连接设备的媒体播放器兼容的格式。连接设备的媒体播放器随后渲染从机器人程序接收的视频和音频。换句话说,机器人程序配置成识别并理解连接设备的媒体播放器的技术要求,从而将视频和音频调整成从传输协议的角度以及从视频格式和音频格式的角度与连接设备兼容的格式。作为示例,用户的移动电话的媒体播放器可以在世界上随时随地访问TV或摄像机视频馈送。

[0143] 图1仅是示例,其不应当过度限制本文的权利要求的范围。本领域的技术人员将认识到本公开的实施方式的许多变化、替代和修改。

[0144] 接下来参考图2,描绘了根据本公开的实施方式的示例性本地网络200。

[0145] 参考图2,本地网络200在车辆即汽车上物理地实现。本地网络200包括安装在车辆中的网络节点服务202以及与其相关联的机器人程序204a和204b。

[0146] 机器人程序204a配置成采用车辆的摄像机以便向拥有或管理车辆的用户提供各种服务。作为示例,可以收集并处理从周围环境捕获的图像,以提供更安全的交通控制。作为另一个示例,当车辆是出租车时,例如对于出租车的驾驶员和乘客两者,摄像机还可以提供安全特征。

[0147] 机器人程序204b配置成采用车辆的车载诊断(OBD)系统以便向拥有或管理车辆的用户提供各种服务。作为示例,可以出于各种目的处理从OBD系统收集的数据,例如用于提供紧急服务、用于防盗、用于碰撞检测和/或预防等。

[0148] 网络节点服务202经由基于例如**Wi-Fi®**、**蓝牙®**、**Li-Fi**等的无线通信接口连接到至少一个其他网络节点服务。至少一个其他网络节点服务可以是本地网络的在用户的家庭或办公室内物理可用的一部分。这允许用户例如在车辆是自动无人驾驶车辆或无人机的情况下远程监视车辆。

[0149] 图2仅是示例,其不应当过度限制本文的权利要求的范围。本领域的技术人员将认识到本公开的实施方式的变化、替代和修改。

[0150] 接下来参考图3,描绘了根据本公开的实施方式的另一示例性本地网络300。

[0151] 参考图3,本地网络300通过在由人类用户携带或佩戴的网络设备上执行的网络节点服务302、客户端304a和机器人程序304b来实现。值得注意的是,这些网络设备不是固定的或物理安装在用户身上的,而是仅由用户携带或穿戴的。可选地,网络节点服务302由用户的移动通信设备提供,例如智能电话、智能手表等。

[0152] 客户端304a配置成向用户提供各种服务,例如用于在用户的耳机上播放音乐、在用户的虚拟现实头戴式耳机上显示虚拟图像等。

[0153] 可选地,机器人程序304a配置成采用至少一个传感器来用于各种监测目的,例如用于监测用户的心率、用户执行的锻炼等。

[0154] 网络节点服务302经由基于例如**Wi-Fi®**、**蓝牙®**、**Li-Fi**等的无线通信接口连接到至少一个其他网络节点服务。作为示例,至少一个其他网络节点服务可以是本地网络的在用户的家庭内物理可用的一部分。作为示例,这可以允许家庭成员远程监测用户的健康状况。作为另一个示例,这可以允许远程监测提供给独自居住在他/她家中的老年人的护理服务。

[0155] 图3仅是示例,其不应当过度限制本文的权利要求的范围。本领域的技术人员将认识到本公开的实施方式的变化、替代和修改。例如,网络设备可以由生物携带或穿戴。

[0156] 图4A和图4B是根据本公开的实施方式的客户端或机器人程序402可以如何与来自不同本地网络的客户端或机器人程序404进行通信的示意图。

[0157] 参考图4A,客户端或机器人程序402不直接与客户端或机器人程序404连接,而是通过分别与客户端或机器人程序402以及客户端或机器人程序404相关联的第一网络节点服务406和第二网络节点服务408来中继数据。

[0158] 参考图4B,如果第二网络节点服务408的连接地址已知并且可用于连接,则客户端或机器人程序402直接连接到第二网络节点服务408以将数据中继到客户端或机器人程序404。

