



(12)发明专利

(10)授权公告号 CN 109639758 B

(45)授权公告日 2020.05.12

(21)申请号 201811290195.2

(22)申请日 2018.10.31

(65)同一申请的已公布的文献号  
申请公布号 CN 109639758 A

(43)申请公布日 2019.04.16

(73)专利权人 中国科学院信息工程研究所  
地址 100093 北京市海淀区闵庄路甲89号

(72)发明人 刘银龙 李婷 张杭生 梁杰

(74)专利代理机构 北京路浩知识产权代理有限公司 11002

代理人 王莹 吴欢燕

(51)Int.Cl.

H04L 29/08(2006.01)

H04L 29/06(2006.01)

G06F 21/62(2013.01)

(56)对比文件

- CN 105791392 A,2016.07.20,
- CN 106254069 A,2016.12.21,
- CN 104780205 A,2015.07.15,
- CN 106101223 A,2016.11.09,
- CN 108366089 A,2018.08.03,
- CN 101645888 A,2010.02.10,
- CN 101645921 A,2010.02.10,
- CN 101645923 A,2010.02.10,
- US 2016156714 A1,2016.06.02,
- US 2014164552 A1,2014.06.12,
- WO 2013004261 A1,2013.01.10,
- CN 105376229 A,2016.03.02,
- CN 105208553 A,2015.12.30,
- CN 108134774 A,2018.06.08,

审查员 王星

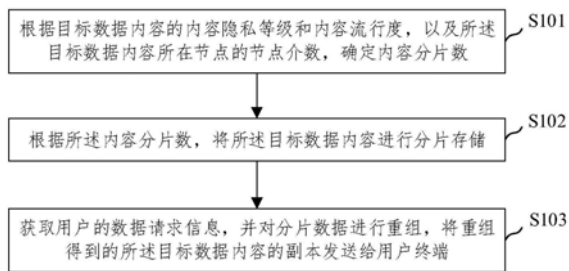
权利要求书2页 说明书8页 附图4页

(54)发明名称

内容中心网络中用户行为隐私的保护方法及装置

(57)摘要

本发明实施例提供一种内容中心网络中用户行为隐私的保护方法及装置,所述方法包括:根据目标数据内容的内容隐私等级和内容流行度,以及节点介数,确定内容分片数;根据内容分片数,将目标数据内容进行分片存储;获取用户的数据请求信息,并对分片数据进行重组,将重组得到的目标数据内容的副本发送给用户终端。本发明实施例提供的内容中心网络中用户行为隐私的保护方法及装置,对数据内容进行隐私等级划分,以及实行分片存储和重组,一方面减少非隐私内容对网络和路由器产生的负担,保证CCN分发效率的优势,另一方面通过分片存储和重组增加时间不确定性,抵抗时间攻击,阻止攻击者从往返时间上判断相邻用户的偏好,保护用户的行为隐私。



1. 一种内容中心网络中用户行为隐私的保护方法,其特征在于,包括:

根据目标数据内容的内容隐私等级和内容流行度,以及所述目标数据内容所在节点的节点介数,通过预设的二元线性回归模型确定内容分片数;

根据所述内容分片数,将所述目标数据内容进行分片存储;

获取用户的数据请求信息,并对分片数据进行重组,将重组得到的所述目标数据内容的副本发送给用户终端;

所述二元线性回归模型如下:

$$N_{\text{Sub}} = \frac{b_1}{P_0} + \frac{b_2}{B_0} + b_0 + \alpha$$

其中, $N_{\text{Sub}}$ 为所述内容分片数, $b_0$ 、 $b_1$ 和 $b_2$ 为所述二元线性回归模型的参数, $P_0$ 为所述目标数据内容的内容流行度, $B_0$ 为所述目标数据内容所在节点的节点介数, $\alpha$ 为根据所述目标数据内容的内容隐私等级确定的修正因子。

2. 根据权利要求1所述的方法,其特征在于,所述内容隐私等级包括:最高隐私保护级别、普通隐私保护级别和公开访问级别。

3. 根据权利要求1所述的方法,其特征在于,所述根据所述内容分片数,将所述目标数据内容进行分片存储,具体包括:

将所述目标数据内容分成若干个分片子包,分片子包的数量等于所述内容分片数;

选取一个节点作为中心节点,将分片子包存储到所述中心节点相邻一跳的节点上,每个相邻一跳的节点上存储一个分片子包;

若存在多余分片子包没有被存储到所述中心节点相邻一跳的节点上,则重新选取一个新的中心节点,将没被存储的分片子包存储到新的中心节点相邻一跳的节点上,直到所有的分片子包全部存储。

4. 根据权利要求1所述的方法,其特征在于,所述将所述目标数据内容分成若干个分片子包,具体包括:

将所述目标数据内容分成若干个分片子包;

为每个分片子包设置相应的分片号标志位和内容名字标志位,以供对分片数据进行重组时使用。

5. 根据权利要求1所述的方法,其特征在于,所述获取用户的数据请求信息,并对分片数据进行重组,将重组得到的所述目标数据内容的副本发送给用户终端,具体包括:

获取用户的数据请求信息,所述数据请求信息中包含请求获取的所述目标数据内容的名字;

根据所述目标数据内容的名字向相应节点发送分片子包获取请求,以供相应节点根据所述目标数据内容的名字和存储的分片子包中的内容名字标志位反馈所述目标数据内容的分片子包,其中,所述目标数据内容被分片存储时,被分成了若干个分片子包后存储到不同的节点中,每个分片子包设置相应的分片号标志位和内容名字标志位;

