(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 104980489 B
(45)授权公告日 2019.12.13

(21)申请号 201510131419.5

(22)申请日 2015.03.24

(65)同一申请的已公布的文献号
申请公布号 CN 104980489 A

(43)申请公布日 2015.10.14

(30)优先权数据
14/247165 2014.04.07 US

(73)专利权人 思科技术公司
地址 美国加利福尼亚州

(72)发明人 M·E·莫斯科

(74)专利代理机构 北京东方亿思知识产权代理有限责任公司 11258
代理人 孙洋

(51)Int.Cl.
H04L 29/08(2006.01)
H04L 9/32(2006.01)

(56)对比文件
US 2013282920 A1,2013.10.24,
CN 102640135 A,2012.08.15,
CN 103179110 A,2013.06.26,
CN 1484155 A,2004.03.24,

审查员 李嵩

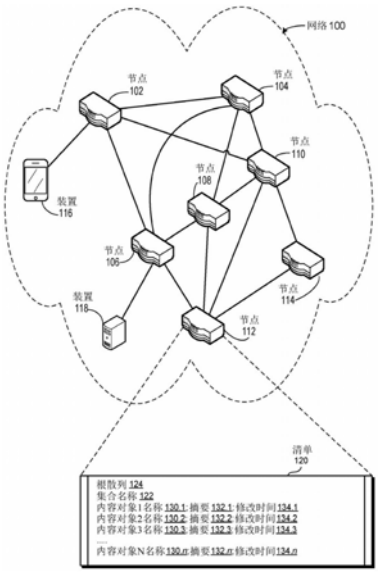
权利要求书1页 说明书16页 附图19页

(54)发明名称

使用匹配的网络名称的安全集合同步

(57)摘要

一个实施例提供一种促进使用确切网络名称促进清单的安全同步的系统。在操作期间,所述系统产生包括所述系统的内容对象的名称的播发兴趣。此名称表示所述系统的对象集合,且包含基于所述系统的密钥的第一散列。所述第一散列对应于表示所述对象集合的清单的一或多个片段的相应内容对象散列。所述系统还基于来自远程节点的数据兴趣中的名称确定对于所述内容对象的请求。



CN 104980489 B

1.一种存储指令的非暂时性计算机可读存储媒体,所述指令在由计算机执行时致使所述计算机执行方法,所述方法包括:

产生包括本地节点的内容对象的名称的播发兴趣,其中所述名称表示所述本地节点处的对象集合,其中所述名称包含基于所述本地节点的密钥的第一散列;

其中所述第一散列对应于表示所述对象集合的清单的一或多个片段的相应内容对象散列;以及

基于来自远程节点的数据兴趣中的名称确定对于所述内容对象的请求。

2.根据权利要求1所述的非暂时性计算机可读存储媒体,其中所述内容对象为所述清单的第一片段;且

其中所述内容对象包括所述清单的第二片段的第二散列。

3.根据权利要求1所述的非暂时性计算机可读存储媒体,其中所述方法进一步包括从具有相同清单散列的多个清单中选举所述本地节点处的用于所述播发兴趣的所述清单,其中所述多个清单分布在多个节点之间。

4.根据权利要求1所述的非暂时性计算机可读存储媒体,其中所述内容对象为所述本地节点处的安全目录,其中所述安全目录包括所述清单的所述片段的所述相应内容对象散列,且其中所述第一散列为所述安全目录的散列。

5.根据权利要求4所述的非暂时性计算机可读存储媒体,其中所述方法进一步包括使用所述本地节点的所述密钥为所述安全目录签名。

6.根据权利要求4所述的非暂时性计算机可读存储媒体,其中所述方法进一步包括从具有相同内容对象散列的多个安全目录中选举所述本地节点处的用于所述播发兴趣的所述安全目录,其中所述多个安全目录分布在多个节点之间。

7.根据权利要求4所述的非暂时性计算机可读存储媒体,其中所述安全目录分布于多个片段当中;且

其中所述安全目录的第一片段的内容对象包含所述安全目录的第二片段的内容对象的散列。

8.根据权利要求1所述的非暂时性计算机可读存储媒体,其中所述方法进一步包括响应于来自远程节点的对于所述片段的数据兴趣而产生包括所述清单的片段的消息,其中所述数据兴趣包含安全目录中的所述内容对象散列中的一者。

9.根据权利要求1所述的非暂时性计算机可读存储媒体,其中所述本地节点的所述密钥将所述本地节点识别为受信任发布者。

10.一种存储指令的非暂时性计算机可读存储媒体,所述指令在由计算机执行时致使所述计算机执行方法,所述方法包括:

从播发兴趣获得远程节点的内容对象的名称,其中所述名称表示所述远程节点处的对象集合,其中所述名称包含基于所述远程节点的密钥的第一散列;

其中所述第一散列对应于表示所述对象集合的清单的一或多个片段的相应内容对象散列;以及

基于所述名称针对所述远程节点产生包括对于所述内容对象的请求的数据兴趣。

使用匹配的网络名称的安全集合同步

技术领域

[0001] 本发明大体上涉及数据安全。更具体来说，本发明涉及使用确切匹配名称使网络中的集合安全地同步。

背景技术

[0002] 在许多计算应用中，网络上的对等机使其相应数据集合同步常常是重要的。数字内容的激增产生了大量需要调和的集合。内容中心网络(CCN)架构已经设计以促进存取及处理此类数字内容。CCN包含实体或节点，例如网络客户端、转发器(例如，路由器)及内容产生器，其通过发送对于各种内容项目的“兴趣”包及接收返回的“内容对象”包而彼此通信。基于唯一名称识别CCN兴趣及内容对象，所述唯一名称通常为阶层结构可变长度识别符(HSVLI)，且包括从最一般层级到最特定层级排序的连续名称组成部分。

[0003] 在许多计算应用中，网络中的装置表达对于其相应数据集合的兴趣常常是重要的。数字内容的激增产生了大量需要调和的集合。CCN架构已经设计以促进存取此类数字内容。这些网络包含实体或节点，例如网络客户端、转发器(例如，路由器及交换器)及内容产生器，其通过发送对于各种内容项目的“兴趣”包及接收包括返回的内容对象的“响应”包而彼此通信。不同于传统因特网协议(IP)网络(其中对象绑定到其位置及其IP地址)，基于独立于位置且通常为HSVLI的特定名称识别CCN中的内容对象。

[0004] 举例来说，连接到计算机网络的多个区域的边界路由器可订用那些区域(例如，“区域1”及“区域2”)。不为边界路由器的其它路由器可仅订用单个区域。以次方式，订用名称空间“区域1”的路由器仅获得用于区域1的网络配置项目，且订用名称空间“区域2”的路由器仅获得用于区域2的网络配置项目。订用两个名称空间的边界路由器可获得用于区域1及区域2的网络配置项目。

[0005] 因为网络配置项目的结构化名称为唯一且持久性的，因此CCN中的节点可基于结构化名称产生每一网络配置项目的散列值，而不必处理每一内容项目的数据。节点还可基于用于路由数据集合的个别网络配置项目的散列产生用于每一路由数据集合的累加散列，以使得所述累加散列表示路由数据集合的内容。举例来说，节点可通过使用加法操作(或某一其它数学函数)来处理用于路由数据集合的个别网络配置项目的散列而产生累加散列。

[0006] 一个典型CCN同步协议使用最长前缀匹配方法，其中对“/parc/events/”的兴趣匹配“/parc/events/calendar.txt”及“/parc/events/conference.txt”两者。随着CCN架构演进，同步协议还演进到允许使用确切名称匹配，而非当前最长前缀匹配。在同步期间，代管集合的节点使用其名称播发所述集合。需要使集合同步的任何其它节点以确切名称发送请求且接收包括所述集合的响应。然而，不良节点可发送恶意播发。结果，接收播发的节点需要确保播发为有效播发。尽管CCN将许多合乎需要的特征引入到网络中，但一些问题对于集合的安全同步仍悬而未决。

发明内容

[0007] 一个实施例提供一种促进使用确切网络名称的清单安全同步的系统。在操作期间，所述系统产生包括所述系统的内容对象的名称的播发兴趣。此名称表示所述系统的对象集合，且包含基于所述系统的密钥的第一散列。所述第一散列对应于表示所述对象集合的清单的一或多个片段的相应内容对象散列。所述系统还基于来自远程节点的数据兴趣中的名称确定对于所述内容对象的请求。

[0008] 在此实施例的变型中，内容对象为清单的第一片段，且包括清单的第二片段的第二散列。

[0009] 在另一变型中，系统从具有相同清单散列的多个清单中选举系统中用于播发兴趣的清单。所述多个清单分布在多个节点之间。

[0010] 在此实施例的变型中，内容对象为系统中的安全目录。此安全目录包括清单的片段的相应内容对象散列；且第一散列为安全目录的散列。

[0011] 在另一变型中，系统使用系统的密钥为安全目录签名。

[0012] 在另一变型中，系统从具有相同内容对象散列的多个安全目录中选举系统处用于播发兴趣的安全目录。所述多个安全目录分布在多个节点之间。

[0013] 在另一变型中，安全目录分布在多个片段之间。所述安全目录的第一片段的内容对象包含所述安全目录的第二片段的内容对象的散列。

[0014] 在此实施例的变型中，，所述系统响应于来自远程节点的对片段的数据兴趣而产生包括清单的片段的消息。所述数据兴趣包含安全目录中的内容对象散列中的一者。

[0015] 在此实施例的变型中，计算装置的密钥将计算装置识别为受信任发布者。

[0016] 一个实施例提供一种促进使用网络名称的多对象兴趣的系统。在操作期间，所述系统从播发兴趣获得远程节点的内容对象的名称。所述名称表示远程节点处的对象集合，且包含基于远程节点的密钥的第一散列。所述第一散列对应于表示所述对象集合的清单的一或多个片段的相应内容对象散列。所述系统进一步针对远程节点基于名称产生包括对于内容对象的请求的数据兴趣。

附图说明

[0017] 图1说明根据本发明的实施例的促进使清单在内容中心网络(CCN)中的节点之间同步的示范性计算机系统。

[0018] 图2说明根据本发明的实施例的在本地节点与远程节点之间的示范性通信。

[0019] 图3呈现根据本发明的实施例的说明用于使与远程清单及本地清单相关联的内容同步的过程的流程图。

[0020] 图4呈现根据本发明的实施例的说明用于基于修改时间使与远程清单及本地清单相关联的内容同步的过程的流程图。

[0021] 图5呈现根据本发明的实施例的说明用于发射对应于清单的播发的过程的流程图。

[0022] 图6A呈现根据本发明的实施例的描绘集合中所表示的清单及内容对象的格式的表。

[0023] 图6B呈现根据本发明的实施例的描绘在同步期间的两个清单的格式的表，其中本

地清单缺少来自远程清单的内容对象。

[0024] 图6C呈现根据本发明的实施例的描绘在同步期间的两个清单的格式的表，其中本地清单中的相同名称的内容对象的摘要不同于远程清单中的摘要，且其中远程节点播发其清单。

[0025] 图6D呈现根据本发明的实施例的描绘在同步期间的两个清单的格式的表，其中本地清单中的相同名称的内容对象的摘要不同于远程清单中的摘要，且其中本地节点播发其清单。

[0026] 图6E呈现根据本发明的实施例的描绘在同步期间的两个清单的格式的表，此时本地清单中的相同名称的内容对象的摘要及修改时间不同于远程清单中的摘要。

[0027] 图7A说明根据本发明的实施例的清单的示范性安全同步。

[0028] 图7B说明根据本发明的实施例的用于清单的安全同步的示范性散列链。

[0029] 图8A呈现根据本发明的实施例的说明节点使用散列链安全地使本地清单同步的过程的流程图。

[0030] 图8B呈现根据本发明的实施例的说明节点使用散列链起始远程清单的安全同步的过程的流程图。

[0031] 图8C呈现根据本发明的实施例的说明节点使用散列链安全地使远程清单同步的过程的流程图。

[0032] 图9A说明根据本发明的实施例的用于清单的安全同步的示范性安全目录。

[0033] 图9B说明根据本发明的实施例的使用安全目录的清单的示范性安全同步。

[0034] 图10A呈现根据本发明的实施例的说明节点安全地使用安全目录使本地清单同步的过程的流程图。

[0035] 图10B呈现根据本发明的实施例的说明节点使用安全目录安全地使远程清单同步的过程的流程图。

[0036] 图11说明根据本发明的实施例的促进CCN中的清单的安全同步的示范性计算机及通信系统。

[0037] 在诸图式中，相同参考数字指代相同图式元件。

具体实施方式

[0038] 呈现以下描述以使所属领域的技术人员能够制备且使用实施例，且在特定应用以及其要求的背景下提供以下描述。所属领域的技术人员将易于了解对所揭示的实施例的各种修改，且在不脱离本发明的精神和范围的情况下，本文中所定义的一般原理可应用于其它实施例以及应用。因此，本发明不限于所示出的实施例，而是应被赋予与本文所揭示的原理以及特征一致的最宽范围。

[0039] 在本发明的实施例中，通过将加密散列与对于对象集合的兴趣并入到内容中心网络(CCN)名称空间内来解决使用确切匹配名称使对象集合安全地同步的问题。在本发明中，术语“内容对象”与“对象”可互换地使用。对于现有技术，在CCN中，主机节点可通过广播包括对象的持久性名称的兴趣包而在任何时间通知内容对象(即，新内容项目)或对象。此兴趣包可称为兴趣。兴趣的分发允许其它节点了解所述对象。响应于接收到播发兴趣，感兴趣的节点发送数据兴趣以获得所需对象。作为响应，主机节点可发送包括所述对象的响应包。

此响应包可称为响应。在本发明中，术语“兴趣包”与“兴趣”可互换地使用。术语“响应包”与“响应”也可互换地使用。

[0040] 播发兴趣为用于在CCN中播发内容对象的兴趣。节点可在获得或更新内容对象之后即刻发送播发兴趣。另一方面，数据兴趣为用于请求CCN中的内容对象(即，数据)的兴趣。节点可发送数据兴趣以表达对于任何内容对象的兴趣(或请求)。在任一兴趣中，CCN名称空间中的名称(例如，阶层结构可变长度识别符(HSVLI))用以识别内容对象。在一些实施例中，名称包含相关名称空间的识别(或名称空间识别)。此名称空间识别为区分兴趣的CCN名称的部分。举例来说，名称可包含用于播发的“/adv”及用于数据的“/data”。

[0041] 对于大对象集合，发送对于相应对象的相应兴趣导致兴趣的低效、带宽密集且反复的分发。可扩展CCN以并入基于清单的内容联网(MBCN)。CCN中的内容消费者节点可使用表示集合的清单名称来表达对于对象集合的兴趣。在一些实施例中，清单为集合中的对象的有序列表。清单可包含对象的相应名称及其对应散列。通过发送对于清单的播发兴趣(其还可被称作播发)，主机节点可使远程节点了解所述集合。然而，主机节点可能是恶意的，且发送不良播发兴趣。

[0042] 为解决此问题，本发明的实施例随此类播发兴趣并入加密散列。举例来说，此散列可为兴趣中的清单的名称的部分。在一些实施例中，可使用散列链获得利用确切匹配名称的此安全同步。如果清单大且需要分段进行分发，则播发兴趣可包含清单的第一片段的散列。除最后一个片段外的相应片段可在指定字段中含有一或多个后续片段的散列，由此形成散列链。结果，在获得每一片段之后，节点即刻了解下一片段的散列。在一些实施例中，可使用安全目录获得利用确切匹配名称的此安全同步。播发兴趣可含有安全目录的散列(或安全目录的第一片段)。安全目录含有清单的相应片段的散列。通过接收目录，节点可获得相应清单片段的相应散列，且使用对应散列发送对于那一片段的兴趣。

[0043] 本发明的实施例提供一种通过使用确切匹配名称促进清单在网络上的节点之间的同步的系统。在本发明的实施例的以下描述中，相关CCN实体为本地节点及远程节点，但角色可反转。本地及远程节点中的每一者与清单相关联，所述清单表示节点处的内容对象的集合。清单通过特定前缀识别，使得具有相同前缀的两个清单对应于相同内容对象集合。

[0044] 在一些实施例中，清单为识别内容对象集合的有序列表。集合中的每一内容对象通过其名称及对应摘要识别，其中摘要为内容对象的散列值。在一些实施例中，每一内容对象还通过修改时间识别，所述修改时间指示修改内容的时间。出于此描述的目的，将清单描述为有序列表，但其它实施例包含结构化为同步树的清单，其含有内容对象以及嵌套的内容对象集合。系统产生用于清单的根散列值。根散列值为基于集合的个别内容对象的散列值的累加散列值。清单的根散列值为用于清单的唯一识别符。

[0045] 系统可使用确切匹配名称使本地清单中的集合与本地清单中的内容同步。远程节点播发其清单的散列。本地节点接收所述播发且确定所播发的远程清单对应于本地清单，其中远程清单及本地清单对应于相同内容对象集合。本地节点通过比较本地清单的根散列值与远程清单的根散列值而确定本地清单的内容是否与远程清单的内容同步。如果其并不匹配，则本地节点通过将对于远程清单的请求发送到远程节点来检索远程清单。

[0046] 在一些实施例中，本地节点基于分段协议发送一组兴趣，且每一兴趣对应于清单的经编号片段。在一些实施例中，所述远程节点可播发对应于其清单的片段的编号。拥有远