[0159] 图5是根据本公开的实施方式的在数据通信系统500中定义的多个组的示意图。

[0160] 数据通信系统500包括提供网络节点服务的网络节点502和504、包括执行客户端或机器人程序的网络设备506A、506B、506C、506D、506E、506F和506G的第一组网络设备、以及包括执行客户端或机器人程序的网络设备508A、508B、508C和508D的第二组网络设备。

[0161] 在网络设备506A、506B、506C、506D、506E、506F和506G上执行的客户端或机器人程序以程序化星形配置可通信地耦接在由网络节点502提供的网络节点服务周围,以形成第一本地网络,而在网络设备508A、508B、508C和508D上执行的客户端或机器人程序以程序化星形配置可通信地耦接在由网络节点504提供的网络节点服务周围,以形成第二本地网络。应当理解,第一本地网络和第二本地网络是通过实现应用层(OSI L7)来创建的,该应用层直接与由客户端或机器人程序提供的本地服务进行交互。

[0162] 参考图5,已经在数据通信系统500中定义了三个不同的组,其中在网络设备506A、506B、506D、506F、508A、508B和508D上执行的客户端或机器人程序形成第一组,在网络设备506G和508C上执行的客户端或机器人程序形成第二组,并且在网络设备506C和506E上执行

的客户端或机器人程序形成第三组。值得注意的是,给定组可能包括来自同一本地网络或来自不同本地网络的客户端或机器人程序。

[0163] 图4A至图4B和图5仅是示例,其不应当过度限制本文的权利要求书的范围。

[0164] 在不脱离由所附权利要求书限定的本公开的范围的情况下有可能对前文中所描述的本公开的实施方式做出修改。诸如“包括”、“包含”、“并入”、“由……组成”、“具有”、“是”的用于描述和要求保护本发明的表达旨在以非排他性方式解释,即允许未明确描述的项目、部件或元件也存在。对单数的引用还应被理解为与复数相关;作为示例,“至少一个”在一个示例中指示“一个”,并且在另一个示例中指示“多个”;此外,“一个或多个”将以类似方式解释。

[0165] 短语“在一个实施方式中”、“根据一个实施方式”等通常意味着跟随短语之后的特定特征、结构或特性包括在本公开的至少一个实施方式中,并且可以包括在本公开的多于一个实施方式中。重要的是,此类短语不一定指同一实施方式。