根据获取到的所述目标数据内容的分片子包中的分片号标志位,将各个分片子包重组所述目标数据内容的副本;

将所述目标数据内容的副本发送给用户终端。

6. 一种内容中心网络中用户行为隐私的保护装置,其特征在于,包括:

计算模块,用于根据目标数据内容的内容隐私等级和内容流行度,以及所述目标数据内容所在节点的节点介数,通过预设的二元线性回归模型确定内容分片数;

分片存储模块,用于根据所述内容分片数,将所述目标数据内容进行分片存储;

内容重组模块,用于获取用户的数据请求信息,并对分片数据进行重组,将重组得到的所述目标数据内容的副本发送给用户终端;

所述二元线性回归模型如下:

$$N_{\text{Sub}} = \frac{b_1}{P_0} + \frac{b_2}{B_0} + b_0 + \alpha$$

其中, $N_{\text{Sub}}$ 为所述内容分片数, $b_0$ 、 $b_1$ 和 $b_2$ 为所述二元线性回归模型的参数, $P_0$ 为所述目标数据内容的内容流行度, $B_0$ 为所述目标数据内容所在节点的节点介数, $\alpha$ 为根据所述目标数据内容的内容隐私等级确定的修正因子。

7.一种电子设备,其特征在于,包括:

存储器和处理器,所述处理器和所述存储器通过总线完成相互间的通信;所述存储器存储有可被所述处理器执行的程序指令,所述处理器调用所述程序指令能够执行如权利要求1至6任一所述的方法。

8.一种非暂态计算机可读存储介质,其上存储有计算机程序,其特征在于,当所述计算机程序被处理器执行时,实现如权利要求1至6任一所述的方法。

## 内容中心网络中用户行为隐私的保护方法及装置

### 技术领域

[0001] 本发明实施例涉及网络通信技术领域,尤其涉及一种内容中心网络中用户行为隐私的保护方法及装置。

### 背景技术

[0002] 随着互联网的快速发展以及用户数的不断增长,当下传统IP互联网所承担的数据流量分发压力越来越重,暴露出许多问题。这些问题使得传统IP互联网架构难以再继续支撑如此庞大的数据流量分发,不能有效地满足当前用户的通信需求。为了解决传统IP互联网中存在的诸多问题,人们正在不遗余力地研究更加适合当下现状的互联网体系架构,其中最具代表性的就是内容中心网络(Content-Centric Networking,CCN)。

[0003] CCN是以内容为中心、可实现网内缓存并具有高内容分发效率的通信网络架构,属于信息中心网络(Information Centric Network,ICN)的范畴,是当下最火热、最主要的未来网络体系架构之一。CCN在解决传统IP互联网问题以及在未来网络的发展中都发挥着至关重要的作用,其网内缓存、内容路由、数据签名等关键机制大大提升了内容分发的效率,但同时也增大了用户隐私的探测以及攻击的范围,严重威胁着用户的隐私安全。CCN存在许多隐私信息泄露问题,主要包括签名隐私泄露、名字隐私泄露、内容隐私泄露、缓存隐私泄露和行为隐私泄露等。行为隐私泄露属于缓存隐私泄露中的一种,攻击者可以通过时间攻击(即,攻击者连续发送兴趣包,获取该内容的响应时间,对比不同响应时间来推测该内容是否缓存在最近的路由节点上),获知邻居用户(与攻击者连接到同一路由节点的用户)对敏感内容的通信痕迹,从而窥探用户的行为隐私。

[0004] 针对因时间攻击而造成的用户行为隐私泄露问题,现有技术中通常采用基于最近访问以及随机回退机制的缓存隐私保护策略,该策略首先在兴趣包头部设置标记,标记上次访问的时间,进而对比识别当前请求的用户是否属于第一次请求;其次通过随机回退机制改变了隐私内容的缓存时间,增加时间不确定性。但对于最近访问机制,攻击者可通过多次请求目标内容,发现延迟现象,则可推测有其他用户在其请求之前也请求了该目标内容,进而获知邻居用户对敏感内容的通信痕迹,发生隐私泄露;对于随机回退机制,因随机回退时需要将内容从存入位置依次向后移动,变动过大,路由的计算难度过大。因此,如何有效地保护用户行为隐私依旧是当下研究CCN隐私保护的重点。

### 发明内容

[0005] 本发明实施例的目的是提供一种克服上述问题或者至少部分地解决上述问题的内容中心网络中用户行为隐私的保护方法及装置。

[0006] 为了解决上述技术问题,一方面,本发明实施例提供一种内容中心网络中用户行为隐私的保护方法,包括:

[0007] 根据目标数据内容的内容隐私等级和内容流行度,以及所述目标数据内容所在节点的节点介数,确定内容分片数;

