文章编号:1671-4598(2019)09-0235-05 DOI:10.16526/j.cnki.11—4762/tp.2019.09.050 中图分类号:TP393.0 文献标识码:A

命名数据网络中基于用户位置分组的广播加密访问控制方案

张 倩[1], 王新平[2]
(1. 扬州大学广陵学院, 江苏 扬州 225000;
2. 江苏大学 计算机科学与通信工程学院, 江苏 镇江 212013)

摘要: 广播加密是命名数据网络中实现内容访问控制的一类重要方法, 利用广播加密, 可实现群组内内容的共享, 但是现有随机分组策略导致缓存内容副本冗余增加, 严重制约了网络性能; 鉴于此, 提出了基于用户位置分组的广播加密访问控制方案, 通过修改兴趣包结构, 加入 TraceRouteTag 字段确定用户在网络中的相对位置, 将同一区域内的用户尽可能分到同一组, 并针对不同的组进行基于广播加密的访问控制, 提高了缓存利用率; ndnSIM 仿真结果表明, 相较于随机分组, 基于用户拓扑位置分组的广播加密方案, 提高了缓存利用率, 降低了内容获取的时间开销。

关键词: 命名数据网络; 接入控制; 广播加密; 基于位置分组; 缓存利用率

User Location Based Broadcast Encryption—Access Control in NDN

Zhang Qian[1], Wang Xinping[2]
(1. Guangling College of Yangzhou University, Yangzhou 225012, China;
2. School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang 212013, China)

Abstract: Broadcast encryption is an important method to implement content access control in Named Data Networking. Through Broadcast encryption, content can be safely shared within network. However, existing Random Grouping Strategy result in increased redundancy of content replicas in the network. which seriously restricts network performance. In view of this, a User Location Grouping based Broadcast Encryption Access Control in NDN (ULBBE—AC) is proposed in this paper. By modifying the interest packet structure, a TraceRouteTag field is added to the interest packet, which is used to determine the user's relative position in the network topology. In ULBBE—AC, the users in the same area will be divided into the same group as much as possible and broadcast encryption—based access control is performed for different groups, which improves cache utilization. The simulation results of ndnSIM show that compared with Radom Group Broadcast Encryption—Access Control, ULBBE—AC improves cache utilization and reduces the time cost of content acquisition.

Keywords: named data networking; access control; broadcast encryption; grouping location; cache utilization

0 引言

命名数据网络[1-2] (named data networking, NDN) 是下一代互联网体系架构的典型代表, 通过分布式缓存与命名路由机制, NDN 实现了网络内容的快速分发。但缓存机制在改善网络性能的同时, 也带来了新的网络问题。由于 NDN 路由器无法验证请求者的身份, 任意用户都可以请求缓存内容, 导致内容隐私存在潜在的泄露风险, 而如何实施内容访问控制, 保证内容提供者发布的内容仅对授权用户有效, 成为当前 NDN 领域一类重要的研究问题。

针对内容访问控制[3], 主流解决方案是对内容进行端到端加密, 实现内容的隐私保护[4-5]。如果为每个用户以其特有的公钥进行加密, 将导致同一内容出现多个不同的内容副本, 严重破坏了缓存利用率。为了充分利用网内缓存, 并让内容提供者直接控制内容的访问权限, 广播加密[6-7]成为 NDN 访问控制中一种较优的可选方案。在广播加密访问控制中, 内容提供者针对目标用户群加密内容, 群组内的用户可以共享加密内容, 只需使用接收到的启用块 (enable block) 与自己的私钥就可以解密内容。在文献 [8] 中, 作者提出了一种基于 (n,t)—Shamir 秘密共享算法所设计的广播加密访问控制方案。该方案中, 内容提供者使用对称密钥加密内容, 为了实现访问控制, 内容提供者将内容密钥分割成 $(n+t)$ 份, 并将其中的 n 份分发给 n 个授权用户作为用户端的解密凭证, 其余 t 份内容密钥置入内容提供者生成的启用块中。进而, 内容提供者通过广播方式发布加密内容与启用块。授权用户使用包含在启用块中的密钥信息和自己持有的解密凭证, 利用多项式插值计算的方法提取内容密钥, 完成内容解密。非授权用户由于没有解密凭证, 因此即使收到了加密内容和启用块, 也无法从中提取内容密钥, 也就无法解密内容。该方案中用户访问权限由内容提供者授权, 不需要第三方干预, 但随着广播组内用户规模增大, 包含密钥信息的启用块的大小相应增大,