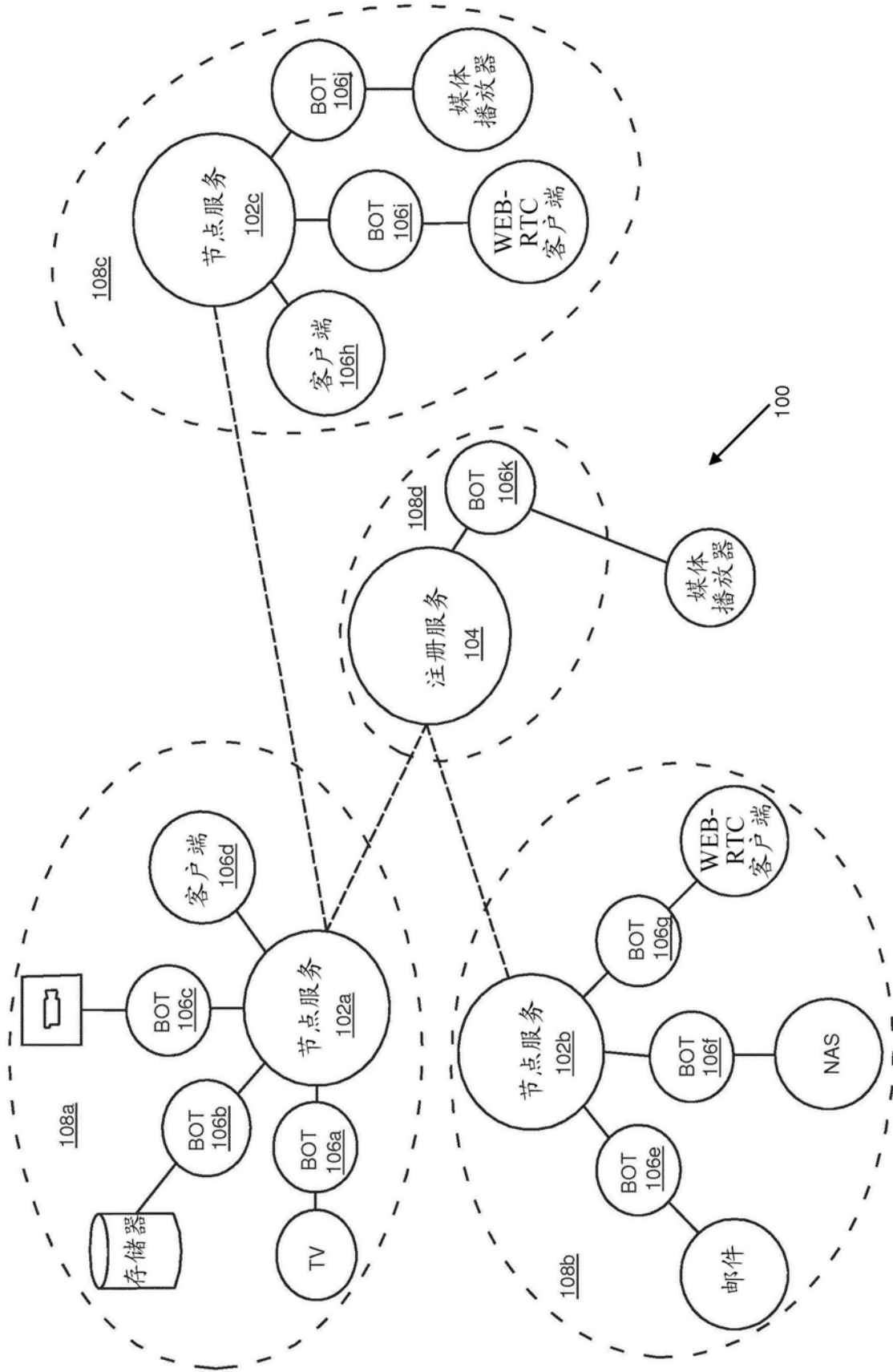


图1

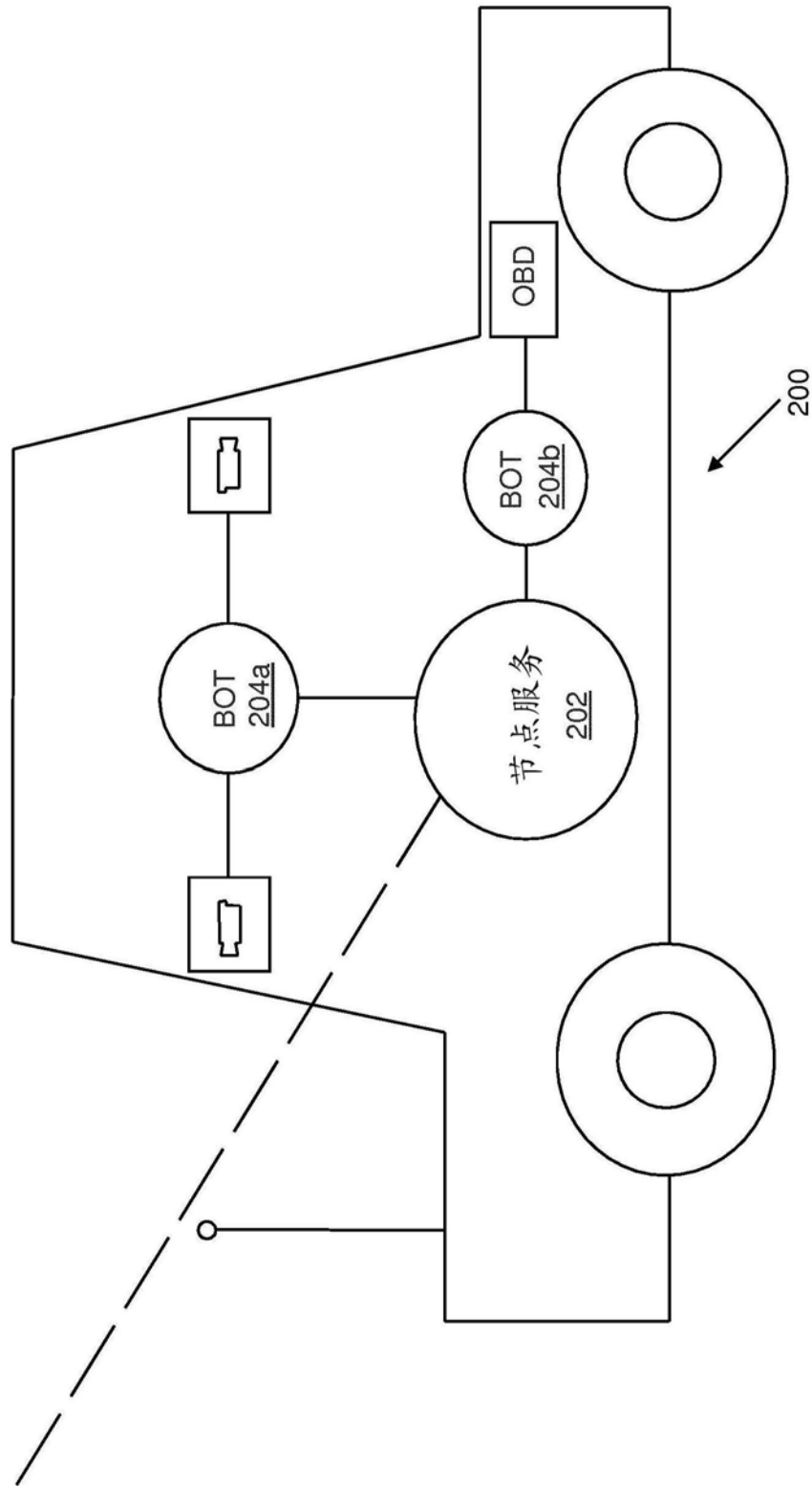