程清单的本地节点确定远程清单中指示的哪些内容对象不同于本地清单中指示的内容对象。随后，本地节点发射对于不同的内容对象的一组兴趣，其中所述兴趣包含所请求内容对象的名称。在一些实施例中，所述兴趣还包含所请求内容对象的对应散列值。以此方式，所述系统使用确切名称匹配来请求及接收不同内容对象集合。

[0047] 在一些实施例中，使用结构化技术发射所述清单，例如按rsync协议的滚动散列技术，而非发送完整清单。rsync协议允许在两个节点之间有效地发射清单，因为所述节点已经具有相同清单的类似但不相同的版本。

[0048] 在一些实施例中，进一步通过对应修改时间识别集合中的内容对象，修改时间指示修改内容对象的时间。用于确定为不同的每一内容对象，本地节点确定远程清单中的内容对象的修改时间比本地清单中的对应内容对象更为新近还是较不新近。如果远程内容对象对应于更为新近的修改时间，则本地节点用来自远程清单的内容对象的值更新本地清单中的内容对象的值。第13/681,306号美国专利申请案(标题为“根据按名称的内容同步的数据输送(Data Transport by Named Content Synchronization)”发明人Van L. Jacobson及Marc E.Mosko，2012年12月19日申请)中含有如何从数据集合移除或“空出(white-out)”内容项目的描述。

[0049] 在一些实施例中，如果远程内容对象对应于较不新近的修改时间，则系统可通过将来自远程清单的内容对象的值插入到本地清单中的对应内容对象的历史字段中来确定是否保留历史。系统相应地对于确定为不同的每一内容对象更新所述值。以此方式，系统使本地节点处的清单与远程节点处的清单同步。

[0050] 在一些实施例中，网络客户端、网络节点(例如，例如路由器等转发器)与发布者经由信息中心网络(ICN)进行通信。在ICN中，每一内容段个别地进行命名，且每一数据段绑定到唯一名称，所述唯一名称区别所述数据与任何其它数据段，例如相同数据或来自其它来源的数据的其它版本。此唯一名称允许网络装置通过散布指示所述唯一名称的请求或兴趣来请求数据，且可独立于数据的存储位置、网络位置、应用程序及运送手段而获得数据。命名数据网络(NDN)或内容中心网络(CCN)为ICN架构的实例；以下术语描述NDN或CCN架构的元件：

[0051] 内容对象：单个命名数据段，其绑定到唯一名称。内容对象为“持久性的”，这意味着内容对象可在计算装置内或跨越不同计算装置移动，但不改变。如果内容对象的任何组成部分改变，则造成所述改变的实体创建包含经更新内容的新内容对象，且将所述新内容对象绑定到新的唯一名称。

[0052] 唯一名称：ICN中的名称通常独立于位置且唯一地识别内容对象。数据转发装置可使用名称或名称前缀朝向产生或存储内容对象的网络节点转发数据包，而不顾及所述内容对象的网络地址或物理位置。在一些实施例中，名称可为阶层结构可变长度识别符(HSVLI)。HSVLI可划分成若干阶层组成部分，其可以各种方式结构化。举例来说，个别名称组成部分parc、home、ndn及test.txt可以左向前缀为主方式(left-oriented prefix-major fashion)结构化以形成名称“/parc/home/ndn/test.txt”。因此，名称“/parc/home/ndn”可为“/parc/home/ndn/test.txt”的“母体(parent)”或“前缀”。额外组成部分可用以区分内容项目的不同版本，例如协作文档。

[0053] 在一些实施例中，名称可包含非阶层式识别符，例如从内容对象的数据(例如，检

查和值)及/或从内容对象的名称的元素导出的散列值。基于散列的名称的描述描述于第13/847,814号美国专利申请案(标题为“用于基于名称的数据包转发的有序元素命名(ORDERED-ELEMENT NAMING FOR NAME-BASED PACKET FORWARDING)”,发明人为Ignacio Solis,2013年3月20日申请)中。名称还可为平面标记(flat label)。下文中,“名称”用于指名称数据网络中的数据段的任何名称,例如阶层名称或名称前缀、平面名称、固定长度名称、任意长度名称或标记(例如,多协议标记交换(MPLS)标记)。

[0054] 兴趣:数据包,其指示对于数据段的请求,且包含所述数据段的名称(或名称前缀)。数据消费者可跨越信息中心网络散布请求或兴趣,CCN/NDN路由器可朝向可提供所请求数据以满足所述请求或兴趣的存储装置(例如,缓存服务器)或数据产生器传播所述请求或兴趣。

[0055] 在一些实施例中,ICN系统可包含CCN架构。然而,本文所揭示的方法也同样适用于其它ICN架构。CCN架构的描述描述于第12/338,175号美国专利申请案(标题为“控制内容中心网络中的兴趣及内容的扩散(CONTROLLING THE SPREAD OF INTERESTS AND CONTENT IN A CONTENT CENTRIC NETWORK)”,发明人为Van L. Jacobson和Diana K.Smetters,于2008年12月18日申请)中。

[0056] 在本发明中,结合图1到6的描述与使用清单的对象集合同步的一般架构相关联;且结合图7及后续图的描述提供关于用于促进集合对象的安全同步的机制的较多细节。

[0057] 图1说明根据本发明的实施例的促进使清单在CCN中的节点之间同步的示范性计算机系统。在图1中,网络100促进清单在CCN中的节点之间的同步。网络100可包含客户端装置116(或消费者)、内容产生装置118(或产生器)及在节点102、104、106、108、110、112及114处的路由器或其它转发器。节点102到114可各自含有一或多个清单。举例来说,节点112含有清单120。清单120包括集合名称122及由以下各者中的一或多者识别的内容对象的有序列表:内容对象名称130.1到130.n;摘要132.1到132.n,及修改时间134.1到134.n。摘要132.1到132.n包括分别由名称130.1到130.n识别的内容对象的散列值。在一些实施例中,摘要可为内容对象的SHA-256散列,其中散列冲突(其中两个不同内容对象的单向散列导致相同值)的可能性足够低,使得摘要为用于内容对象的唯一识别符。清单120还包含根散列124,其为基于集合的个别内容对象的摘要(即,散列值)132.1到132.n的累加散列值。根散列124为用于清单120的唯一识别符,且表示集合中的内容对象。

[0058] 在一些实施例中,清单指示名称及对应摘要,但不指示修改时间。此类系统可包含例如文件服务器,其中文本文件的先前版本为重要的且因此由系统保留。在其它实施例中,清单指示名称、对应摘要及修改时间。系统可使用修改时间来确定应保留内容项目的哪些版本。举例来说,如果内容项目指示链接状态,则系统不需要与先前版本有关的信息。在此情况下,仅保留具有最近修改时间的内容对象。

[0059] 网络中的任何两个节点可含有表示相同数据集合的清单,其中可使用本文中所描述的方法使所述清单同步。术语“本地节点”及“远程节点”可应用于内容中心网络(CCN)中的任何节点,且用于本发明中以区分CCN中的两个节点。

[0060] 表示相同数据集合的清单在两个节点之间的同步是基于三部分名称。第一部分为识别所述集合的可路由前缀,例如“/a/b”。第二部分含有相关名称空间的识别(或名称空间识别),且可为用于播发的“/adv”或用于数据传送的“/data”。第三部分为散列值或所播发

或传送的内容。因此,CCN名称具有以下形式:

[0061] /collection_prefix/adv_or_data/protocol_data

[0062] 发送散列播发的兴趣的实例为:

[0063] /a/b/adv/＜roothash＞

[0064] 接收到此播发且含有具有相同可路由前缀“/a/b”的本地清单的本地节点基于分段协议在片段0、1...直到结束片段m中检索所播发的清单。此类兴趣看起来像:

[0065] /a/b/data/＜roothash＞/＜segment number＞

[0066] 基于所检索清单中的条目,系统确定所检索清单中识别的哪些内容对象不同于本地清单中识别的内容对象。系统基于不同内容对象的名称检索所述内容对象:

[0067] /a/b/data/＜name of content object＞

[0068] 在一些实施例中,系统基于所请求内容对象的散列值检索不同内容对象:

[0069] /a/b/data/＜hash(content object)＞

[0070] 在一些实施例中,系统基于清单中的名称检索不同内容对象。此技术允许系统检索对象的任何高速缓存的副本,而非使用在集合的名称空间下的内容的名称。举例来说,为从图6B中的清单140检索第一项目,系统发送对于名称及摘要的兴趣:

[0071] /chef/events/calendar.txt,摘要＝{1}

[0072] 图2说明根据本发明的实施例的在本地节点与远程节点之间的示范性通信。节点102(远程节点)与节点106(本地节点)之间的通信200促进基于清单促进对象集合的同步。节点102及节点106各自含有具有相同路由前缀或集合名称“/a/b”的清单。远程节点102发射send_advertisement兴趣220(即,播发兴趣),其为含有由集合名称“/a/b”识别的其清单的根散列值的散列播发。兴趣采用以下形式:“/a/b/adv/＜roothash＞”。本地节点106接收所播发的兴趣,且执行check_advertised_collection程序222以基于相同集合前缀202(“/a/b”)确定节点106是否含有与所播发清单指示相同集合的清单。接着,本地节点106确定其本地清单的根散列是否不同于远程清单的根散列。不同散列值指示集合需要与彼此同步。本地节点106接着通过发送对于清单的一组兴趣来执行retrieve_manifest程序224。所述组兴趣基于分段协议而分段。所述兴趣在request_remote_manifest_in_segments兴趣226(即,数据兴趣)中发送且具有以下形式:“/a/b/data/＜roothash＞/S0”、“/a/b/data/＜roothash＞/S1”、“/a/b/data/＜roothash＞/S2”等。在一些实施例中,播发节点可包含需要传送其清单的片段的编号。在send_remote_manifest_in_segments消息228中,远程节点102响应于所述组兴趣而发回所请求的清单。所请求的内容对象采用以下形式:“/a/b/data/＜roothash＞/S0+有效负载”,其中有效负载含有清单的所请求片段。

[0073] 拥有远程清单的本地节点106执行determine_set_difference程序230。在一些实施例中,此程序的结果为通过名称识别的内容对象的列表。在其它实施例中,结果为通过其对应摘要识别的内容对象的列表。本地节点106接着对于确定为不同的每一内容对象发射request_set_difference兴趣234。所述兴趣采用以下形式:“/a/b/data/name 130.3”。本地节点106在远程节点102发射send_set_difference内容对象236时接收所请求的内容对象,其中所请求的内容对象采用以下形式:“/a/b/data/name 130.3+有效负载”。因此,本地节点106通过请求并接收确定为不同的所有内容对象使得本地清单的内容与远程清单的内容同步而执行resolve_set_difference程序232。在一些实施例中,本地节点106执行下文

相对于图4描述的sync_based_on_mod_time程序240。

[0074] 图3呈现根据本发明的实施例的说明用于使与远程清单及本地清单相关联的内容同步的过程的流程图。在图2的实例中，节点106可为本地节点，且节点102可为远程节点。在操作期间，本地节点接收对应于远程节点处的远程清单的播发兴趣(操作302)。清单表示节点处的内容对象的集合。本地节点确定远程清单与本地清单指示相同内容对象集合(操作304，对应于图2中的check_advertised_collection程序222)。

[0075] 在一些实施例中，本地节点通过比较清单的集合名称或来确定清单是否指示相同集合。本地节点接着确定其本地清单的根散列值是否不同于远程清单的根散列值(操作306)。清单的根散列值为用于所述清单的唯一识别符，且包括所述清单中表示的内容对象的摘要的累加散列值。如果本地清单的根散列值与远程清单的根散列值不相同(操作308)，则表示相同集合的本地清单与远程清单不同步且需要调和。本地节点通过发送对于远程清单的请求及响应于所述请求接收远程清单(操作310，对应于图2中的retrieve_manifest程序224)来下载或传送远程清单。

[0076] 本地节点确定远程清单中识别的哪些内容对象不同于本地清单中识别的内容对象(操作312，对应于图2中的determine_set_difference程序230)。在一些实施例中，本地节点通过比较本地清单中识别的内容对象的摘要与远程清单中识别的相同名称的内容对象的摘要来确定集合差异。如果本地节点确定了差异，则本地节点发射对应于所确定的不同内容对象集合的一组数据兴趣(操作314)，且接收返回的所请求内容对象(操作316)。这对应于图2中所示的resolve_set_difference程序232。因此，本地清单的内容与远程清单的内容得以同步。

[0077] 如果本地节点已改变，则本地节点播发新根散列值。其可紧接着进行此操作，或基于网络或其它时点考虑调度下一播发。举例来说，本地节点可至少每秒播发其根散列一次，但不大于每秒四次。因此，在调和期间，由于根散列归因于更新而改变，节点可播发每秒至多四个改变。否则，节点可以稳定状态每秒播发一次。

[0078] 图4呈现根据本发明的实施例的说明用于基于修改时间使与远程清单及本地清单相关联的内容同步的过程的流程图。注意，内容的同步还可基于与内容对象相关联的序号，其中较大序号指示内容对象的较为新近版本。内容的同步还可基于内容对象的名称的排序，其中隐式排序次序指示内容对象的较为新近版本。此过程表示为图2中的sync_based_on_mod_time程序240。基于先前确定的集合差异，本地节点接收包含修改时间的所请求内容对象集合，所述修改时间指示修改对应内容对象的时间(操作402)。对于每一内容对象，本地节点确定远程清单中的内容对象的修改时间比本地清单中的对应内容对象更为新近还是较不新近(操作404)。如果来自远程清单的内容对象的修改时间更为新近(操作406)，则系统用来自远程清单的内容对象的值更新本地清单中的内容对象的值(操作408)。在一些实施例中，本地节点可通过在更新本地清单中的内容对象的值之前将(较不新近)内容对象的对应值及修改时间插入到本地清单中的历史字段中来确定是否保持本地清单中的其(较不新近)内容对象的值。如果在集合中还存在需要检索的内容对象(操作410)，则系统返回到操作404。如果不存在，则系统已完成检索必要的内容对象。

[0079] 如果来自远程清单的内容对象的修改时间不如本地清单中的对应内容对象新近(操作406)，则系统通过将(较不新近)内容对象的对应值及修改时间插入到本地清单中的

历史字段中(操作414)来确定是否保存来自远程清单的(较不新近)内容对象的值(操作412)。如果在需要检索的集合中还存在内容对象(操作410),则系统返回到操作404。如果没有,则系统已完成检索必要内容对象。因此,确定为不同的所有内容对象已经更新,且可能保留或保存在本地清单的历史字段中,使得本地清单的内容与远程清单的内容同步。

[0080] 图5呈现根据本发明的实施例的说明用于发射对应于清单的播发的过程的流程图。图5中的节点描述为本地节点,因为其将数据包发射到远程节点。注意,图5中的本地节点对应于图2中的节点102,其在先前已称为远程节点102。应注意,CCN中的任何节点可称为远程节点或本地节点。

[0081] 本地节点发射对应于清单的播发兴趣,其中清单表示节点处的内容对象的集合(操作502,对应于图2中的send_advertisement消息220)。此播发为类似于信标的兴趣,且基于所使用的“/adv”名称空间识别,不请求返回任何内容。在从请求清单的远程节点接收到数据兴趣之后,本地节点即刻将所述清单发射到远程节点(操作504,对应于接收图2中的request_remote_manifest_in_segments兴趣226及send_remote_manifest_in_segments消息228)。在从远程节点接收到对于本地清单中识别的内容对象的请求之后,本地节点即刻将所请求的内容对象发射到请求远程节点(操作506,对应于接收图2中的兴趣234及send_set_difference消息236)。

[0082] 图6A呈现根据本发明的实施例的描绘集合中所表示的清单及内容对象的格式的表。清单120包括通过集合名称122及以下各者中的一或多者识别的内容对象的有序列表:内容对象名称130.1到130.n;摘要132.1到132.n;以及一修改时间134.1到134.n。摘要132.1到132.n包括分别由名称130.1到130.n识别的内容对象的散列值。清单120还包含根散列124,其为基于集合的个别内容对象的散列值132.1到132.n的累加散列值。清单120的根散列124为用于清单120的唯一识别符。

[0083] 如关于图1所描述,清单120可指示用于集合中表示的每一内容对象的名称及对应摘要。在一些实施例中,清单120还可包含用于集合中表示的每一内容对象的修改时间。修改时间字段的使用取决于基础应用程序或所执行的服务。注意,清单120指示集合名称122。图6B到6E中所描绘的清单还包含集合名称,但因为示范性清单包括相同数据集合,因此集合名称未包含在图6B到6E中。

[0084] 图6B到6E描绘两个节点,节点102及节点106,其中的每一者含有清单。在此实例中,节点102为远程节点,且节点106为本地节点。本地节点106含有清单160,且远程节点102含有清单140。清单140与160含有相同名称集合或路由前缀,且因此表示相同内容对象或数据的集合。时间由标记T1、T2等指示,且相对于这些时间标记描绘清单140及160的内容。

[0085] 须强调,清单由在图6A中说明为根散列124的根散列值进一步识别,其为基于集合的个别内容对象的摘要的累加散列值。在以下实例中,根散列值及摘要指示为括号中的数目,例如“{999}”,但数目可远大于此。此外,仅将随时间推移而改变的内容对象的摘要以及清单140和160的范例根散列值描绘为表示累加散列值的样本。

[0086] 图6B呈现根据本发明的实施例的描绘在同步期间的两个清单的格式的表,其中本地清单缺少来自远程清单的内容对象。在时间T1,本地节点106从远程节点102接收具有根散列{999}的清单140的散列播发。本地节点106确定其清单160与远程清单140表示相同数据集合,且检索清单140。本地节点106确定具有根散列{60}的本地清单160与具有根散列