收稿日期:2019-03-22; **修回日期**:2019-04-09。
基金项目:扬州大学广陵学院自然科学研究项目(ZKYB18003)。
作者简介:张 倩(1985-),女,硕士研究生,工程师,主要从事未来网络理论与技术方向的研究。

用户从启用块中提取密钥的时间开销呈线性增长，网络传输与存储的开销也相应增大。因此，单纯通过广播加密进行内容的访问控制虽然可靠性较高，但牺牲了网络的有效性。

对广播群体进行用户分组，是有效减少启用块开销，改善网络性能的好方法，但如果采用基于随机分组的广播加密访问控制方案 radom group broadcast encryption－access control（RGBE－AC），容易造成 NDN 中出现严重的内容副本冗余，极大降低了 NDN 网络中缓存利用率。针对上述问题，本文提出了一种基于用户位置分组的广播加密访问控制方案 user location based broadcast encryption－access control（ULBBE－AC），该方案通过在 NDN 兴趣包中引入 TraceRouteTag 标签，让内容提供者能够直接确定用户在网络中的相对位置，进而建立用户位置树对用户进行位置分组，通过用户分组有效控制了启用块的计算和传输开销。ndnSIM 仿真结果表明：相比于 RGBE－AC，ULBBE－AC 降低了网内缓存中针对不同分组加密内容副本的冗余，提升了缓存利用率。

1 ULBBE－AC 方案设计

1.1 NDN 基础

NDN 的运行架构与 IP 网络完全不同，命名路由与网内缓存机制是 NDN 的核心特征。NDN 中有两类包，一种称为兴趣包，一种称为数据包，NDN 用户通过发送兴趣包、获取数据包，完成通信过程。由于兴趣包寻址仅仅依赖其中包含的内容名称，不采用 IP 寻址方式，因而构成了与现有 IP 架构完全不同的通信模式。典型的 NDN 路由器包含一个大容量缓存（content store，CS）、一个待定请求判决表（pending interest table，PIT）以及一个前向转发表（forwarding information base，FIB）。这里，CS 用于存储经过该路由器的内容文件，PIT 用于记录该路由器转发出去的兴趣包名称及到达接口（防止相同名称请求多次重发并为接收数据包提供回传路径信息），FIB 是一个路由表，为接收兴趣包提供转发路径信息。

当 NDN 路由器收到用户发送的兴趣包请求后，首先按照名称的最大前缀匹配原则在路由器的 CS 中查找该内容，如果匹配成功，路由器或内容提供者将会为用户返回携带所请求内容的数据包；如果路由器在自身的 CS 匹配不成功，会进一步在 PIT 表中查询该内容名，如果在 PIT 中可以找到，说明之前路由器已经转发了相同的内容请求，为了避免重复流量流入网络，路由器就不再转发该兴趣包，仅仅在 PIT 中记录该兴趣包的到达接口，用于接收到数据后正确回传；如果在 PIT 中未匹配到相同条目，说明之前没有相同的内容请求被转发出去，进一步根据兴趣包携带的内容名在 FIB 表中查找路由信息（名称对应的转发接口），然后根据 FIB 指示信息将兴趣包转发出去。

转发出去的兴趣包在网内路由器处逐一查找，如果未命中将被转发至内容提供者处。最终获取到的数据包将按照兴趣包被转发的反向路径返回，并在返回过程中被路径上的路由器进行缓存，这一缓存操作可以方便其他用户就近获取该内容，有效减小了其他用户的请求时延。而且，当同一区域内的用户都请求某些热点内容时，这种网络优势更加明显。