图2



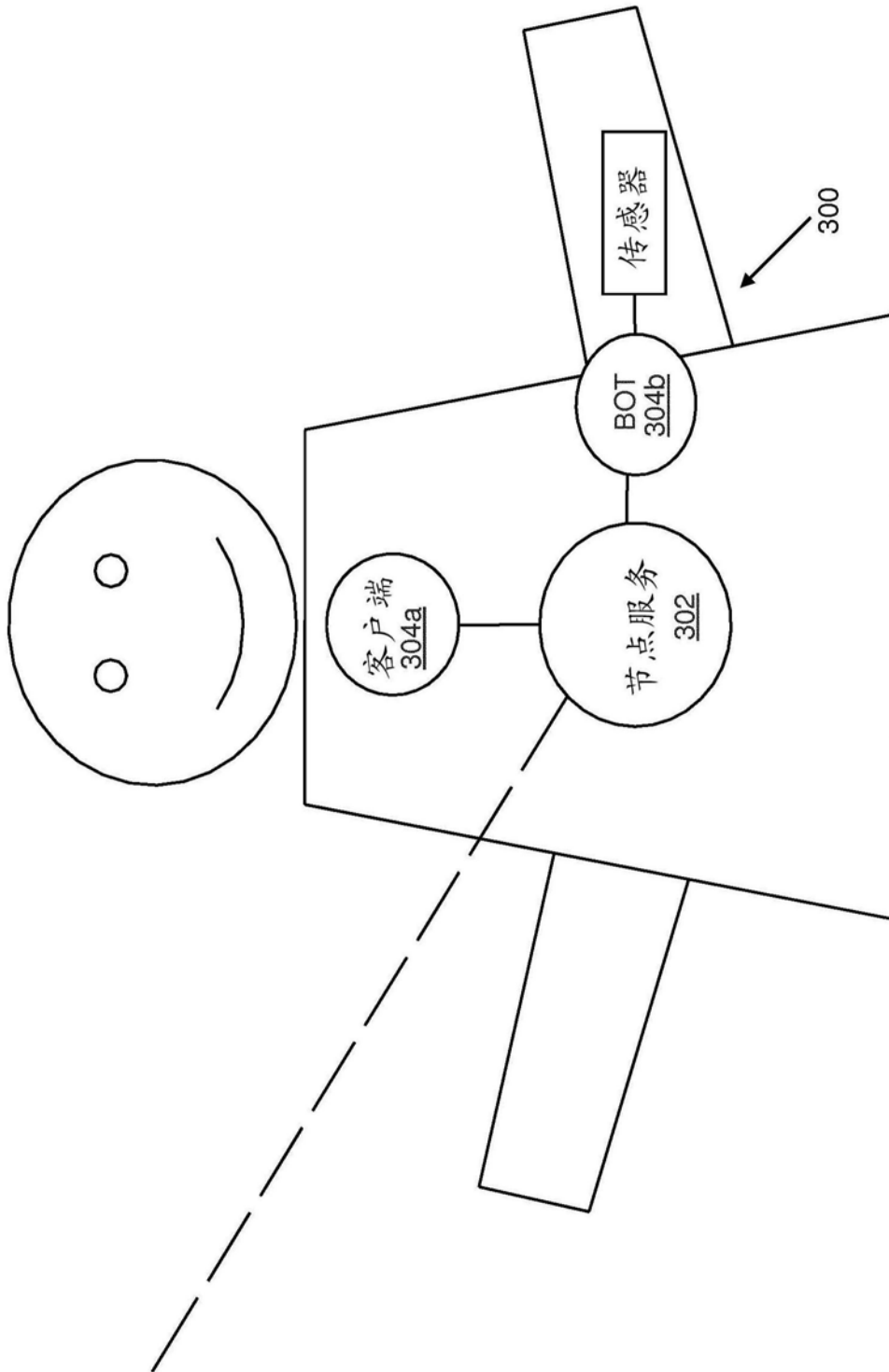


图3