{999}的远程清单140不同步。本地节点106接着确定其本地清单160与远程清单140之间的集合差异。在此实例中，清单160缺少由名称“/fruit/lychee/peel”识别的内容对象，因此本地节点106通过那一名称将对于内容对象的兴趣发送到远程节点102。远程节点102返回所请求的内容对象。在时间T2，本地节点106用缺少的内容对象更新其清单160。基于时间T2处的清单160的内容，系统产生用于清单160的新根散列，其现在等于远程清单的根散列。此由时间T2处的清单160的根散列值{60}→{999}描绘。因此，本地清单与远程清单已使其集合同步，且两者含有相同根散列值{999}。

[0087] 图6C呈现根据本发明的实施例的描绘在同步期间的两个清单的格式，其中本地清单中的相同名称内容对象的摘要不同于远程清单中的摘要，且其中远程节点播发其清单。在时间T3，本地节点106从远程节点102接收具有根散列{999}的清单140的散列播发。本地节点106确定其清单160与远程清单140表示相同数据集合，且检索清单140。本地节点106确定具有根散列{53}的本地清单160与具有根散列{999}的远程清单140不同步。本地节点106接着确定其本地清单160与远程清单140之间的集合差异。在此实例中，清单160缺少由具有摘要{279}的名称“/fruit/lychee/peel”识别的内容对象，因此本地节点106基于那一名称及摘要将对于内容对象的兴趣发送到远程节点102。远程节点102返回所请求的内容对象。在时间T4.a，本地节点106用缺少的内容对象更新其清单160。基于时间T4.a处的清单160的内容，系统产生用于清单160的新根散列。此由时间T4.a处的清单160的根散列值{53}→{772}描绘。然而，具有其初始根散列{999}的清单140现在与具有新根散列{772}的清单160不同步。

[0088] 随后，远程节点102从本地节点106接收具有新根散列{772}的清单160的散列播发。远程节点102确定其清单140与清单160表示相同数据集合，且检索清单160。远程节点102确定具有根散列{999}的那一清单140与具有根散列{772}的清单160不同步。远程节点102接着确定其清单140与清单160之间的集合差异。在此实例中，清单140缺少由具有摘要{41}的名称“fruit/lychee/peel”识别的内容对象，因此，远程节点102基于那一名称及摘要将对于内容对象的兴趣发送到本地节点106。本地节点106返回所请求的内容对象。在时间T5.a，远程节点102用缺少的内容对象更新其清单140。基于时间T5.a处的清单140的内容，系统产生用于清单140的新根散列。此由时间T5.a处的清单140的根散列值{999}→{772}描绘。因此，在时间T5.a，节点102处的清单140与节点106处的清单160同步。节点102及106已使其集合同步，且两者含有相同根散列值{772}。

[0089] 图6D呈现根据本发明的实施例的描绘在同步期间的两个清单的格式，其中本地清单中的相同名称内容对象的摘要不同于远程清单中的摘要，且其中本地节点播发其清单。在时间T3，远程节点102从本地节点106接收具有根散列{53}的清单160的散列播发。远程节点102确定其清单140与清单160表示相同数据集合，且检索清单160。远程节点102确定具有根散列{999}的其清单140与具有根散列{53}的清单160不同步。远程节点102接着确定其清单140与清单160之间的集合差异。在此实例中，清单140缺少由具有摘要{41}的名称“/fruit/lychee/peel”识别的内容对象，因此，远程节点102基于那一名称及摘要将对于内容对象的兴趣发送到本地节点106。本地节点106返回所请求的内容对象。在时间T4.b，远程节点102用缺少的内容对象更新其清单140。基于时间T4.b处的清单140的内容，系统产生用于清单140的新根散列。此由时间T4.b处的清单140的根散列值{999}→{772}描绘。然而，具有

其初始根散列{53}的清单160现在与具有新根散列{772}的清单140不同步。

[0090] 随后，本地节点106从远程节点102接收具有新根散列{772}的清单140的散列播发。本地节点106确定其清单160与清单140表示相同数据集合，且检索清单140。本地节点106确定具有根散列{53}的其清单160与具有根散列{772}的清单140不同步。本地节点106接着确定其本地清单160与远程清单140之间的集合差异。在此实例中，清单160缺少由具有摘要{41}的名称“/fruit/lychee/peel”识别的内容对象，因此，本地节点106基于那一名称及摘要将对于内容对象的兴趣发送到远程节点102。远程节点102返回所请求的内容对象。在时间T5.b，本地节点106用缺少的内容对象更新其清单160。基于时间T5.b处的清单160的内容，系统产生用于清单160的新根散列。此由时间T5.b处的清单160的根散列值{53}→{772}描绘。因此，在时间T5.b，节点102处的清单140与节点106处的清单160同步。节点102及106已使其集合同步，且两者含有相同根散列值{772}。

[0091] 图6C及6D说明任何节点可为远程或本地节点，且发送或接收与清单相关联的确定为不同的散列播发、清单及内容对象的次序可取决于给出时间的集合中的内容(例如，清单140及160在时间[T3，T4.a，T5.a]及时间[T3，15T4.b，T5.b]的内容)而不同。即，使用本发明中所描述的方法，任何节点可发送或接收散列播发、传送清单且使节点处的清单的内容同步，由此导致两个节点处的数据集合的同步。

[0092] 图6E呈现根据本发明的实施例的描绘在同步期间的两个清单的格式的表，此时本地清单中的相同名称的内容对象的摘要不同于远程清单中的摘要。在时间T6，本地节点106从远程节点102接收具有根散列{999}的清单140的散列播发。本地节点106确定其清单160与远程清单140表示相同数据集合，且检索清单140。本地节点106确定具有根散列{80}的本地清单160与具有根散列{999}的远程清单140不同步。本地节点106接着确定其本地清单160与远程清单140之间的集合差异。在此实例中，清单140及清单160两者都指示对应于其集合中表示的每一内容对象的修改时间134。系统确定清单140及清单160中具有相同名称的内容对象具有不同摘要及不同修改时间。

[0093] 应注意，修改时间可包含与修改对应内容对象的秒、分钟、小时、天、月及年有关的信息。为简单起见，图6E中的示范性清单仅含有天的时间。清单140含有由具有摘要{1}及修改时间8:05am的名称“/chef/events/calendar.txt”识别的内容对象。清单160含有由具有不同摘要{320}及不同修改时间7:30am的相同名称识别的内容对象。本地节点106接着基于不同内容对象的名称及摘要将对于内容对象的兴趣发送到远程节点102。远程节点102返回所请求的内容对象。

[0094] 本地节点106确定来自远程清单140的具有修改时间8:05am的内容对象比来自其本地清单160的具有修改时间7:30am的内容对象更为新近。因此，在时间T7，本地节点106用不同且较为新近的内容对象更新其清单160。基于时间T7的清单160的内容，系统产生用于清单160的新根散列。此由时间T7处的清单160的根散列值{80}→{999}描绘。因此，在时间T7，本地节点106处的清单160与远程节点102处的清单140同步。节点102及106已使其集合同步，且两者含有相同根散列值{999}。

[0095] 在一些实施例中，系统将已改变内容对象的先前版本(例如，由具有摘要{320}及修改时间7:30am的名称“/chef/events/calendar.txt”识别的内容对象)保留在清单160的历史字段中。在其它实施例中，当远程节点102从本地节点106接收到具有根散列{80}的清

单160的散列播发且下载本地清单160时，远程节点102确定由具有摘要{320}及修改时间7：30am的名称“/chef/events/calendar.txt”识别的所接收内容对象的版本不如其自身的清单中的版本新近。在此情况下，远程节点102处的清单140保持与本地节点106处的清单160不同步。清单将在稍后时间在本地节点106从远程节点102接收到含有最近经更新内容对象的清单140的散列播发时经历同步，如上文所描述。

[0096] 在本发明的实施例中，除包括可路由前缀、相关名称空间的识别及清单的根散列值的三部分名称之外，用于清单的播发兴趣还携载内容对象的散列。图7A说明根据本发明的实施例的清单的示范性安全同步。在操作期间，节点102发射send_advertisement兴趣712(即，播发兴趣)，其为含有通过集合名称“/a/b”识别的其清单的根散列值的散列播发。此外，兴趣712进一步包括第一内容散列(表示为contenthash_1)。第一内容散列为清单的第一片段(即，片段0)的加密散列，如结合图2所描述。加密散列为基于节点的加密识别码(例如，密钥)产生的散列。此允许网络100区别开清单的所有潜在片段0与内容对象散列给出的片段。

[0097] 如果另一节点104也包含清单，则节点104的第一内容散列(表示为contenthash_2)可不同于contenthash_1。节点104还发射send_advertisement兴趣714。在接收到兴趣712及714之后，节点106可即刻确定应从哪一节点获得清单。在一些实施例中，节点102及104使用分布式选举来选取一个散列链用于节点102及104两者使用。此导致大大减小用以描述一个清单的散列量。在一些实施例中，选举具有最大散列值的散列链。假定contenthash_1具有的值比contenthash_2高。结果，节点104通过响应于兴趣712而发送数据兴趣来从节点102检索清单的第一片段，且获得对应散列链的第一内容散列。

[0098] 如果节点102为有效发布者(即，有效发布者节点)，则节点104获得节点102的整个散列链且开始播发节点102的散列值。然而，具有较大内容散列值的节点可能不是受信任发布者。举例来说，不良节点702也可能发射具有最大散列值的恶意send_advertisement兴趣716(以点线表示)。如果节点702的密钥不受信任，则节点104可舍弃此类播发兴趣，且继续播发节点104的散列。看到对于清单的多个兴趣(例如，兴趣712、714及716)的节点106可首先选择节点702的最大内容对象散列。然而，因为对应散列链并不是来自受信任发布者，因此节点106基于选择策略尝试另一播发兴趣。选择策略的实例包含但不限于内容散列值的次序及随机次序以避免前置攻击(front-loading attack)。假定contenthash_1具有最高散列值。节点106接着发送包括contenthash_1的request_remote_manifest兴趣722。

[0099] 如果不良节点702伪造根散列(表示为roothash_1)，则节点702可能用一或多个所伪造的内容对象散列(例如，contenthash_3)使网络溢流。节点106检索所伪造播发的第一片段以查看密钥识别符并确定节点702是否为受信任参与者。因为节点702的密钥识别符是伪造的，因此节点106不信任播发716的兴趣。另一方面，如果不良节点702使用真正根散列但伪造内容对象散列，则节点106检索对应于相应播发兴趣的第一片段(例如，兴趣712、714及716)以查看对应密钥识别符并确定节点是否为可接受参与者。节点106可在第一可接受播发之后停止此迭代并遵循其散列链。因为节点必须遵循散列链，因此使下载管线化受到散列链的扇出的限制。

[0100] 图7B说明根据本发明的实施例的用于清单的安全同步的示范性散列链。假定清单700分段成n个片段736.1到736.n(即，清单片段0到(n-1))。相应清单片段呈分别由名称

732.1到732.n表示的相应内容对象730.1到730.n形式。名称包含前缀、相关名称空间的识别、清单700的根散列，及内容对象散列(即，对应内容对象的散列)。举例来说，名称732.1包含清单700的根散列及内容对象730.1的散列。此允许网络区别开清单700的所有潜在片段0与内容对象散列给出的片段。清单700的每一内容对象内部为下一清单片段的散列。此允许从对应于片段0的播发兴趣开始对清单片段进行安全编链。

[0101] 在此实例中，清单700的内容对象表示导致n个对象。从最终对象向后作业，将下一对象的内容对象散列在不同字段中插入到前一对象中。应注意，清单的最后一个内容对象不会具有下一内容对象的散列，且对应字段可为空的。用于内容对象730.1到730.n的散列分别为738.1到738.n(应注意，738.n未展示于图7B上)。在一些实施例中，使用与代管清单的节点相关联的密钥识别符734产生相应散列。此密钥识别符734可包含于相应内容对象中。内容对象730.4的散列(未展示于图7B上)为738.4，且包含在前一内容对象730.3中。类似地，用于内容对象730.3的散列为738.3，且包含在前一内容对象730.2中。以此方式，第一内容对象730.1包含下一内容对象730.2的散列738.2。

[0102] 在一些实施例中，清单700中的相应内容对象包含内容对象的签名。举例来说，内容对象730.1、730.2、730.3、...、730.n分别包含签名740.1、740.2、740.3、...、740.n。签名对应于对应内容对象中的其余元素的签名。举例来说，签名740.1为签名{名称730.1、密钥识别符734、清单片段0、散列738.2}的签名。

[0103] 一旦产生了第一内容对象730.1，则产生散列链的第一散列738.1。738.1的第一内容对象散列涵盖内容对象及散列链指针。因此，用于安全同步的播发兴趣由包括集合名称、相关名称空间的识别(例如，“adv”)、清单700的根散列及内容对象散列738.1的名称表示。如果相应节点具有不同密钥识别符，则每一节点产生唯一散列链，甚至对于相同清单700也是如此。结果，基于密钥识别符734的播发兴趣是唯一的，且转发器处的兴趣聚集得以避免。然而，如果节点已经知晓清单700的散列，则节点不需要检索清单700的每一实例，只要节点具有来自受信任源的至少一个实例即可。

[0104] 图8A呈现根据本发明的实施例的说明节点使用散列链安全地使本地清单同步的过程的流程图。在操作期间，节点创建包括对应片段S0到Sn的清单的相应内容对象(操作802)。从Sn开始，节点选择当前内容对象(操作804)，计算用于当前内容对象的散列并将所述散列插入到前一内容对象中(操作806)。节点接着检查当前对象是否为第一内容对象(操作808)。如果不是，则节点选择前一内容对象作为当前内容对象(操作810)，且继续计算当前内容对象的散列并将所述散列插入到前一内容对象中(操作806)。如果当前内容对象为第一内容对象，则节点发射具有内容对象名称的播发兴趣，所述内容对象名称包括前缀(或集合名称)、名称空间识别(例如，“adv”或“data”)、清单的根散列及对应于片段S0的第一内容对象散列(操作812)。

[0105] 图8B呈现根据本发明的实施例的说明节点使用散列链起始远程清单的安全同步的过程的流程图。在操作期间，节点接收具有内容对象名称的一或多个播发兴趣，所述内容对象名称包括前缀、名称空间识别及清单的根散列；并获得对应于相应播发兴趣的清单的相应初始片段(操作852)。在图7B的实例n中，在接收到播发712之后，节点即刻获得清单700的片段0(即，内容对象730.1)。应注意，节点包含清单且可能需要同步，如结合图2所描述。节点识别最大的内容对象散列值(操作854)，并检查所述清单是否来自有效(或受信任)发

布者(操作856)。在图7B中的实例中,密钥识别符734用于检查有效发布者。如果不是,则节点舍弃对应清单(操作858),且继续识别次大内容对象散列值(操作854)。

[0106] 如果所述兴趣是来自有效发布者,则节点检查根散列是否不同于本地根散列(操作862)。如果根散列不同,则节点起始同步过程(操作870),如结合图3所描述。否则,节点确定所识别的有效内容对象散列值是否大于本地内容对象散列值(操作864)。如果所识别的有效内容对象散列值大于本地内容对象散列值(操作866),则节点获得具有较大内容对象散列值的散列链(操作868)。

[0107] 图8C呈现根据本发明的实施例的说明节点使用散列链安全地使远程清单同步的过程的流程图。在操作期间,节点发射具有内容对象名称的数据兴趣,所述内容对象名称包括前缀、对应名称空间识别(例如,“data”)、根散列及对应于S0的内容散列(操作882)。节点接收具有清单片段的内容对象,提取所述清单片段,且获得下一内容对象的内容对象散列(操作884)。节点接着检查是否还存在内容对象(操作886)。如果还存在内容对象,则节点发射具有内容对象名称的数据兴趣,所述内容对象名称包括前缀、对应名称空间识别、根散列及下一内容对象的内容对象散列(操作888)。否则,节点从所接收清单片段建构清单(操作890)。

[0108] 在本发明的实施例中,除包括可路由前缀、相关名称空间的识别及清单的根散列值的三部分名称之外,用于清单的播发兴趣还携载内容对象的散列。此内容对象可对应于包括清单的相应内容对象的散列值的安全目录。并非播发清单的第一片段的内容对象散列,节点可播发枚举清单的所有片段的安全目录的名称。在一些实施例中,还可对安全目录进行分段。此可通过使下载管线化而允许较快执行,因为装置可在一个往返之后检索目录的多个片段。

[0109] 此实施例具有另一益处。因为其使用安全目录用于签名,因此包括清单的个别内容对象不为发布者特定的。因此,内容对象的散列值并不取决于哪一节点产生了目录,由此改善高速缓存及重复使用。

[0110] 图9A说明根据本发明的实施例的用于清单的安全同步的示范性安全目录。在此实例中,用于清单700的安全目录900包含清单700的第一内容对象730.1的名称732.1。目录900还列出清单700的内容对象散列738.1到738.n。在一些实施例中,清单700的内容对象未加签名,且对于具有相同清单700的每一发布者可为相同的。唯一的差异是安全目录900的签名。如果清单700的安全目录900对于单个内容对象来说过大,则在第一内容对象之后的后续对象可不加签名且在发布者之间相同。仅安全目录的第一片段可含有发布者特定信息,例如签名及时间戳,且对于目录的后边片段使用安全方法,例如散列链。