- [0008] 根据所述内容分片数,将所述目标数据内容进行分片存储;
- [0009] 获取用户的数据请求信息,并对分片数据进行重组,将重组得到的所述目标数据内容的副本发送给用户终端。
- [0010] 另一方面,本发明实施例提供一种内容中心网络中用户行为隐私的保护装置,包括:
- [0011] 计算模块,用于根据目标数据内容的内容隐私等级和内容流行度,以及所述目标数据内容所在节点的节点介数,确定内容分片数;
- [0012] 分片存储模块,用于根据所述内容分片数,将所述目标数据内容进行分片存储;
- [0013] 内容重组模块,用于获取用户的数据请求信息,并对分片数据进行重组,将重组得到的所述目标数据内容的副本发送给用户终端。
- [0014] 再一方面,本发明实施例提供一种电子设备,包括:
- [0015] 存储器和处理器,所述处理器和所述存储器通过总线完成相互间的通信;所述存储器存储有可被所述处理器执行的程序指令,所述处理器调用所述程序指令能够执行上述的方法。
- [0016] 又一方面,本发明实施例提供一种非暂态计算机可读存储介质,其上存储有计算机程序,当所述计算机程序被处理器执行时,实现上述的方法。
- [0017] 本发明实施例提供的内容中心网络中用户行为隐私的保护方法及装置,对数据内容进行隐私等级划分,以及实行分片存储和重组,一方面减少非隐私内容对网络和路由器产生的负担,保证CCN分发效率的优势,另一方面通过分片存储和重组增加时间不确定性,抵抗时间攻击,阻止攻击者从往返时间上判断相邻用户的偏好,保护用户的行为隐私。

## 附图说明

- [0018] 图1为本发明实施例提供的内容中心网络中用户行为隐私的保护方法示意图;
- [0019] 图2为本发明实施例提供的分片存储算法的逻辑流程示意图;
- [0020] 图3为本发明实施例提供的分片组装算法的逻辑流程示意图;
- [0021] 图4为本发明实施例提供的内容中心网络中用户行为隐私的保护装置示意图;
- [0022] 图5为本发明实施例提供的电子设备的结构示意图。

## 具体实施方式

[0023] 为了使本发明实施例的目的、技术方案和优点更加清楚,下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例是本发明一部分实施例,而不是全部的实施例。基于本发明的实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例,都属于本发明保护的范围。

[0024] 图1为本发明实施例提供的内容中心网络中用户行为隐私的保护方法示意图,如图1所示,本发明实施例提供一种内容中心网络中用户行为隐私的保护方法,其执行主体为内容中心网络中用户行为隐私的保护装置,简称保护装置,所述方法包括:

- [0025] 步骤S101、根据目标数据内容的内容隐私等级和内容流行度,以及所述目标数据内容所在节点的节点介数,确定内容分片数;
- [0026] 步骤S102、根据所述内容分片数,将所述目标数据内容进行分片存储;

[0027] 步骤S103、获取用户的数据请求信息,并对分片数据进行重组,将重组得到的所述目标数据内容的副本发送给用户终端。

[0028] 具体来说,首先,对数据内容进行隐私等级划分,并根据目标数据内容的内容隐私等级和内容流行度,以及该目标数据内容所在节点的节点介数,利用多元线性回归理论求出内容分片数,其中,结合内容隐私等级对内容分片数进行修正,以确保得出最佳的内容分片数。

[0029] 然后,针对目标数据内容,根据计算得到的内容分片数,将该目标数据内容进行分片存储。

[0030] 当用户请求该目标数据内容时,对分片数据进行重组,将重组得到的所述目标数据内容的副本发送给用户终端。

[0031] 本发明实施例提供的内容中心网络中用户行为隐私的保护方法,对数据内容进行隐私等级划分,以及实行分片存储和重组,一方面减少非隐私内容对网络和路由器产生的负担,保证CCN分发效率的优势,另一方面通过分片存储和重组增加时间不确定性,抵抗时间攻击,阻止攻击者从往返时间上判断相邻用户的偏好,保护用户的行为隐私。

[0032] 在上述实施例的基础上,进一步地,所述内容隐私等级包括:最高隐私保护级别、普通隐私保护级别和公开访问级别。

[0033] 具体来说,为了减少非隐私数据内容对网络和路由器产生的负担,保障网络分发效率,本发明实施例从数据内容提供商和数据内容消费者两个方面将数据内容划分为公开访问级别、普通隐私保护级别和最高隐私保护级别。

[0034] 其具体划分方法如下:

[0035] 1) 数据内容提供商在发布数据内容时在数据内容的头部设置一个隐私级别标志位。将内容划分为三个级别{H,N,P},其中H表示最高隐私保护级别,即一些比较敏感,需要特别保护的隐私内容;N表示普通隐私保护级别,即用户不想共享的内容,需要有一定的保护;P表示公开访问级别,即用户愿意共享给他人的内容,如公开视频,各大公开网站的网页信息等等。

[0036] 2) 将用户进行等级划分,分为:普通用户,即请求的内容可以共享给他人,属于公开访问级别;VIP用户,请求的内容不愿共享给他人,属于普通隐私保护级别;SVIP用户,请求的内容属于敏感内容,属于最高隐私保护级别。在发出的兴趣包头部设置用户等级标志位来标记用户等级,则数据内容消费者发出兴趣包后,路由节点可以根据用户等级标志位,判断用户想请求的数据内容的隐私级别。

[0037] 为防止以上两个隐私标志位发生冲突,做出规定:如若发生隐私级别冲突,则以高隐私级别的为准。

[0038] 本发明实施例提供的内容中心网络中用户行为隐私的保护方法,对数据内容进行隐私等级划分,以及实行分片存储和重组,一方面减少非隐私内容对网络和路由器产生的负担,保证CCN分发效率的优势,另一方面通过分片存储和重组增加时间不确定性,抵抗时间攻击,阻止攻击者从往返时间上判断相邻用户的偏好,保护用户的行为隐私。