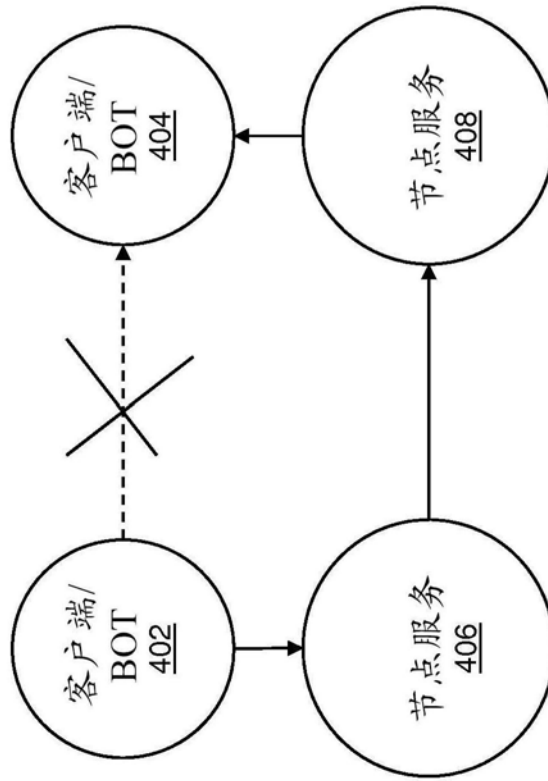


图4A

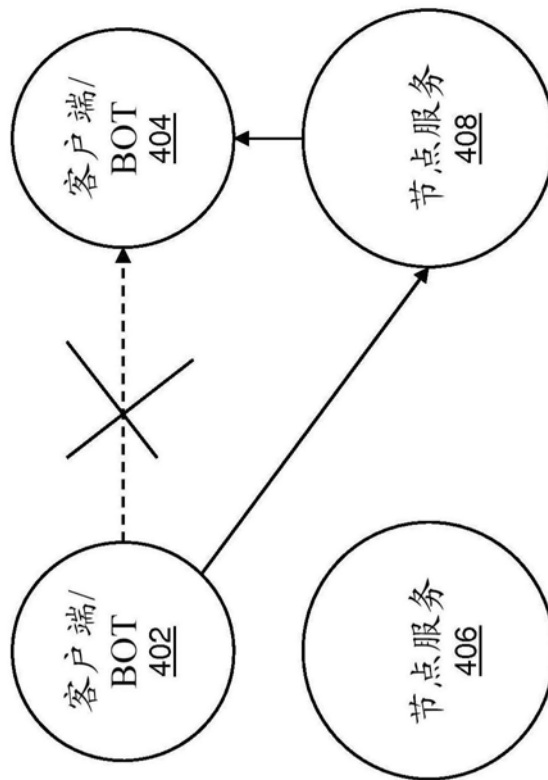