[0111] 在此实例中,系统将清单700分解成分别具有散列738.1到738.n的n个内容对象730.1到730.n。在一些实施例中,内容对象730.1到730.n并不包含发布者特定数据且未加签名。系统创建条目包括散列738.1到738.n的安全目录900。目录900可加签名。目录900的内容对象可具有散列<cataloghash>。所得播发兴趣具有形式为“/a/b/adv/<roothash>/<cataloghash>”的名称。来自对于相同清单的多个发布者的安全目录可使用分布式选举以收敛于一个安全目录上。分布式选举的实例包含但不限于最大及最小散列值。使用安全目录的安全同步的一个优势为目录的内容对象可在所有发布者之间相同。结果,分布式选举仅用于使用安全目录名称。在一些实施例中,目录的内容可在对于相同清单散列的

所有发布者之间相同。

[0112] 图9B说明根据本发明的实施例的使用安全目录的清单的示范性安全同步。在操作期间，节点102发射send_advertisement兴趣912(即，播发兴趣)，其为含有由集合名称“/a/b”识别的其清单的根散列值及对应安全目录(例如，目录900)的散列＜cataloghash＞的散列播发。兴趣采用以下形式：“/a/b/adv/＜roothash＞/＜cataloghash＞”。此安全目录包含清单的片段的相应内容对象散列。节点106接收所述兴趣，并发送包括目录的第一片段的兴趣的request_catalog兴趣914(即，数据兴趣)。兴趣914可采用以下形式：“/a/b/data/＜roothash＞/catalog/S0，内容散列＝＜cataloghash＞”。换句话说，当节点请求具有内容对象散列的数据时，那一散列值处于兴趣914的相异字段中，且可能不并入在名称中。

[0113] 在一些实施例中，在接收到数据兴趣之后，节点102即刻为目录签名(程序932)，且发送包括对应内容对象(C0)的send_catalog消息916。此消息916包含目录的第一片段S0，且采用以下形式：“/a/b/data/＜roothash＞/catalog/S0+有效负载”，其中所述有效负载含有目录的所请求片段。消息916中的内容对象的散列为＜cataloghash＞(即，hash(C0)＝＜cataloghash＞)。在接收到目录之后，节点106即刻验证节点102的签名以确保节点102为目录的有效发布者，且检索相应内容对象散列(程序934)。节点106接着发送对于清单片段的一组兴趣。所述组兴趣基于分段协议而分段。所述兴趣在request_manifest_in_segments消息918(即，数据兴趣)中发送，且为以下形式：“/a/b/data/＜roothash＞/＜contenthash_1＞”、“/a/b/data/＜roothash＞/contenthash_2”、“/a/b/data/＜roothash＞/contenthash_3”，等。在实例图9A中，＜contenthash_1＞、＜contenthash_2＞及＜contenthash_3＞分别对应于散列738.1、738.2及738.3。

[0114] 图10A呈现根据本发明的实施例的说明节点安全地使用安全目录使本地清单同步的过程的流程图。在操作期间，节点创建包括对应片段S0到Sn的清单的相应内容对象(操作1002)。节点创建用于名称对应于对应于片段S0的第一内容对象的名称的清单的目录(操作1004)。从S0开始，节点选择当前内容对象(操作1006)，且计算用于当前内容对象的散列并将所述散列插入到目录中(操作1008)。节点接着检查当前目标是否为最后一个内容对象(操作1010)。如果不是，则节点选择下一内容对象作为当前内容对象(操作1012)，且继续计算当前内容对象的散列并将所述散列插入到目录中(操作1008)。

[0115] 如果当前内容对象是最后一个内容对象，则节点为目录签名，并发射具有目录名称的播发兴趣，所述目录名称包括前缀(或集合名称)、名称空间识别(例如，“adv”)、清单的根散列及目录的散列(包括目录的签名(即，目录的签名为目录的散列的一部分))(操作1014)。节点接收具有目录名称的数据兴趣，所述目录名称包括前缀、名称空间识别(例如，“data”)、清单的根散列及目录的散列(操作1016)。节点基于目录名称发射带签名的目录(操作1018)，如结合图9B所描述。

[0116] 图10B呈现根据本发明的实施例的说明节点使用安全目录安全地使远程清单同步的过程的流程图。在操作期间，节点接收具有目录名称的播发兴趣，所述目录名称包括前缀(或集合名称)、名称空间识别(例如，“adv”)、清单的根散列及目录的散列(操作1052)。应注意，节点包含清单且可能需要同步，如结合图2所描述。节点发射具有目录名称的数据兴趣，所述目录名称包括前缀、名称空间识别(例如，“data”)、清单的根散列及目录的散列(操作1054)。节点接收带签名的目录并验证所述签名(操作1056)。

[0117] 节点接着基于签名验证来检查目录是否为有效目录(操作1058)。如果目录有效，则节点从所述目录获得对应清单片段的相应内容对象散列(操作1060)。节点接着通过发射具有对应内容对象名称的相应数据兴趣而起始安全同步过程，所述内容对象名称包括前缀、名称空间识别、根散列及来自目录的相应内容对象散列(操作1062)。

[0118] 图11说明根据本发明的实施例的促进清单在CCN中的安全同步的示范性计算机及通信系统。计算机及通信系统1102包含处理器1104、存储器1106，及存储装置1108。存储器1106可包含充当管理存储器的易失性存储器(例如，RAM)，且可用以存储一或多个存储器池。此外，计算机及通信系统1102可耦合到显示装置1110、键盘1112，及指向装置1114。存储装置1108可存储操作系统1116、内容处理系统1118，及数据1132。

[0119] 安全内容处理系统1118可包含指令，所述指令在由计算机及通信系统1102执行时可致使计算机及通信系统1102执行本发明中描述的方法及/或过程。具体来说，安全内容处理系统1118可促进CCN中的清单的安全同步。在一些实施例中，安全内容处理系统1118可在多个计算机及通信系统上执行，所述多个计算机及通信系统能够交换描述与安全内容处理系统1118相关联的操作的状态的数据。

[0120] 综上所述，本发明的实施例提供促进CCN中的清单的安全同步的计算机系统及方法。在操作期间，所述系统产生包括系统的内容对象的名称的播发兴趣。此名称表示系统的对象集合，且包含基于系统的密钥的第一散列。所述第一散列对应于表示对象集合的清单的一或多个片段的相应内容对象散列。所述系统还基于来自远程节点的数据兴趣中的名称确定对于内容对象的请求。

[0121] 此具体实施方式中所描述的数据结构及代码通常存储在计算机可读存储媒体上，所述计算机可读存储媒体可以是能存储由计算机系统使用的代码及/或数据的任何装置或媒体。计算机可读存储媒体包含但不限于易失性存储器、非易失性存储器、磁性以及光学存储装置，例如磁盘驱动器、磁带、CD(压缩光盘)、DVD(数字通用光盘或数字视频光盘)或能够存储目前已知或稍后开发的计算机可读媒体的其它媒体。

[0122] 在具体实施方式部分中所描述的方法和过程可以编码及/或数据形式实施，所述编码及/或数据可以存储于如上文所描述的计算机可读存储媒体中。当计算机系统读取并且执行存储于计算机可读存储媒体上的编码及/或数据时，计算机系统执行以数据结构以及编码形式实施且存储在计算机可读存储媒体内的方法及程序。

[0123] 此外，上文描述的方法及过程可以包含在硬件模块或设备中。所述硬件模块或设备可包含但不限于专用集成电路(ASIC)芯片、现场可编程门阵列(FPGA)、在特定时间执行特定软件模块或一段代码的专用处理器或共享处理器及现在已知或稍后开发的其它可编程逻辑装置。当激活硬件模块或设备时，这些硬件模块或设备执行其内部所包含的方法及过程。

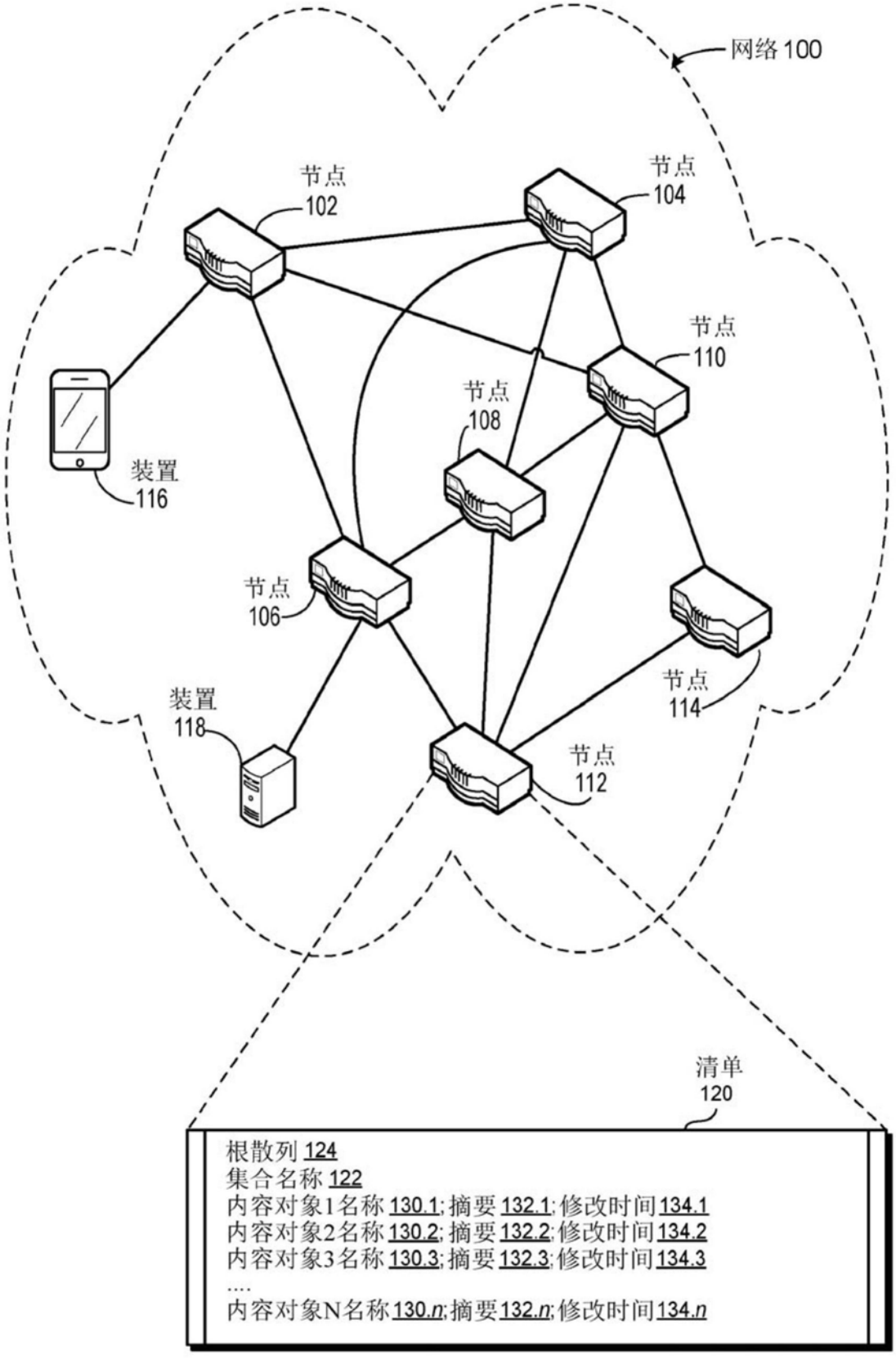

网络100
节点102
节点104
节点110
节点108
装置116
节点106
节点114
装置118
节点112
清单120
根散列 124
集合名称 122
内容对象1名称 130.1;摘要 132.1;修改时间134.1
内容对象2名称 130.2;摘要 132.2;修改时间134.2
内容对象3名称 130.3;摘要 132.3;修改时间134.3
....
内容对象N名称130.n;摘要132.n;修改时间134.n

图1

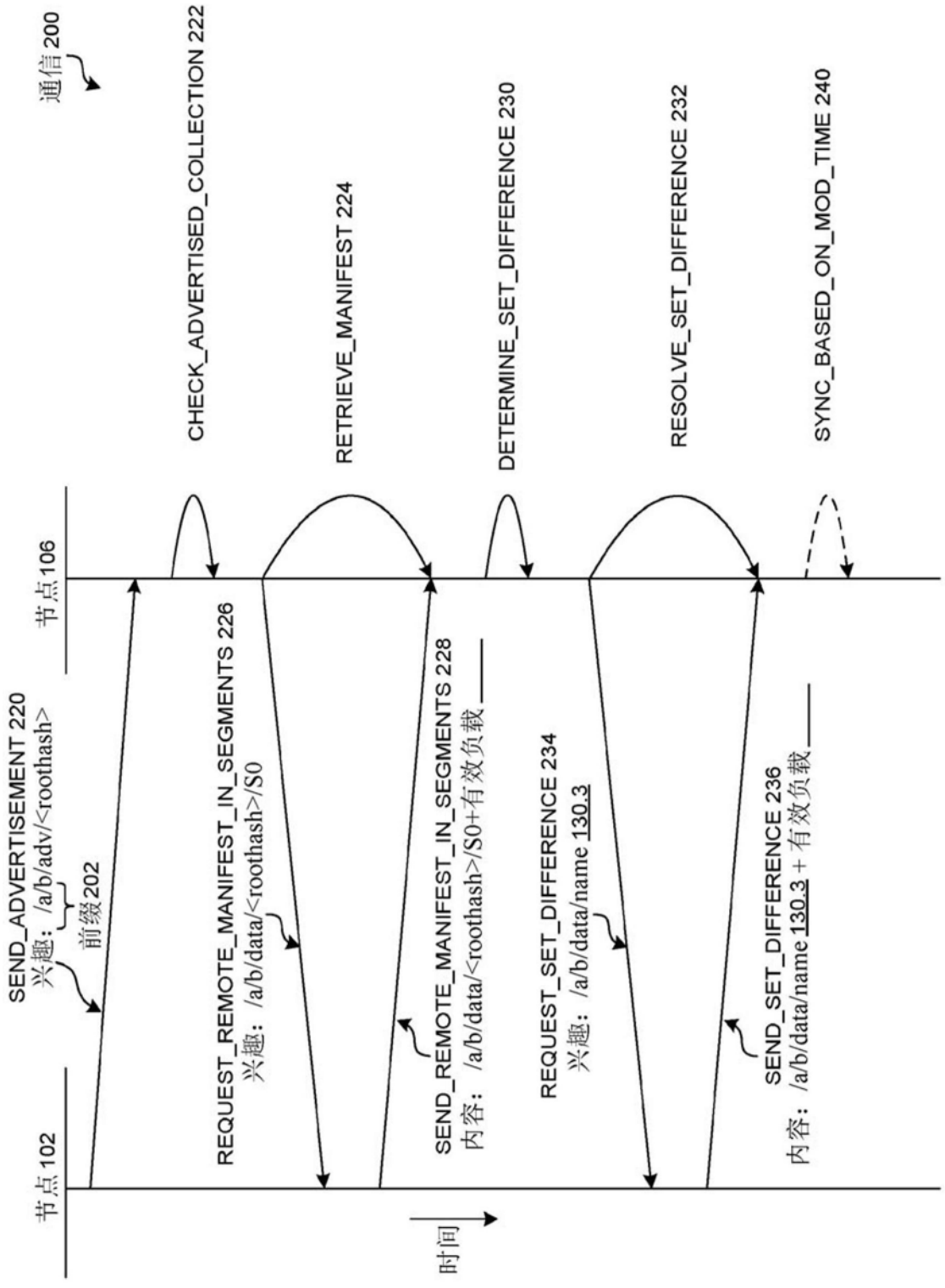

通信 200
CHECK_ADVERTISED_COLLECTION 222
RETRIEVE_MANIFEST 224
DETERMINE_SET_DIFFERENCE 230
RESOLVE_SET_DIFFERENCE 232
SYNC_BASED_ON_MOD_TIME 240
节点 106
节点 102
SEND_ADVERTISEMENT 220
兴趣：/a/b/adv/<roothash>
前缀 202
REQUEST_REMOTE_MANIFEST_IN_SEGMENTS 226
兴趣：/a/b/data/<roothash>/S0
SEND_REMOTE_MANIFEST_IN_SEGMENTS 228
内容：/a/b/data/<roothash>/S0+有效负载
REQUEST_SET_DIFFERENCE 234
兴趣：/a/b/data/name 130.3
SEND_SET_DIFFERENCE 236
内容：/a/b/data/name 130.3 + 有效负载
时间