[0039] 在以上各实施例的基础上,进一步地,通过预设的二元线性回归模型确定所述内容分片数;

[0040] 所述二元线性回归模型如下:

$$[0041] \quad N_{\text{Sub}} = \frac{b_1}{P_0} + \frac{b_2}{B_0} + b_0 + \alpha$$

[0042] 其中,  $N_{\text{Sub}}$  为所述内容分片数,  $b_0$ 、 $b_1$  和  $b_2$  为所述二元线性回归模型的参数,  $P_0$  为所述目标数据内容的内容流行度,  $B_0$  为所述目标数据内容所在节点的节点介数,  $\alpha$  为根据所述目标数据内容的内容隐私等级确定的修正因子。

[0043] 具体来说, 为了确定合理的内容分片数, 本发明实施例从内容流行度、节点介数以及内容隐私等级三个方面考虑求解内容分片数。一方面根据内容流行度以及节点介数, 采用二元线性回归理论确定初步内容分片数; 另一方面要根据内容隐私等级确定内容分片数的修正因子。

[0044] 确定内容分片数的预设的二元线性回归模型如下:

$$[0045] \quad N_{\text{Sub}} = \frac{b_1}{P_0} + \frac{b_2}{B_0} + b_0 + \alpha$$

[0046] 其中,  $N_{\text{Sub}}$  为内容分片数,  $b_0$ 、 $b_1$  和  $b_2$  为二元线性回归模型的参数,  $P_0$  为目标数据内容的内容流行度, 即固定访问次数中该内容被访问的频率, 和  $N_{\text{Sub}}$  成反比,  $B_0$  为目标数据内容所在节点的节点介数, 即网络中经过该节点的最短路径数目占有所有最短路径总数的比值, 和  $N_{\text{Sub}}$  成反比,  $\alpha$  为根据目标数据内容的内容隐私等级确定的修正因子。

[0047] 本发明实施例提供的内容中心网络中用户行为隐私的保护方法, 对数据内容进行隐私等级划分, 以及实行分片存储和重组, 一方面减少非隐私内容对网络和路由器产生的负担, 保证CCN分发效率的优势, 另一方面通过分片存储和重组增加时间不确定性, 抵抗时间攻击, 阻止攻击者从往返时间上判断相邻用户的偏好, 保护用户的行为隐私。

[0048] 在以上各实施例的基础上, 进一步地, 所述根据所述内容分片数, 将所述目标数据内容进行分片存储, 具体包括:

[0049] 将所述目标数据内容分成若干个分片子包, 分片子包的数量等于所述内容分片数;

[0050] 选取一个节点作为中心节点, 将分片子包存储到所述中心节点相邻一跳的节点上, 每个相邻一跳的节点上存储一个分片子包;

[0051] 若存在多余分片子包没有被存储到所述中心节点相邻一跳的节点上, 则重新选取一个新的中心节点, 将没被存储的分片子包存储到新的中心节点相邻一跳的节点上, 直到所有的分片子包全部存储。

[0052] 具体来说, 图2为本发明实施例提供的分片存储算法的逻辑流程示意图, 如图2所示, 求出内容分片数后, 节点  $R_0$  (称  $R_0$  为管理节点) 开始根据数据内容分片数将目标数据内容进行分片, 分成若干个分片子包, 分片子包的数量等于所述内容分片数, 并在每个分片子包上设置两个特殊标志位: 分片号标志位 Fragment 以及内容名字标志位 CName。前者用于标记同一内容的不同分片子包; 后者用于标记不同内容, 存储该内容的内容名字, 防止进行分片组装时, 相同分片号会混淆。这两个标记为之后的分片组装做准备。

[0053] 假设在此CCN中, 采用ALWAYS普遍缓存策略, 在返回数据包路径上的所有节点均会缓存该目标数据内容。

[0054] 分片之后, 将各个分片子包按预设算法规则存储于  $R_0$  的周围节点上进行存储。分片存储算法如下:

[0055] 首先,需设定一个中心节点 $R_c$  (此时 $R_c=R_0$ ),再查询 $R_c$ 周围相邻一跳的节点上是否存在该目标数内容的完整副本或该目标数据内容的分片(通过查询内容名字标志位来判断)。如果在某节点上的查询结果为完整的目标数据内容的副本,则先将该节点上的目标数据内容副本进行删除,再将这个目标数据内容分片存储在该节点上,结束之后开始向另一条路径上的节点继续进行查询存储,而不再在同路径方向上进行查询。此时,该节点称为管理节点的隶属节点 $R_j$ ,并加入隶属节点集合;如果查询结果为该目标数据内容的分片,直接换其他路径方向进行节点查询,不再进行其他操作;如果两者都不存在,则直接将该目标数据内容分片在该节点上进行存储,同样加入隶属节点集合,称为隶属节点 $R_{j+1}$ ,同时由管理节点 $R_0$ 记录该节点号,存储于中心节点集合。

[0056] 其次,如果 $R_0$ 周围的相邻一跳的节点查询结束后,分片还没有存储完,则开始进行中心节点转换, $R_0$ 先从中心节点集合中随机选取任意一个节点作为下一个中心节点 $R_c'$ ,此时 $R_c'$ 将不再等于 $R_0$ (这个地方需要考虑中心节点集合是否是空,如果是空,从隶属节点集合中选取节点作为下一个中心节点 $R_c'$ ;如果此时没有任何隶属节点,则周围相邻一跳节点中无法存储分片,直接删除该管理节点上的内容,进行管理节点转换)。找到下一个中心节点 $R_c'$ 之后,重复上面查询步骤,直到完成内容分片存储,每个相邻一跳的节点上存储一个分片子包。