图4B

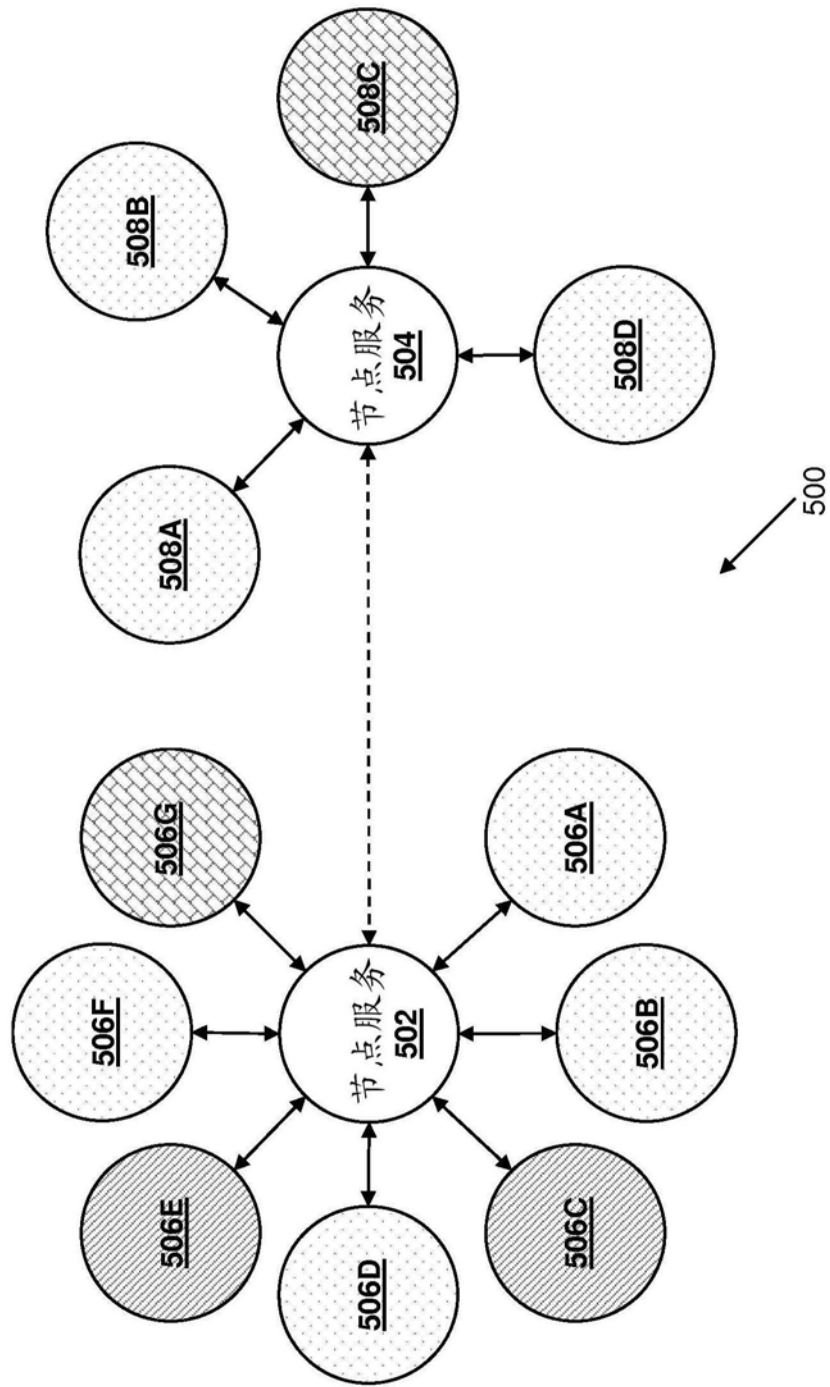


图5