但是缓存机制在改善网络性能的同时，也对如何有效利用缓存提出了严格要求。就基于广播加密的访问控制而言，传统广播加密访问控制倾向于关注用户密钥的获取、广播头（启用块）和加密内容的分发、以及用户如何解密内容，但在 NDN 网络中使用广播加密，用户分组问题不容忽视。不难发现，即使用户为同一广播组成员，且邻近路由器处存在加密的内容（针对其他广播组加密），但是由于在网络拓扑中所处位置的差异，用户也只能到靠近内容提供者的路由器处或提供者处获取加密内容及启用块，这种由于广播用户分组的不合理导致 NDN 缓存带来的优势被严重破坏。而本文针对这一问题，通过修改兴趣包结构，让其携带能确定用户网络位置的标识 TraceRoutetag，便于内容提供者根据该标识对用户进行基于网络位置的广播组划分，使得同一广播组内的用户尽可能处于同一个区域内，从而达到提高网内副本利用率的目的。下面将对本文方案的实现过程进行详细阐述：

1.2 方案描述

1.2.1 修改兴趣包获取用户拓扑位置

传统广播加密采用随机分组策略，如图 1 所示，来自不同广播分组的用户请求相同兴趣，导致边缘路由器的缓存内存有不同广播分组的加密内容，加密内容只有各自广播组内用户才可解密获取，这极大的降低了广播加密内容的利用率。若根据用户拓扑位置，将属于临近地理区域的用户分为一组，如图 2 所示，则路由器缓存内只包含该区域内广播组用户请求内容，这极大的降低了副本的冗余，有效提高了广播加密内容的利用率，改善了 NDN 的缓存效率。

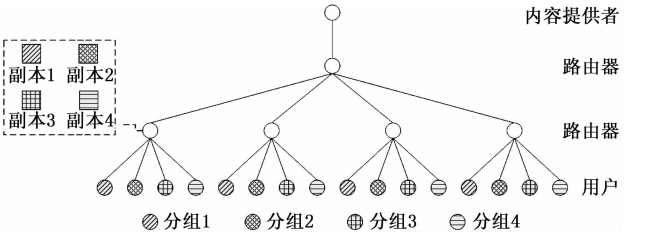

图 1 随机分组模型

图 2 基于用户位置的分组模型设每个路由器的接口编号都从 1 开始，用户发出的兴趣包的 TraceRouteTag 随着转发的变化如图 4 所示。初始兴趣包中 TraceRoutetag 的值为空，每经过一个路由器，便在兴趣包的 TraceRoutetag 条目中存入该路由器的编号和接口编号。经过路由器的转发到达内容提供者时，TraceRoutetag 的内容为｛Router1，face2；Router2，face1；…；Router5，face1｝。内容提供者

根据收到兴趣包的 TraceRouteTag 数据进行逆序，得到一条从内容提供者到用户的传输路径，从而定位用户拓扑位置，并将临近拓扑位置的用户分到同一广播分组内，在组内实施广播加密。

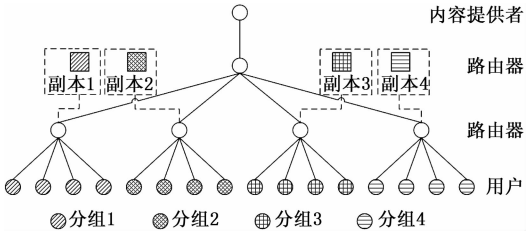

图 2　基于用户位置的分组模型

1.2.2　广播加密分发文件

基于修改兴趣包实现用户拓扑位置发现功能，内容提供者可以将临近位置的用户分到同一广播分组内，并在组内实施广播加密，达成接入控制效果。ULBBE－AC 中，具体广播加密过程如下：