[0057] 最后存储结束后,目标数据内容在整个网络上会分散存储成多个小的分片区域网络,每个区域内相同数据内容的分片不会重复。每个分片区域网络会有一个管理节点和多个隶属节点,管理节点上存储着其他隶属节点的节点信息,其他各个隶属节点上也于存储着管理节点的信息。

[0058] 本发明实施例提供的内容中心网络中用户行为隐私的保护方法,对数据内容进行隐私等级划分,以及实行分片存储和重组,一方面减少非隐私内容对网络和路由器产生的负担,保证CCN分发效率的优势,另一方面通过分片存储和重组增加时间不确定性,抵抗时间攻击,阻止攻击者从往返时间上判断相邻用户的偏好,保护用户的行为隐私。

[0059] 在以上各实施例的基础上,进一步地,所述将所述目标数据内容分成若干个分片子包,具体包括:

[0060] 将所述目标数据内容分成若干个分片子包;

[0061] 为每个分片子包设置相应的分片号标志位和内容名字标志位,以供对分片数据进行重组时使用。

[0062] 具体来说,求出内容分片数后,节点 $R_0$ (称 $R_0$ 为管理节点)开始根据数据内容分片数将目标数据内容进行分片,并在每个分片子包上设置两个特殊标志位:分片号标志位Fragment以及内容名字标志位CName。前者用于标记同一内容的不同分片子包;后者用于标记不同内容,存储该内容的内容名字,防止进行分片组装时,相同分片号会混淆。这两个标记为之后的分片组装做准备。

[0063] 本发明实施例提供的内容中心网络中用户行为隐私的保护方法,对数据内容进行隐私等级划分,以及实行分片存储和重组,一方面减少非隐私内容对网络和路由器产生的负担,保证CCN分发效率的优势,另一方面通过分片存储和重组增加时间不确定性,抵抗时间攻击,阻止攻击者从往返时间上判断相邻用户的偏好,保护用户的行为隐私。

[0064] 在以上各实施例的基础上,进一步地,所述获取用户的数据请求信息,并对分片数



据进行重组,将重组得到的所述目标数据内容的副本发送给用户终端,具体包括:

[0065] 获取用户的数据请求信息,所述数据请求信息中包含请求获取的所述目标数据内容的名字;

[0066] 根据所述目标数据内容的名字向相应节点发送分片子包获取请求,以供相应节点根据所述目标数据内容的名字和存储的分片子包中的内容名字标志位反馈所述目标数据内容的分片子包,其中,所述目标数据内容被分片存储时,被分成了若干个分片子包后存储到不同的节点中,每个分片子包设置相应的分片号标志位和内容名字标志位;

[0067] 根据获取到的所述目标数据内容的分片子包中的分片号标志位,将各个分片子包重组成为所述目标数据内容的副本;

[0068] 将所述目标数据内容的副本发送给用户终端。

[0069] 具体来说,图3为本发明实施例提供的分片组装算法的逻辑流程示意图,如图3所示,当用户发出内容请求时,该数据请求信息中包含请求获取的目标数据内容的名字,离该用户最近的节点 $R_u$ 查看自己是否属于管理节点,如果不是,则按CCN转发规则转发给下一个节点继续查询,看其周围一跳节点中是否有管理节点,依旧没有,查看相隔二跳的节点,直到查询到目标内容最近的管理节点为止。并将兴趣包转发给该管理节点。管理节点 $R_0$ 收到用户请求后,首先根据CName标志位查询到对应的隶属节点集合,并从隶属节点集合中随机安排一个节点进行分片组装,此处定义进行组装的节点为 $R_i$  ( $i=1,2,\dots,N_c$ )。

[0070]  $R_i$ 向管理节点 $R_0$ 请求相应的隶属节点信息, $R_0$ 返回给 $R_i$ ,同时将自己存储的目标数据内容分片传送给 $R_i$ , $R_i$ 再向其余各个节点发送分片子包获取请求,请求包中包含组装目标数据内容的名字和 $R_i$ 的位置信息,请求它们将该目标数据内容分片通过最短路径发送给 $R_i$ 。收到请求包的隶属节点 $R_j$ 则开始查询内容名字标志位CName找到对应的目标数据内容分片,再根据 $R_i$ 节点的位置经过最短路径传送给 $R_i$ 。 $R_i$ 收到各个节点发送的目标数据内容分片后,就会根据分片号标志位Fragment将内容组装起来。组装完成之后, $R_i$ 直接将完整的目标数据内容副本返回离用户最近的节点 $R_u$ , $R_u$ 再返回给用户终端。

[0071] 同时 $R_i$ 将组装完成的目标数据内容副本随机发送给其相邻一跳且没有内容分片的节点,再由节点进行新一轮的内容分片,这样可以增大内容在网络上的缓存概率,减少用户请求时延,提高内容分发效率。如果其相邻一跳的节点都已经存在内容分片,则直接删除这个组装完成的内容副本。

[0072] 本发明实施例提供的内容中心网络中用户行为隐私的保护方法,对数据内容进行隐私等级划分,以及实行分片存储和重组,一方面减少非隐私内容对网络和路由器产生的负担,保证CCN分发效率的优势,另一方面通过分片存储和重组增加时间不确定性,抵抗时间攻击,阻止攻击者从往返时间上判断相邻用户的偏好,保护用户的行为隐私。