图2

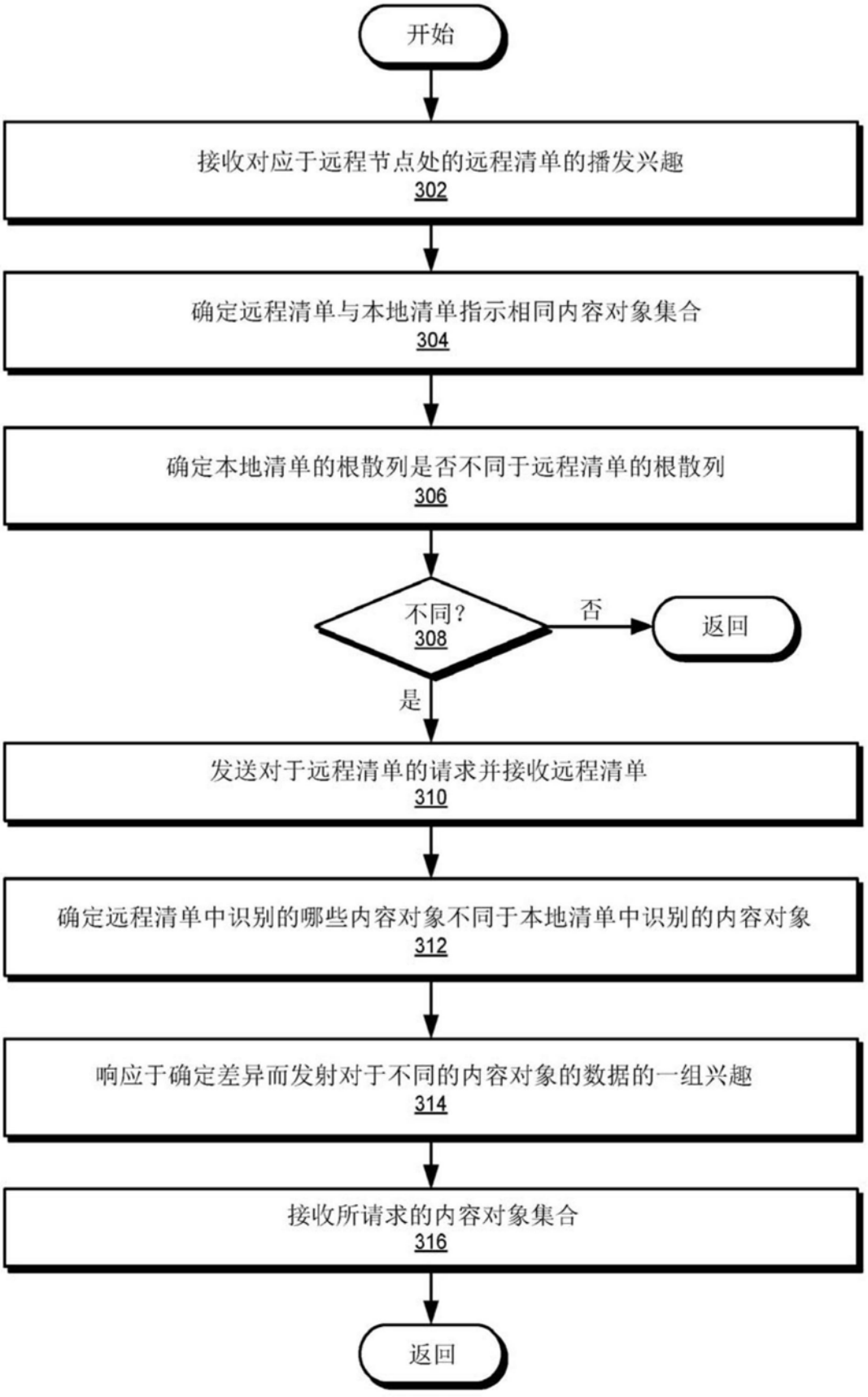

开始
接收对应于远程节点处的远程清单的播发兴趣
302
确定远程清单与本地清单指示相同内容对象集合
304
确定本地清单的根散列是否不同于远程清单的根散列
306
不同?
308
否
返回
是
发送对于远程清单的请求并接收远程清单
310
确定远程清单中识别的哪些内容对象不同于本地清单中识别的内容对象
312
响应于确定差异而发射对于不同的内容对象的数据的一组兴趣
314
接收所请求的内容对象集合
316
返回

图3

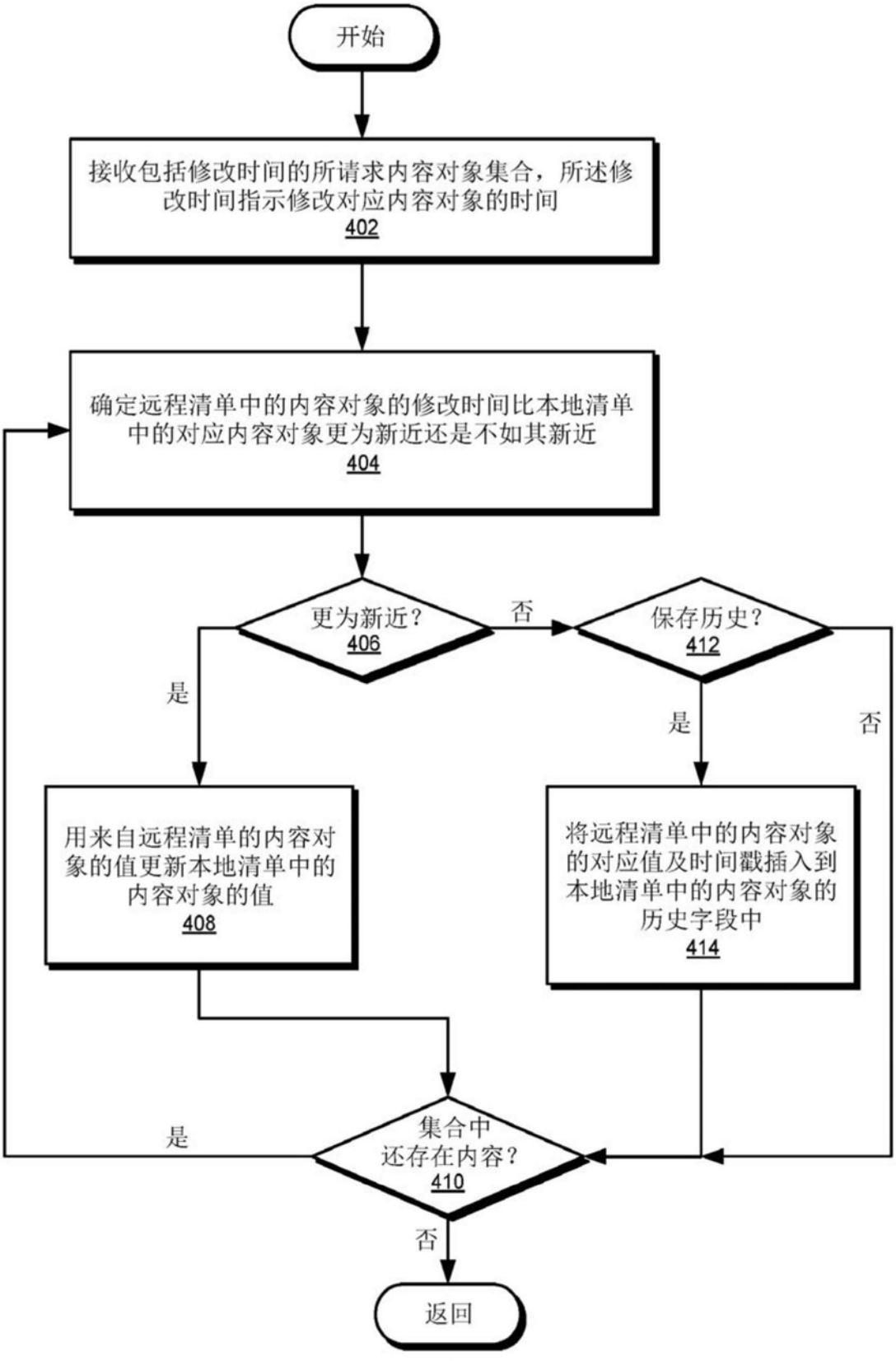

开始
接收包括修改时间的所请求内容对象集合，所述修改时间指示修改对应内容对象的时间
402
确定远程清单中的内容对象的修改时间比本地清单中的对应内容对象更为新近还是不如其新近
404
更为新近？
406
否
保存历史？
412
是
是
否
用来自远程清单的内容对象的值更新本地清单中的内容对象的值
408
将远程清单中的内容对象的对应值及时间戳插入到本地清单中的内容对象的历史字段中
414
是
集合中还存在内容？
410
否
返回

图4

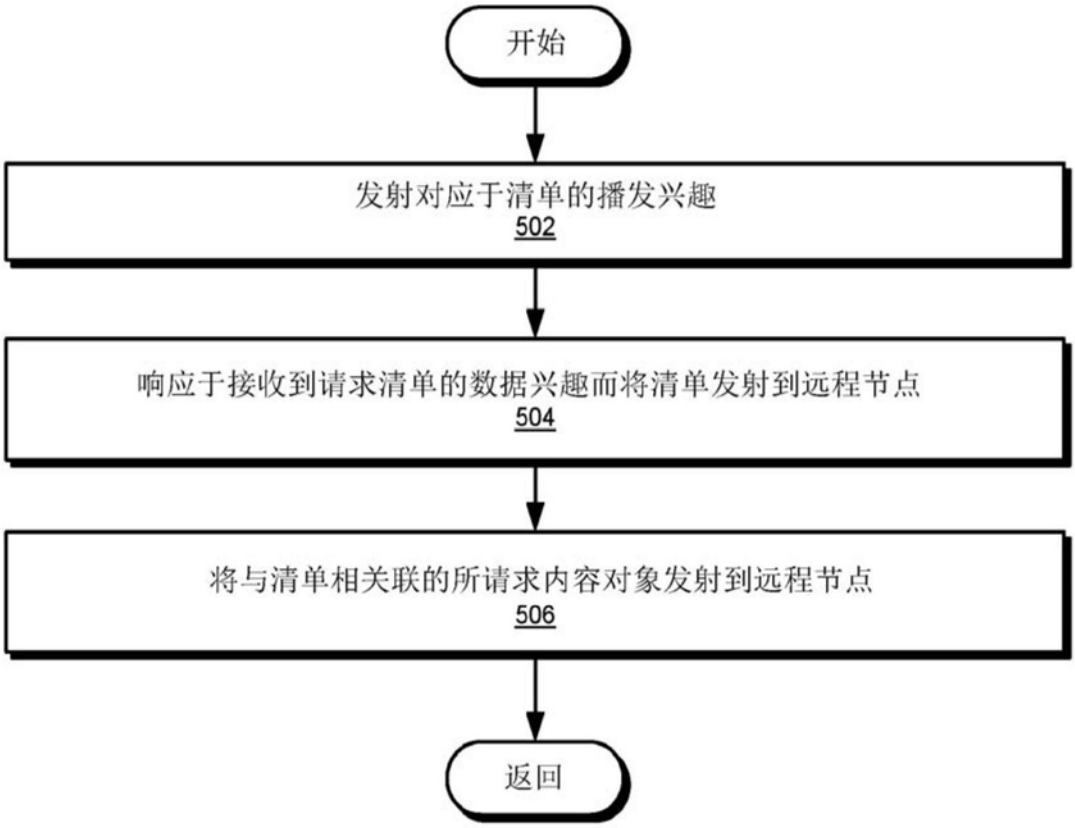

开始
发射对应于清单的播发兴趣
502
响应于接收到请求清单的数据兴趣而将清单发射到远程节点
504
将与清单相关联的所请求内容对象发射到远程节点
506
返回

图5

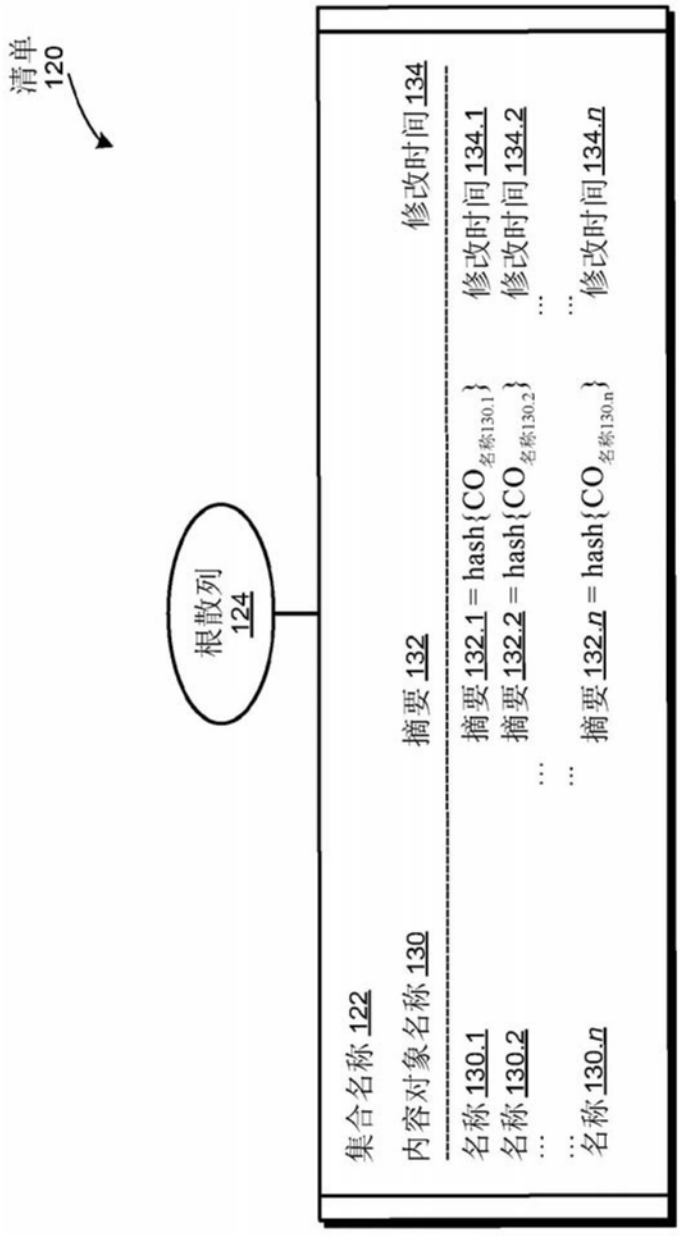

清单
120
根散列
124
集合名称 122
内容对象名称 130
摘要 132
修改时间 134
名称 130.1
名称 130.2
名称 130.n
摘要 132.1 = hash{CO名称130.1}
摘要 132.2 = hash{CO名称130.2}
摘要 132.n = hash{CO名称130.n}
修改时间 134.1
修改时间 134.2
修改时间 134.n

图6A

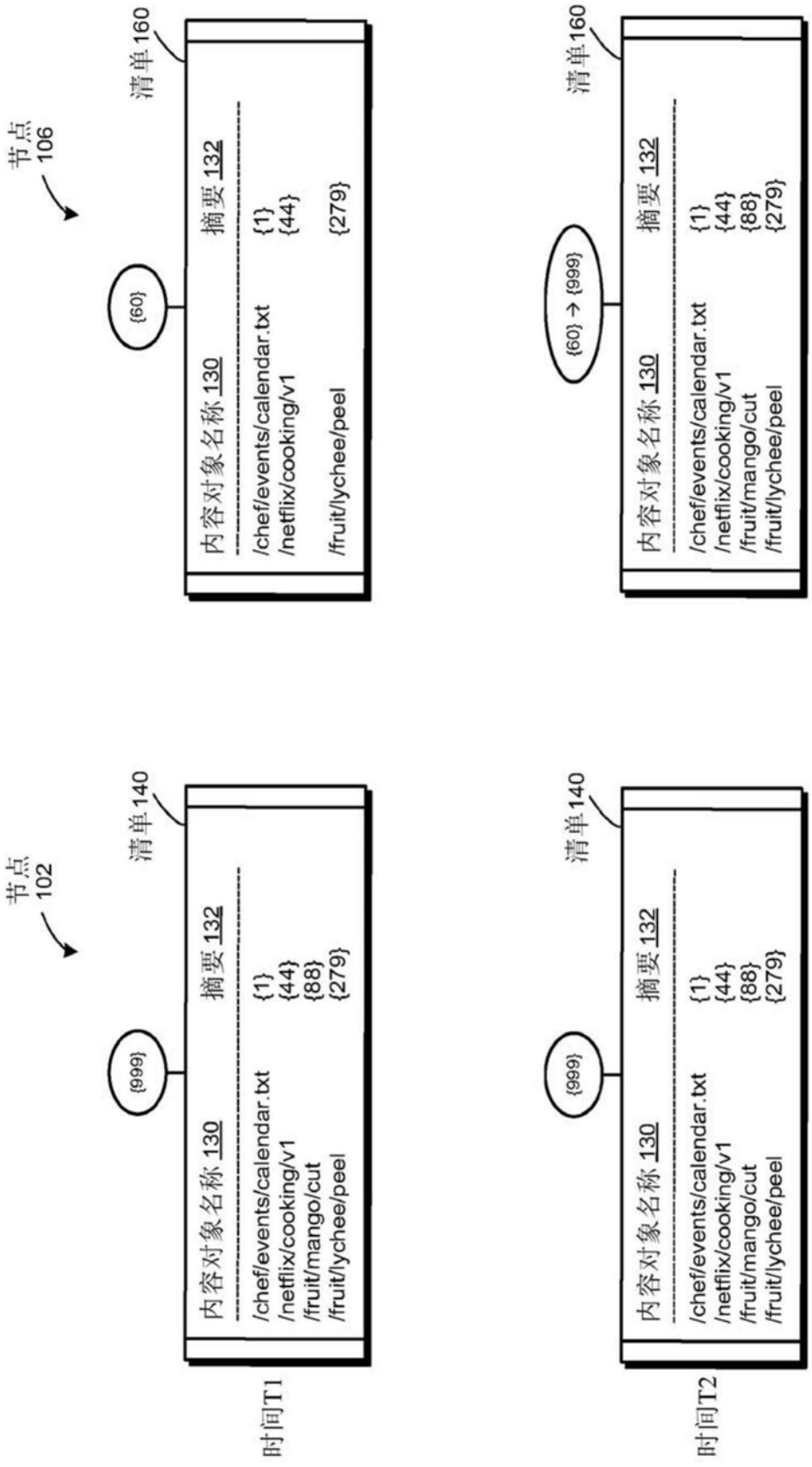

节点
106
清单160
{60}
内容对象名称 130
摘要 132
/chef/events/calendar.txt {1}
/netflix/cooking/v1 {44}
/fruit/lychee/peel {279}
{60} → {999}
节点
102
清单140
{999}
/fruit/mango/cut {88}
时间T1
时间T2