[0073] 图4为本发明实施例提供的内容中心网络中用户行为隐私的保护装置示意图,如图4所示,本发明实施例提供一种内容中心网络中用户行为隐私的保护装置,用于执行上述任一实施例中所述的方法,具体包括计算模块401、分片存储模块402和内容重组模块403,其中:

[0074] 计算模块401用于根据目标数据内容的内容隐私等级和内容流行度,以及所述目标数据内容所在节点的节点介数,确定内容分片数;分片存储模块402用于根据所述内容分片数,将所述目标数据内容进行分片存储;内容重组模块403用于获取用户的数据请求信

息,并对分片数据进行重组,将重组得到的所述目标数据内容的副本发送给用户终端。

[0075] 具体来说,首先,对数据内容进行隐私等级划分,并通过计算模块401根据目标数据内容的内容隐私等级和内容流行度,以及该目标数据内容所在节点的节点介数,利用多元线性回归理论求出内容分片数,其中,结合内容隐私等级对内容分片数进行修正,以确保得出最佳的内容分片数。

[0076] 然后,针对目标数据内容,通过分片存储模块402根据计算得到的内容分片数,将该目标数据内容进行分片存储。

[0077] 当用户请求该目标数据内容时,通过内容重组模块403对分片数据进行重组,将重组得到的所述目标数据内容的副本发送给用户终端。

[0078] 本发明实施例提供一种内容中心网络中用户行为隐私的保护装置,用于执行上述任一实施例中所述的方法,通过本实施例提供的装置执行上述某一实施例中所述的方法的具体步骤与上述相应实施例相同,此处不再赘述。

[0079] 本发明实施例提供的内容中心网络中用户行为隐私的保护装置,对数据内容进行隐私等级划分,以及实行分片存储和重组,一方面减少非隐私内容对网络和路由器产生的负担,保证CCN分发效率的优势,另一方面通过分片存储和重组增加时间不确定性,抵抗时间攻击,阻止攻击者从往返时间上判断相邻用户的偏好,保护用户的行为隐私。

[0080] 图5为本发明实施例提供的电子设备的结构示意图,如图5所示,所述设备包括:处理器501、存储器502和总线503;

[0081] 其中,处理器501和存储器502通过所述总线503完成相互间的通信;

[0082] 处理器501用于调用存储器502中的程序指令,以执行上述各方法实施例所提供的方法,例如包括:

[0083] 根据目标数据内容的内容隐私等级和内容流行度,以及所述目标数据内容所在节点的节点介数,确定内容分片数;

[0084] 根据所述内容分片数,将所述目标数据内容进行分片存储;

[0085] 获取用户的数据请求信息,并对分片数据进行重组,将重组得到的所述目标数据内容的副本发送给用户终端。

[0086] 本发明实施例提供一种计算机程序产品,所述计算机程序产品包括存储在非暂态计算机可读存储介质上的计算机程序,所述计算机程序包括程序指令,当所述程序指令被计算机执行时,计算机能够执行上述各方法实施例所提供的方法,例如包括:

[0087] 根据目标数据内容的内容隐私等级和内容流行度,以及所述目标数据内容所在节点的节点介数,确定内容分片数;

[0088] 根据所述内容分片数,将所述目标数据内容进行分片存储;

[0089] 获取用户的数据请求信息,并对分片数据进行重组,将重组得到的所述目标数据内容的副本发送给用户终端。

[0090] 本发明实施例提供一种非暂态计算机可读存储介质,所述非暂态计算机可读存储介质存储计算机指令,所述计算机指令使所述计算机执行上述各方法实施例所提供的方法,例如包括:

[0091] 根据目标数据内容的内容隐私等级和内容流行度,以及所述目标数据内容所在节点的节点介数,确定内容分片数;

[0092] 根据所述内容分片数,将所述目标数据内容进行分片存储;

[0093] 获取用户的数据请求信息,并对分片数据进行重组,将重组得到的所述目标数据内容的副本发送给用户终端。

[0094] 本领域普通技术人员可以理解:实现上述方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成,前述的程序可以存储于一计算机可读取存储介质中,该程序在执行时,执行包括上述方法实施例的步骤;而前述的存储介质包括:ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

[0095] 以上所描述的装置及设备实施例仅仅是示意性的,其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的,作为单元显示的部件可以是或者也可以不是物理单元,即可以位于一个地方,或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。本领域普通技术人员在不付出创造性的劳动的情况下,即可以理解并实施。

[0096] 通过以上的实施方式的描述,本领域的技术人员可以清楚地了解到各实施方式可借助软件加必需的通用硬件平台的方式来实现,当然也可以通过硬件。基于这样的理解,上述技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来,该计算机软件产品可以存储在计算机可读存储介质中,如ROM/RAM、磁碟、光盘等,包括若干指令用以使得一台计算机设备(可以是个人计算机,服务器,或者网络设备等)执行各个实施例或者实施例的某些部分所述的方法。

[0097] 最后应说明的是:以上实施例仅用以说明本发明的技术方案,而非对其限制;尽管参照前述实施例对本发明进行了详细的说明,本领域的普通技术人员应当理解:其依然可以对前述各实施例所记载的技术方案进行修改,或者对其中部分技术特征进行等同替换;而这些修改或者替换,并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。