图6B

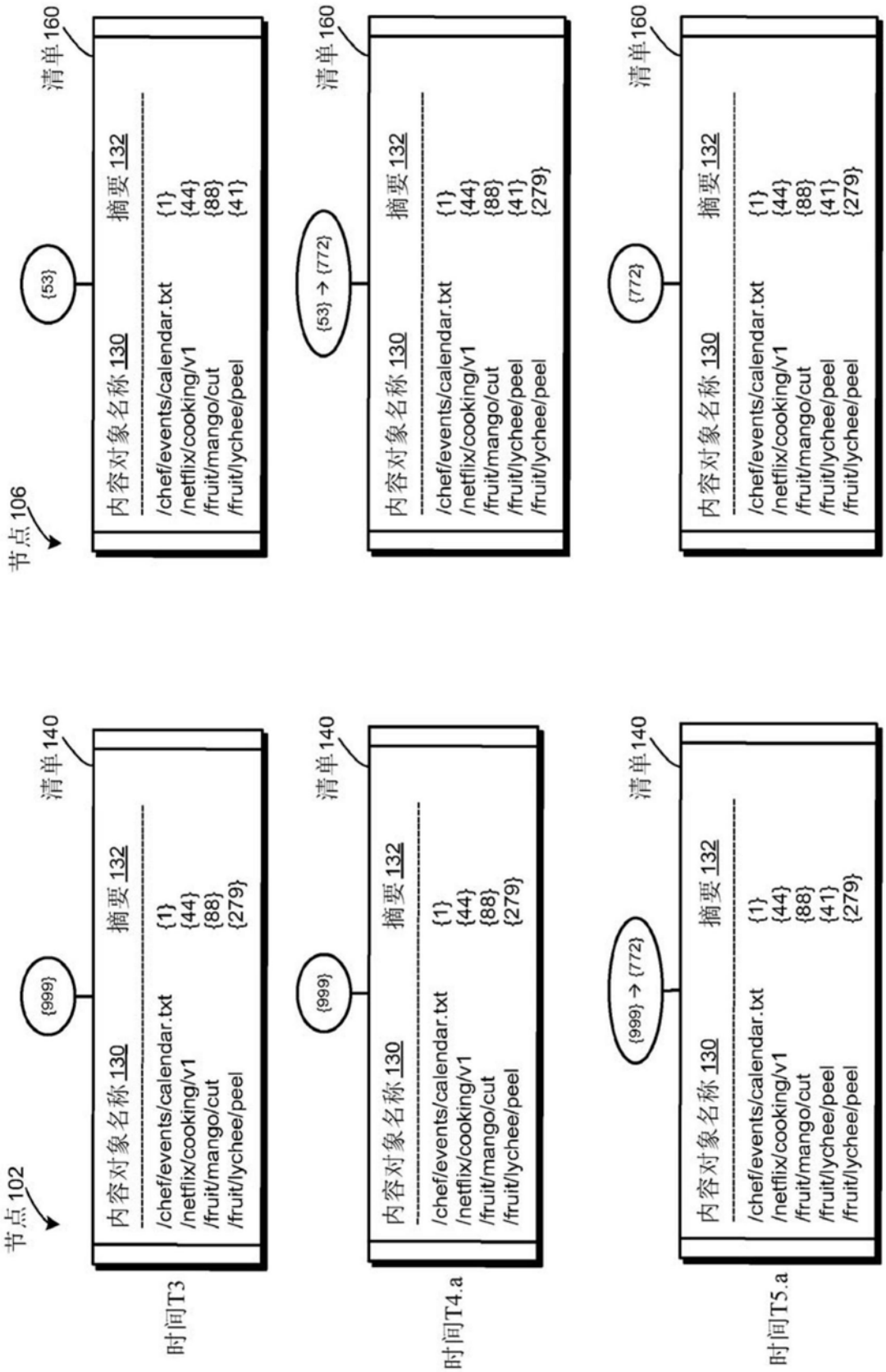

节点106
清单160
{53}
内容对象名称130
摘要132
/chef/events/calendar.txt {1}
/netflix/cooking/v1 {44}
/fruit/mango/cut {88}
/fruit/lychee/peel {41}
{53} → {772}
{772}
/fruit/lychee/peel {279}
节点102
清单140
{999}
{999} → {772}
时间T3
时间T4.a
时间T5.a

图6C

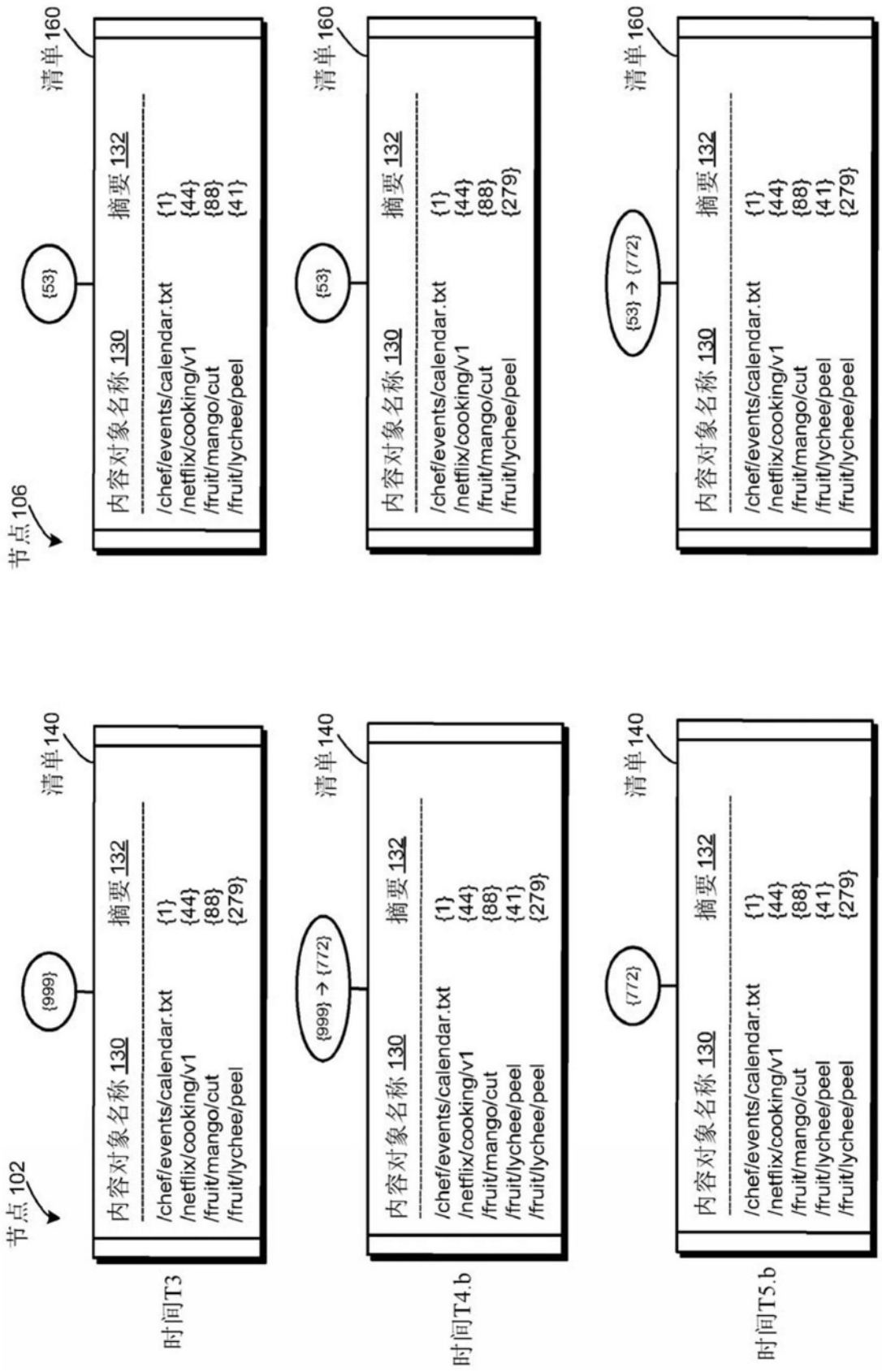

节点106
清单160
{53}
内容对象名称 130
摘要 132
/chef/events/calendar.txt {1}
/netflix/cooking/v1 {44}
/fruit/mango/cut {88}
/fruit/lychee/peel {41}
{279}
{53} → {772}
节点102
清单140
{999}
{999} → {772}
{772}
时间T3
时间T4.b
时间T5.b

图6D

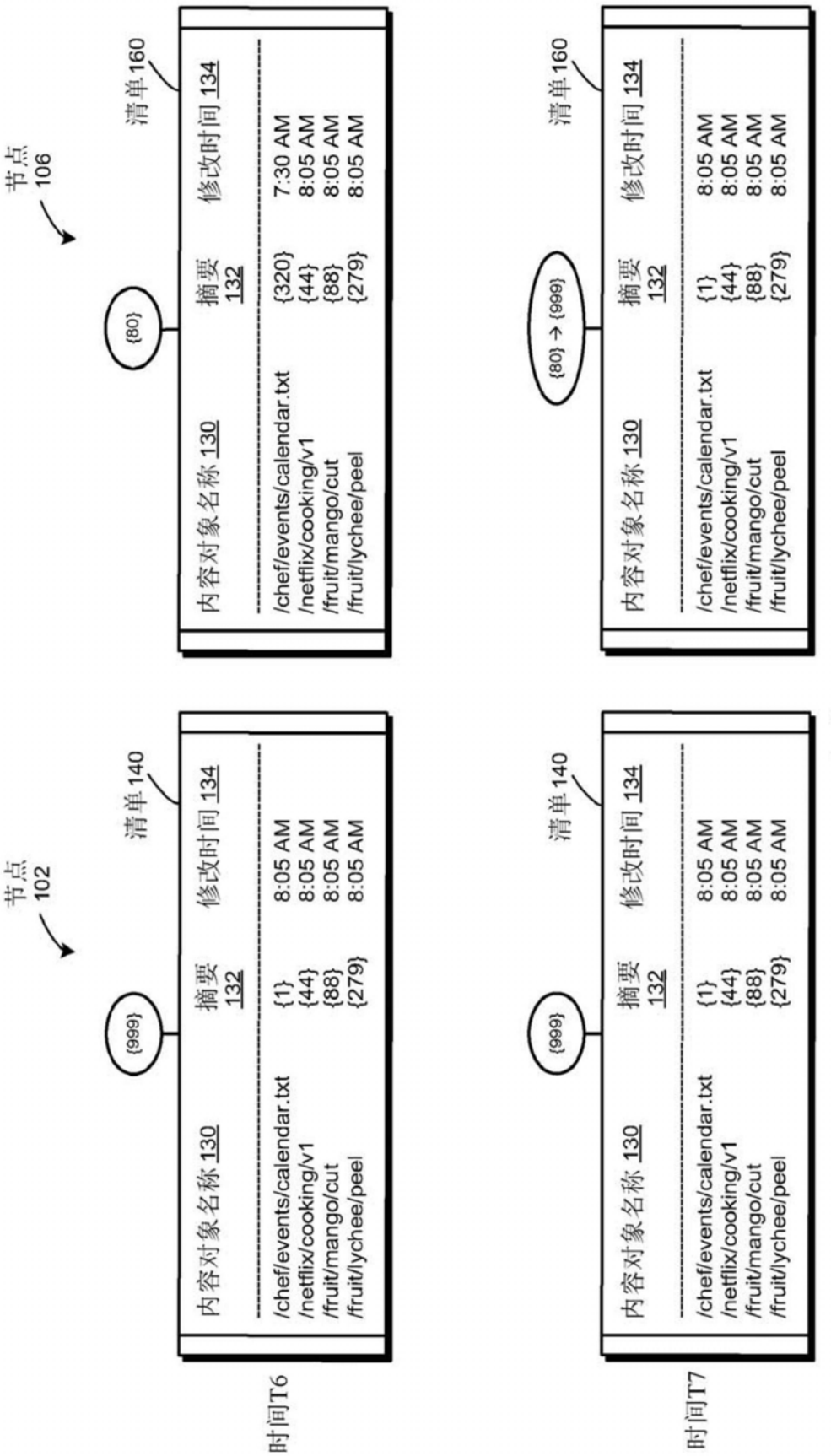

节点
102
清单140
{999}
摘要
132
修改时间 134
内容对象名称 130
/chef/events/calendar.txt {1} 8:05 AM
/netflix/cooking/v1 {44} 8:05 AM
/fruit/mango/cut {88} 8:05 AM
/fruit/lychee/peel {279} 8:05 AM
时间T6
节点
106
清单160
{80}
摘要
132
修改时间 134
内容对象名称 130
/chef/events/calendar.txt {320} 7:30 AM
/netflix/cooking/v1 {44} 8:05 AM
/fruit/mango/cut {88} 8:05 AM
/fruit/lychee/peel {279} 8:05 AM
清单140
{999}
摘要
132
修改时间 134
内容对象名称 130
/chef/events/calendar.txt {1} 8:05 AM
/netflix/cooking/v1 {44} 8:05 AM
/fruit/mango/cut {88} 8:05 AM
/fruit/lychee/peel {279} 8:05 AM
时间T7
清单160
{80} → {999}
摘要
132
修改时间 134
内容对象名称 130
/chef/events/calendar.txt {1} 8:05 AM
/netflix/cooking/v1 {44} 8:05 AM
/fruit/mango/cut {88} 8:05 AM
/fruit/lychee/peel {279} 8:05 AM

图6E

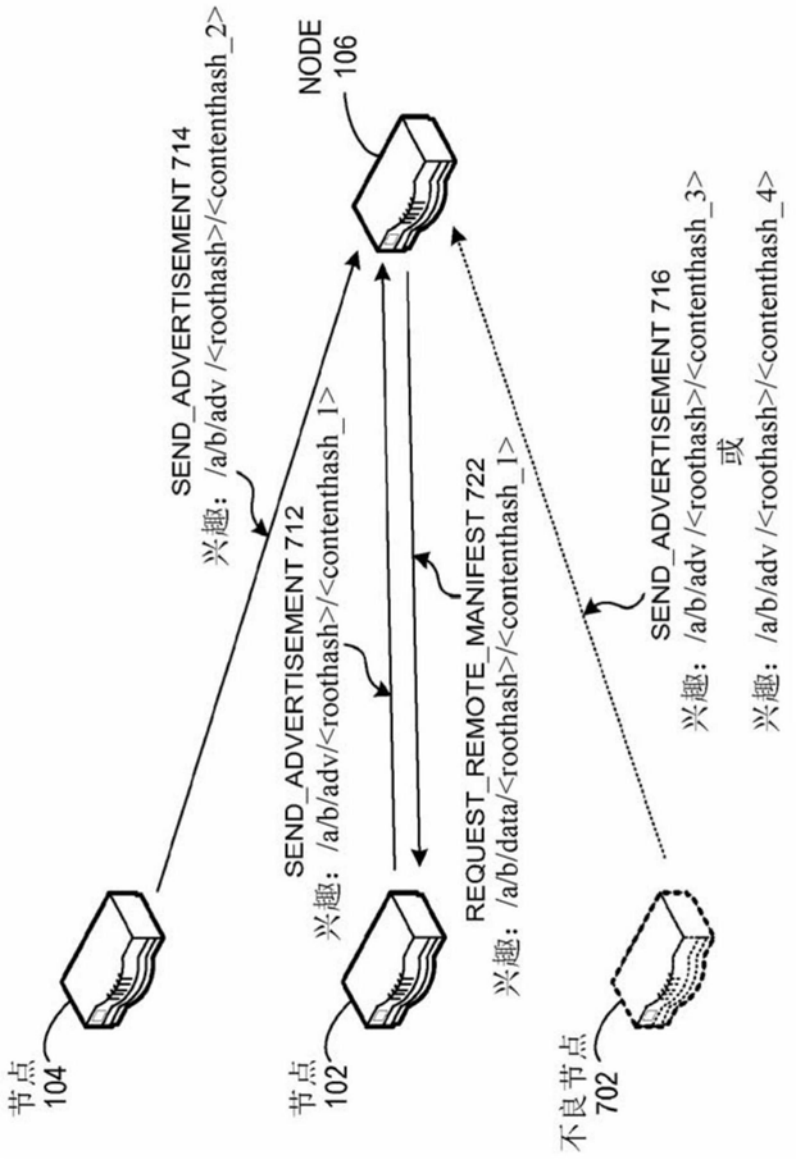

NODE
106
SEND_ADVERTISEMENT 714
兴趣：/a/b/adv /<roothash>/<contenthash_2>
SEND_ADVERTISEMENT 712
兴趣：/a/b/adv/<roothash>/<contenthash_1>
REQUEST_REMOTE_MANIFEST 722
兴趣：/a/b/data/<roothash>/<contenthash_1>
SEND_ADVERTISEMENT 716
兴趣：/a/b/adv /<roothash>/<contenthash_3>
或
兴趣：/a/b/adv /<roothash>/<contenthash_4>
节点
104
节点
102
不良节点
702