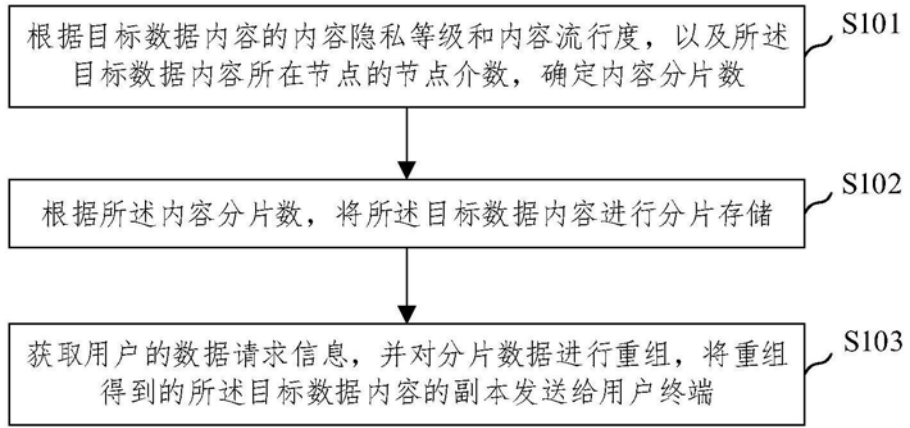


图1

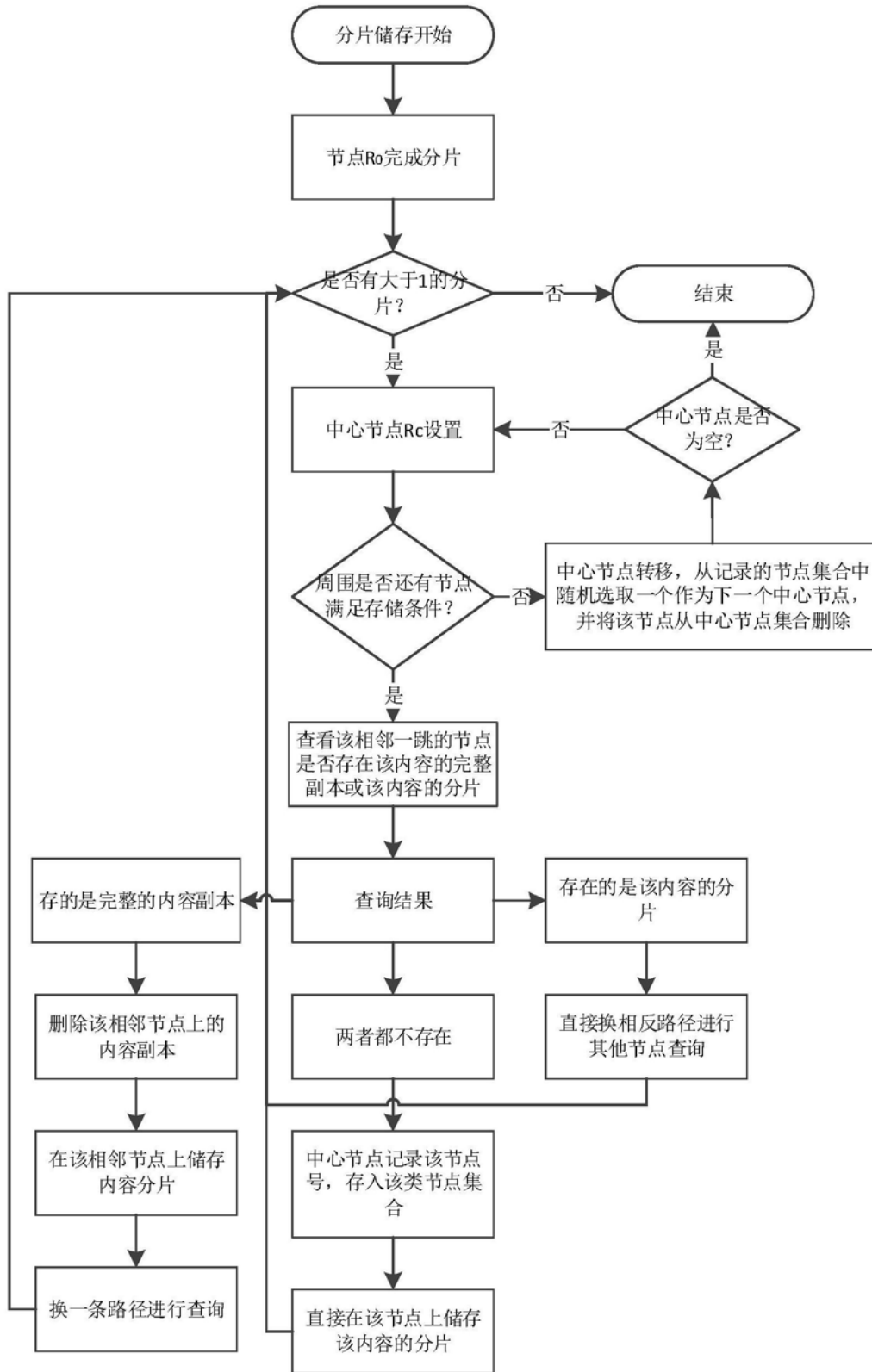


图2