图7A

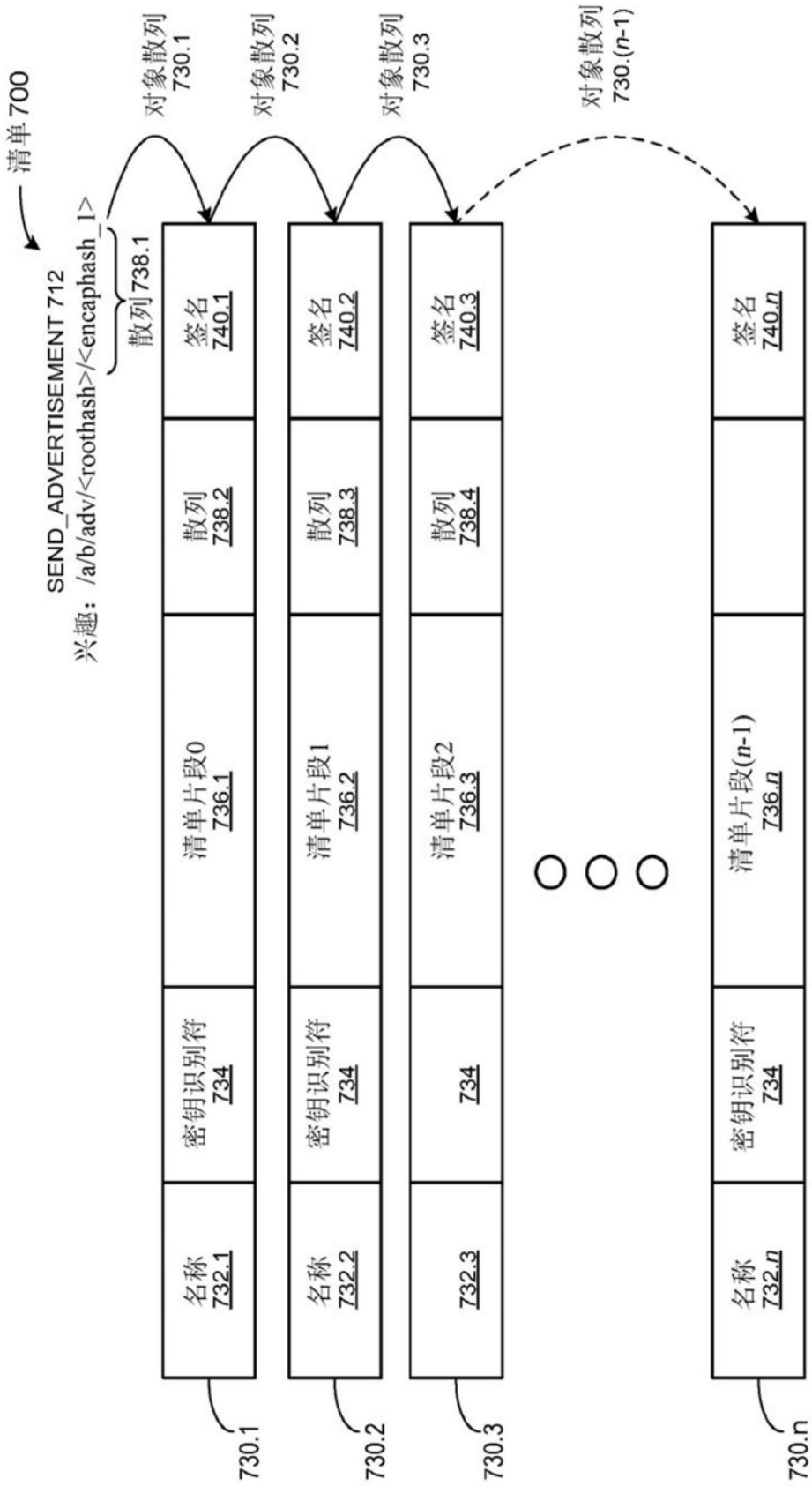

清单 700
SEND_ADVERTISEMENT 712
兴趣：/a/b/adv/<roothash>/<encaphash_1>
散列 738.1
对象散列 730.1
对象散列 730.2
对象散列 730.3
对象散列 730.(n-1)
名称 732.1
密钥识别符 734
清单片段0 736.1
散列 738.2
签名 740.1
名称 732.2
密钥识别符 734
清单片段1 736.2
散列 738.3
签名 740.2
732.3
734
清单片段2 736.3
散列 738.4
签名 740.3
名称 732.n
密钥识别符 734
清单片段(n-1) 736.n
签名 740.n
730.1
730.2
730.3
730.n

图7B

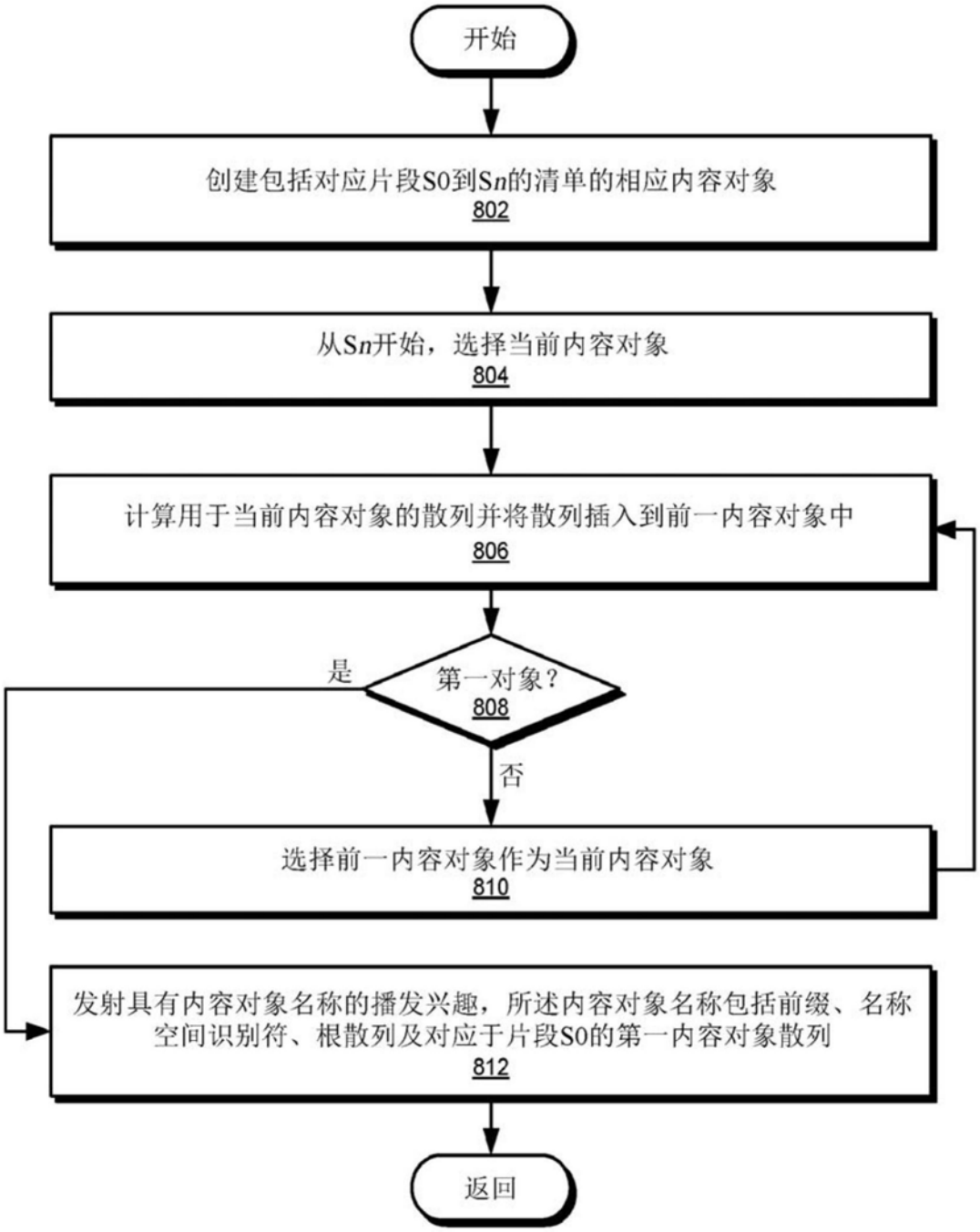

开始
创建包括对应片段S0到Sn的清单的相应内容对象
802
从Sn开始，选择当前内容对象
804
计算用于当前内容对象的散列并将散列插入到前一内容对象中
806
第一对象？
808
是
否
选择前一内容对象作为当前内容对象
810
发射具有内容对象名称的播发兴趣，所述内容对象名称包括前缀、名称空间识别符、根散列及对应于片段S0的第一内容对象散列
812
返回

图8A

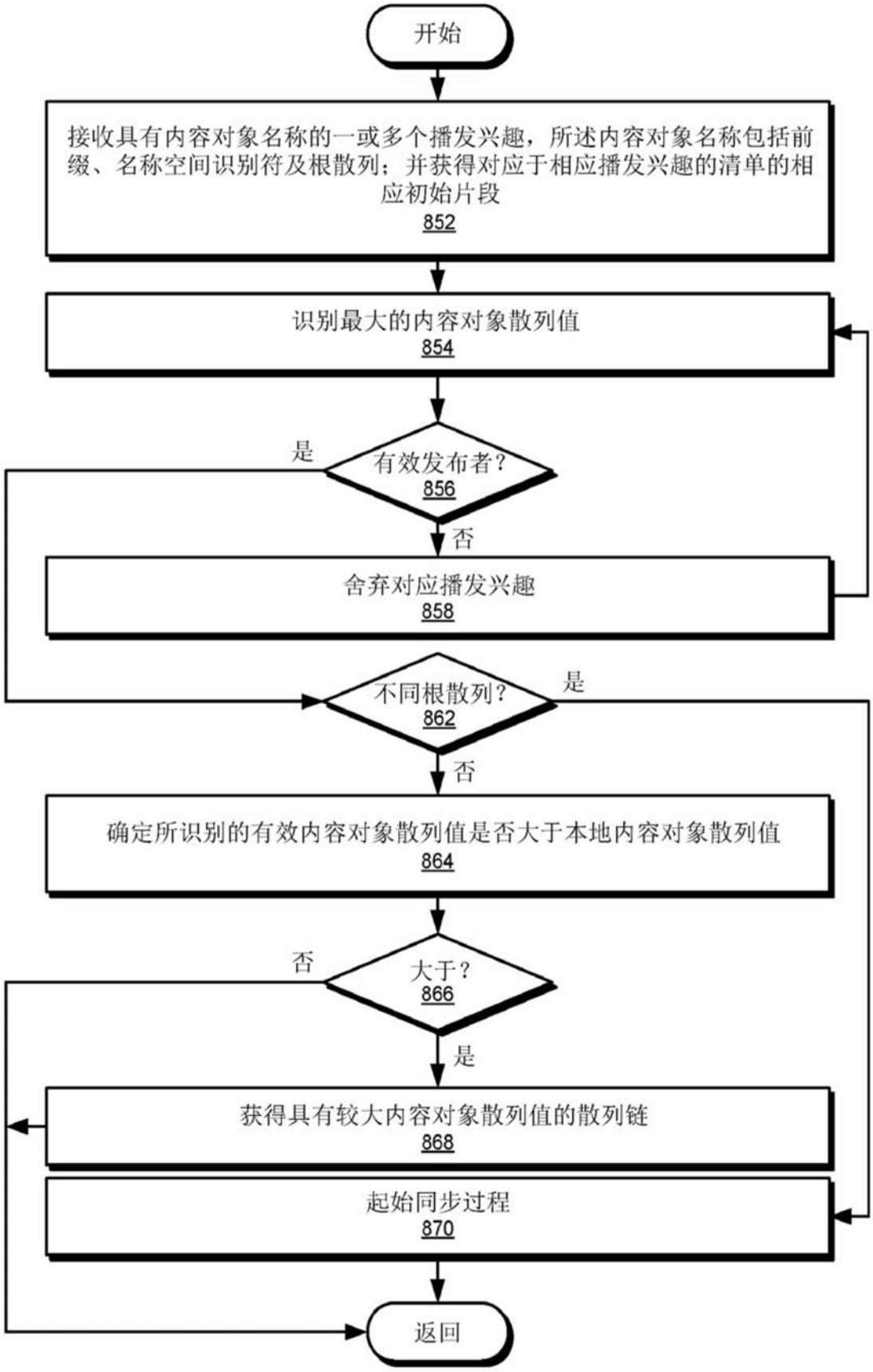

开始
接收具有内容对象名称的一或多个播发兴趣，所述内容对象名称包括前缀、名称空间识别符及根散列；并获得对应于相应播发兴趣的清单的相应初始片段
852
识别最大的内容对象散列值
854
是
有效发布者？
856
否
舍弃对应播发兴趣
858
不同根散列？
862
是
否
确定所识别的有效内容对象散列值是否大于本地内容对象散列值
864
否
大于？
866
是
获得具有较大内容对象散列值的散列链
868
起始同步过程
870
返回

图8B

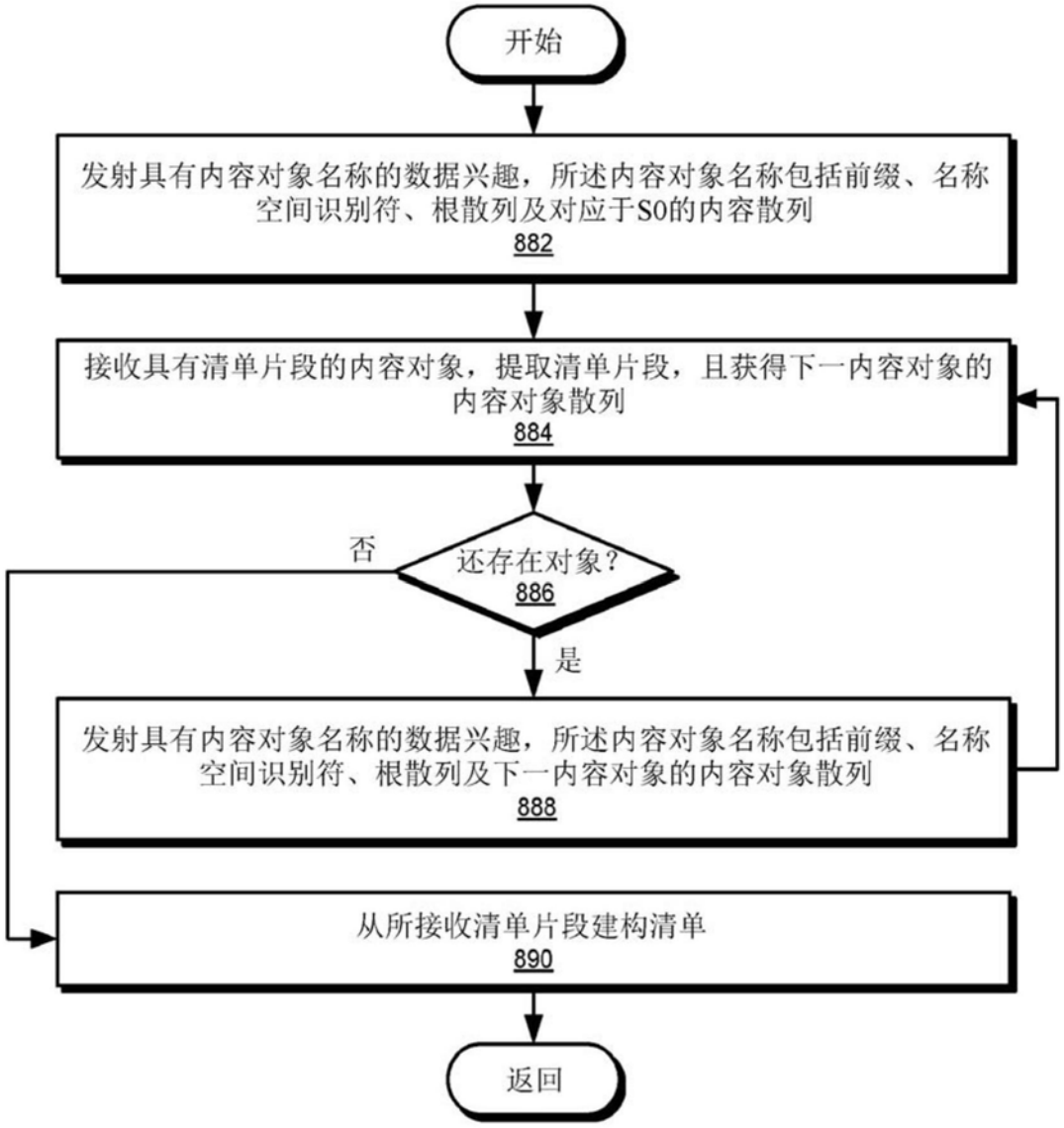

开始
发射具有内容对象名称的数据兴趣，所述内容对象名称包括前缀、名称空间识别符、根散列及对应于S0的内容散列
882
接收具有清单片段的内容对象，提取清单片段，且获得下一内容对象的内容对象散列
884
否
还存在对象？
886
是
发射具有内容对象名称的数据兴趣，所述内容对象名称包括前缀、名称空间识别符、根散列及下一内容对象的内容对象散列
888
从所接收清单片段建构清单
890
返回

图8C

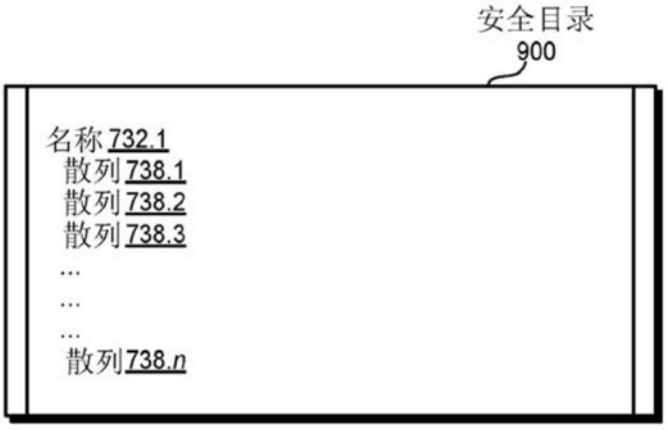

安全目录
900
名称 732.1
散列 738.1
散列 738.2
散列 738.3
...
...
...
散列 738.n

图9A

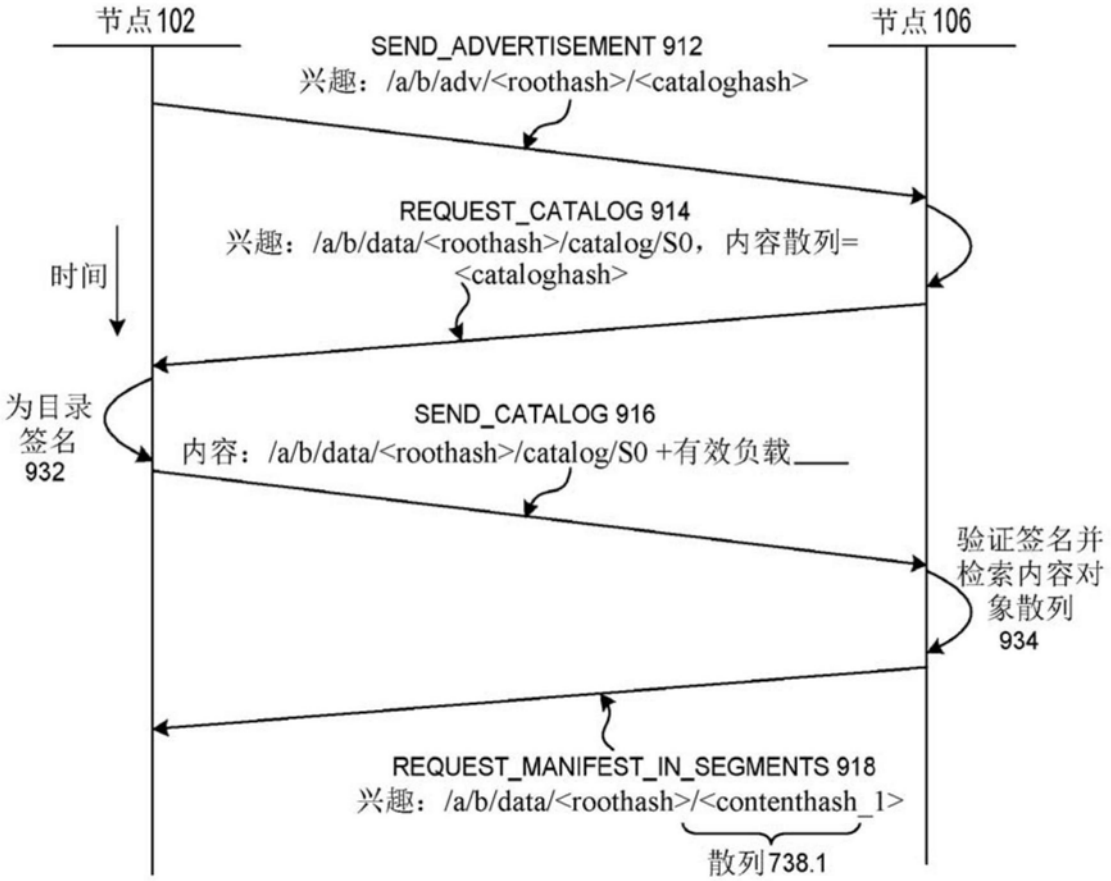

节点102
节点106
SEND_ADVERTISEMENT 912
兴趣：/a/b/adv/<roothash>/<cataloghash>
REQUEST_CATALOG 914
兴趣：/a/b/data/<roothash>/catalog/S0，内容散列=
<cataloghash>
时间
为目录
签名
932
SEND_CATALOG 916
内容：/a/b/data/<roothash>/catalog/S0 +有效负载
验证签名并
检索内容对
象散列
934
REQUEST_MANIFEST_IN_SEGMENTS 918
兴趣：/a/b/data/<roothash>/<contenthash_1>
散列738.1

图9B

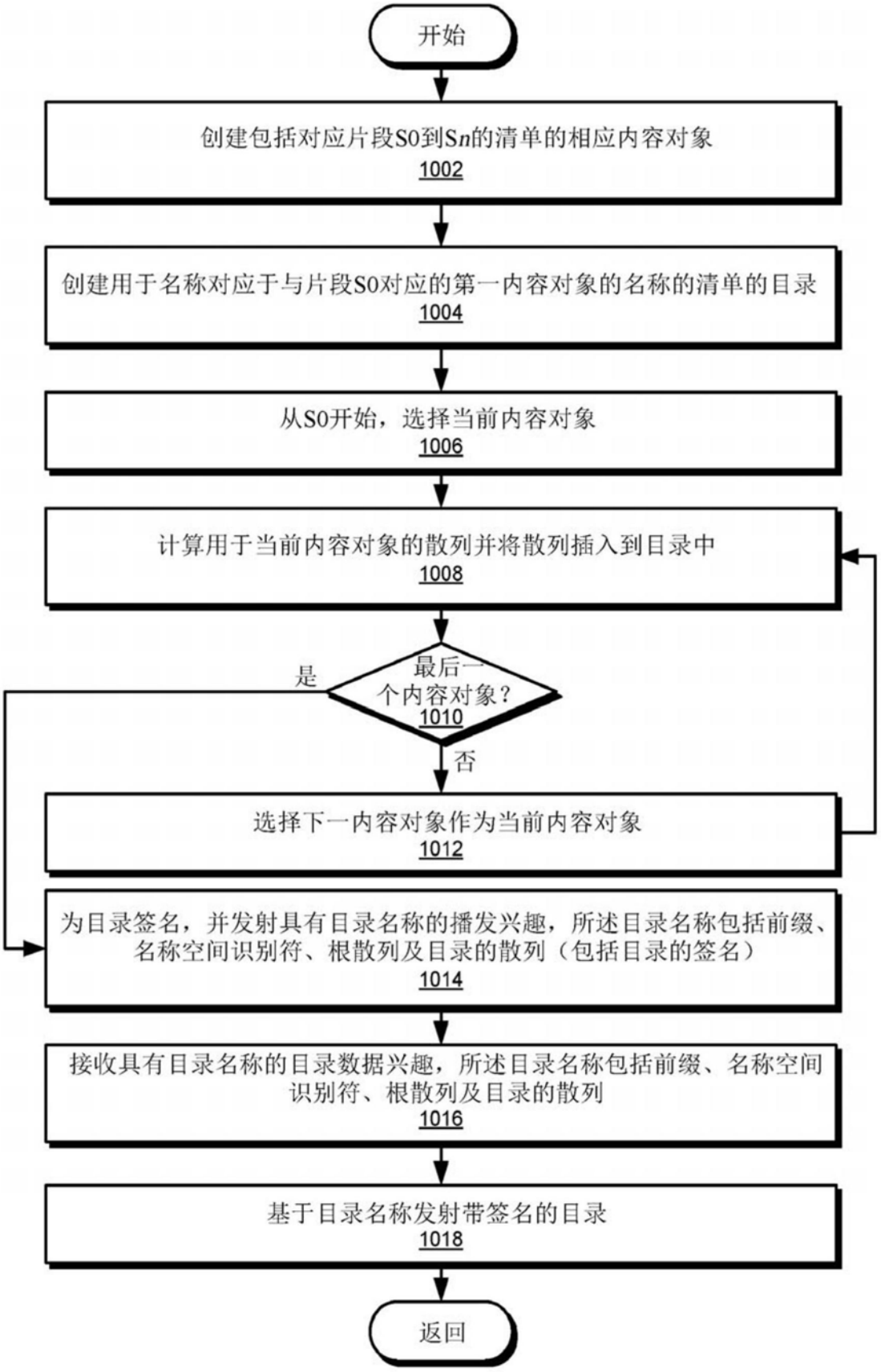

开始
创建包括对应片段S0到Sn的清单的相应内容对象
1002
创建用于名称对应于与片段S0对应的第一内容对象的名称的清单的目录
1004
从S0开始，选择当前内容对象
1006
计算用于当前内容对象的散列并将散列插入到目录中
1008
最后一个内容对象？
1010
是
否
选择下一内容对象作为当前内容对象
1012
为目录签名，并发射具有目录名称的播发兴趣，所述目录名称包括前缀、名称空间识别符、根散列及目录的散列（包括目录的签名）
1014
接收具有目录名称的目录数据兴趣，所述目录名称包括前缀、名称空间识别符、根散列及目录的散列
1016
基于目录名称发射带签名的目录
1018
返回

图10A

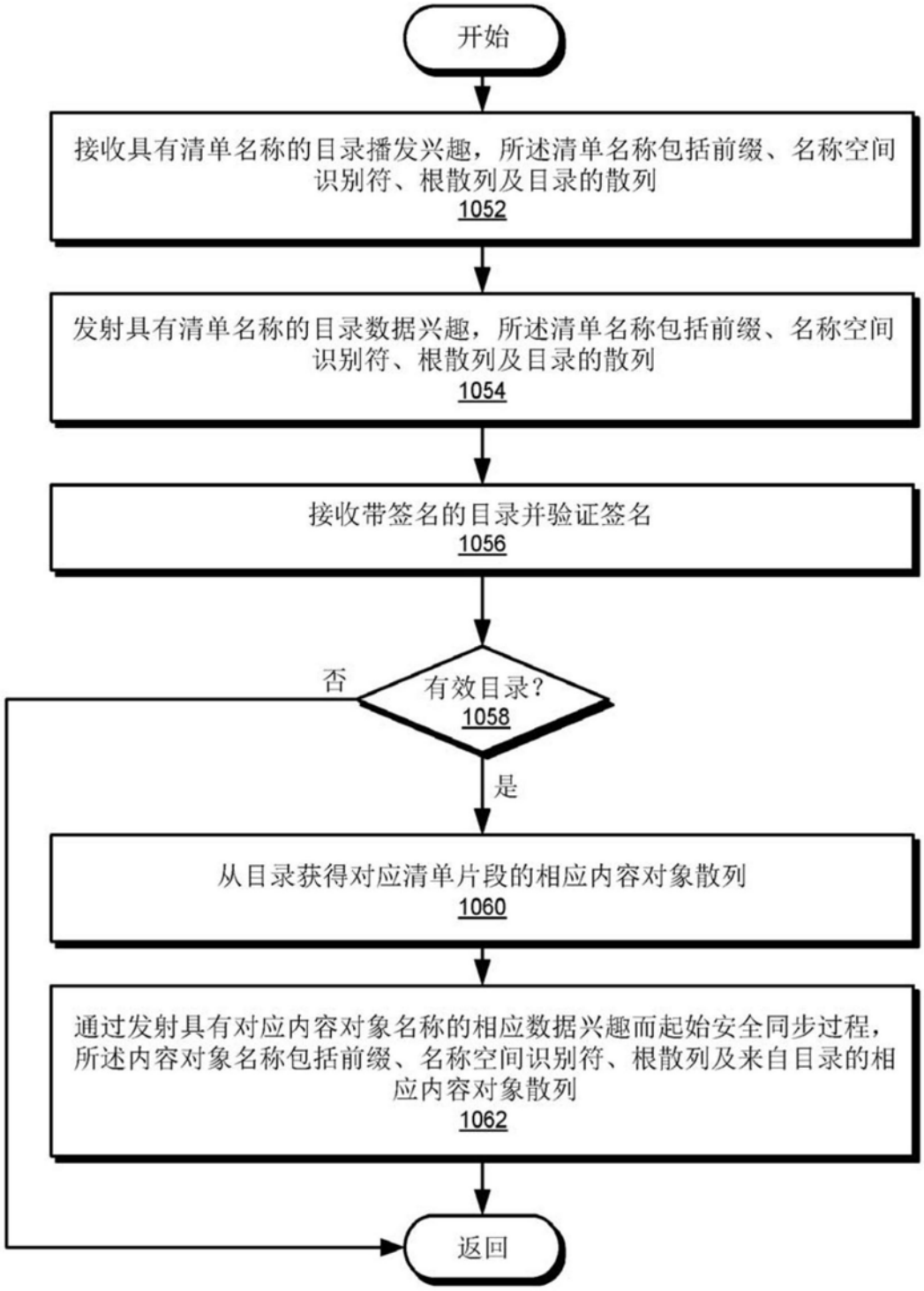

开始
接收具有清单名称的目录播发兴趣，所述清单名称包括前缀、名称空间识别符、根散列及目录的散列
1052
发射具有清单名称的目录数据兴趣，所述清单名称包括前缀、名称空间识别符、根散列及目录的散列
1054
接收带签名的目录并验证签名
1056
有效目录？
1058
否
是
从目录获得对应清单片段的相应内容对象散列
1060
通过发射具有对应内容对象名称的相应数据兴趣而起始安全同步过程，所述内容对象名称包括前缀、名称空间识别符、根散列及来自目录的相应内容对象散列
1062
返回

图10B

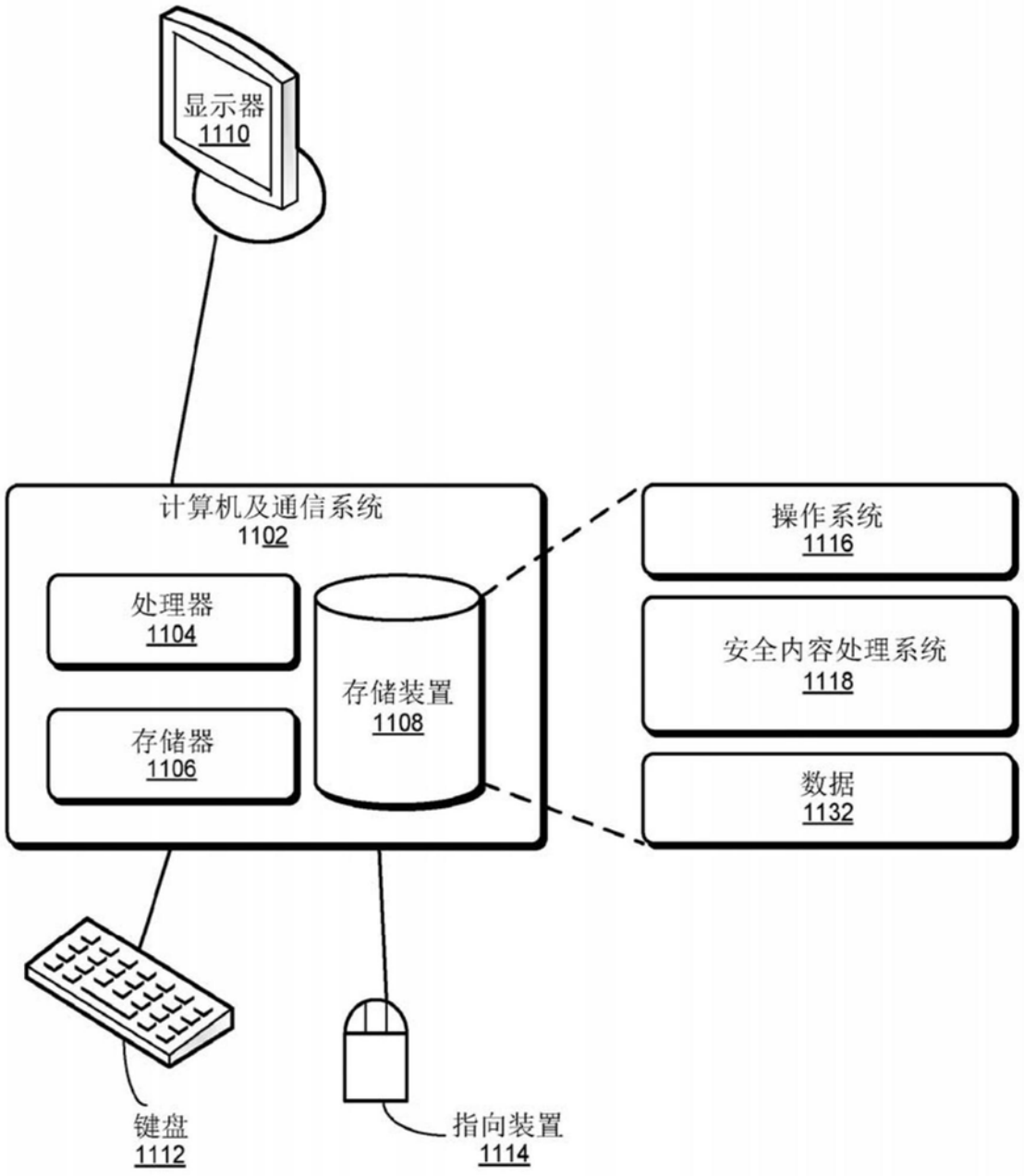

显示器
1110
计算机及通信系统
1102
处理器
1104
存储器
1106
存储装置
1108
操作系统
1116
安全内容处理系统
1118
数据
1132
键盘
1112
指向装置
1114

图11