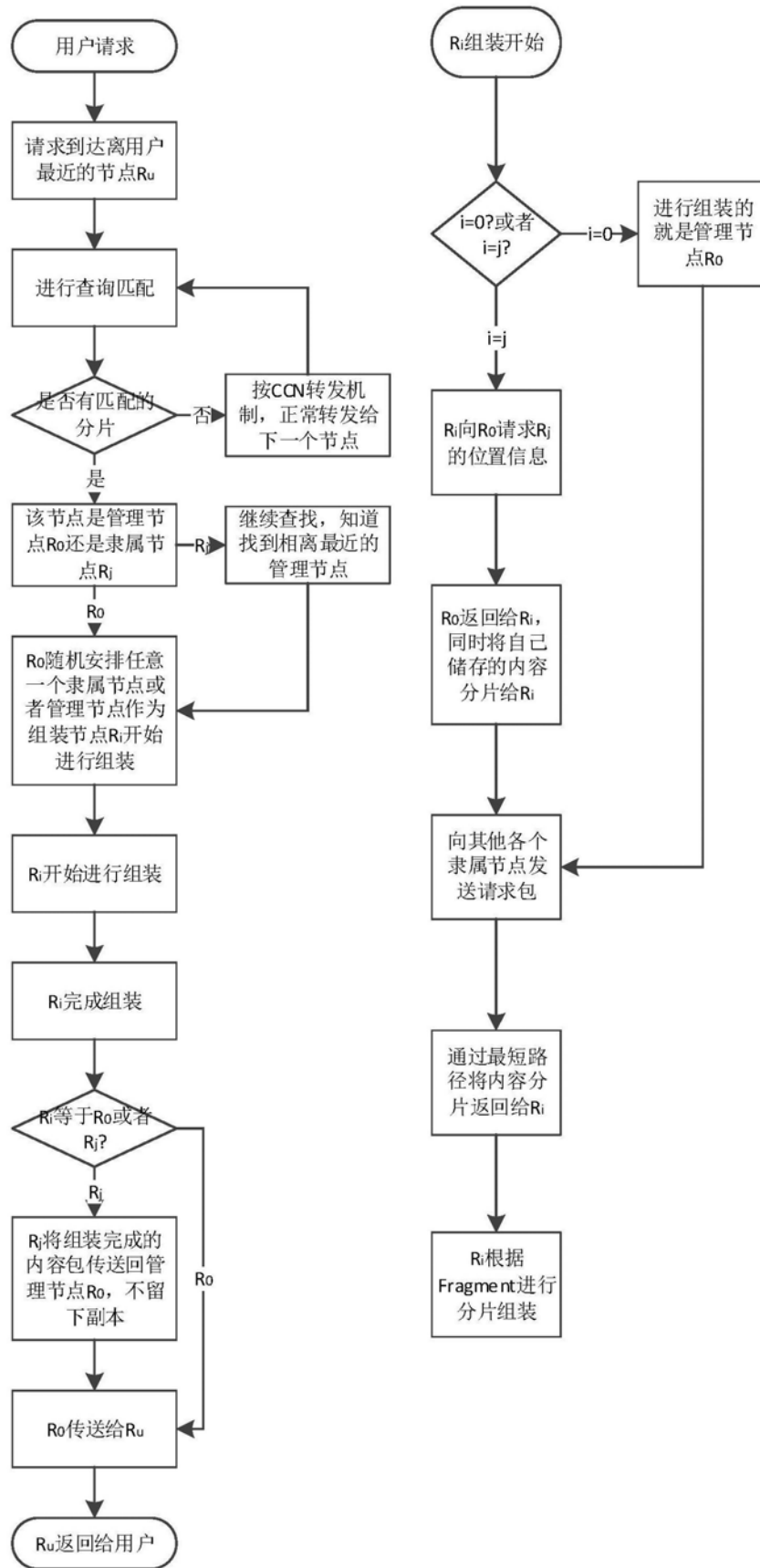


图3



图4

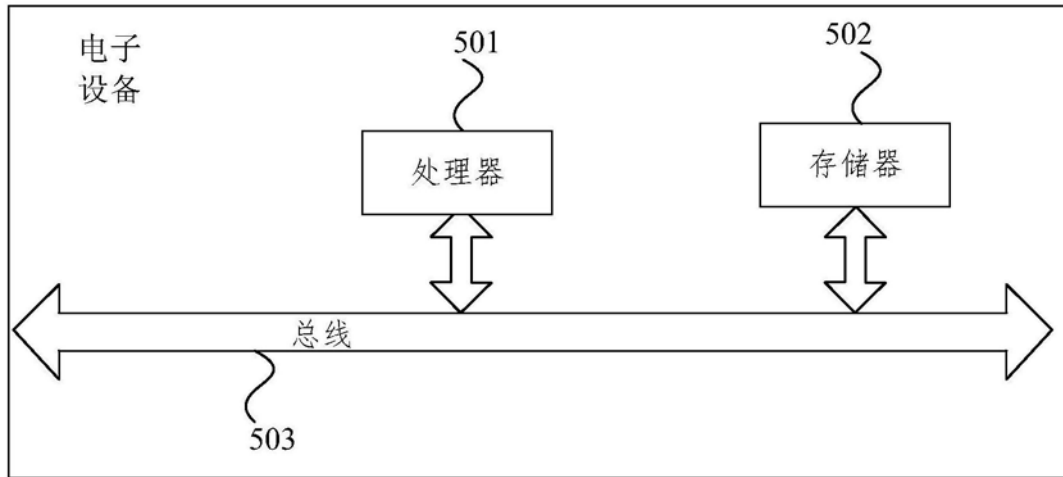


图5