假设 G 和 G_1 是两个阶为素数 p 的乘法循环群，g 为 G 的生成元；$\alpha \in Z_p$；$e: G \times G \to G_1$ 为一个双线性映射。内容提供者为其下所有广播组接受者 $i = 1,2,\cdots,n,n+2,\cdots,2n$ 计算 $g_i = g^{(\alpha^i)} \in G$，并随机选择 $\gamma \in Z_p$，计算 $v = g^{\gamma} \in G$，获得广播加密系统公钥为 $PK = (g, g_1, \cdots, g_n, g_{n+2}, \cdots, g_{2n}, v) \in G^{2n+1}$。

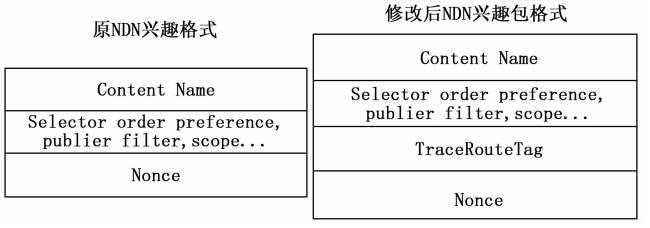

图 3　修改后兴趣包

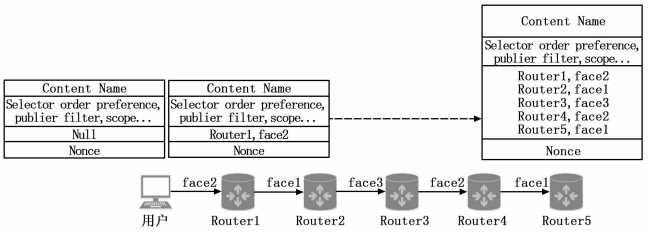

图 4　TracerRouteTag

内容提供者非对称加密的公钥私钥对为 (P_C, Pr_C)，用户的非对称加密的公钥私钥对为 (P_i, Pr_i)，身份信息为 id_i。

Step 1：初始化阶段，当用户 i 向内容提供者进行注册时，发送一个注册兴趣包/xyz.com/subscribe/id_i 向内容提供者进行订阅。该兴趣包中携带着用户 i 的身份信息 id_i，并由内容提供者的公钥 P_C 加密来保证安全性。内容提供者收到注册兴趣包后，使用自己的私钥 Pr_C 解密获取用户 i 的身份信息 id_i。提供者根据用户 i 的身份 id_i 将用户 i 加入广播子组 $S = \{1,2,\cdots n\}$，并为用户生成广播加密的用户私钥 $SK_i = g_i^{\gamma} \in G$（即 $SK_i = v^{(\alpha^i)}$），并将该私钥 SK_i 和分组信息使用 i 的公钥 $\{ \backslash \mathrm{mathop} \{ \backslash \mathrm{rm\ P} \} \backslash \mathrm{nolimits} \}_i$ 加密，返回给 i。

Step 2：i 完成注册后获得了用户私钥 SK_i，而且获知了自己所在的用户组 S，此时，i 向内容提供者发送一个名为的兴趣包/xyz.com/S/abc 请求感兴趣的内容。内容提供者收到兴趣包后，随机选择 $t \in Z_p$，计算 $K = e(g_{n+1}, g)^t \in G$ 以及 $Hdr = (g^t, (v \cdot \prod_{i \in S} g_{n+1-j})^t) \in G^2$ 得到广播加密会话密钥 K 以及广播头（启用块）Hdr。并使用生成的会话密钥 K 对内容 M 进行对称加密得到加密内容 C_M，即 $C_M = SymEnc(K, M)$。随后，提供者将加密的内容 C_M 发送给用户 i。

Step 3：i 收到加密的内容 C_M 后，进一步向内容提供者请求解密所需的广播头（启用块）Hdr。收到广播头（启用块）后，i 就可以结合启用块 Hdr 和广播加密私钥 SK_i 通过计算：$K = \dfrac{e(g_i, (v \cdot \prod_{i \in S} g_{n+1-j})^t)}{e(SK_i \cdot \prod_{\substack{j \in S \\ j \neq i}} g_{n+1-j+i}, g^t)}$ 获得内容密钥 K，从而通过计算 $M = SymDec(C_M, K)$ 获得内容 M。

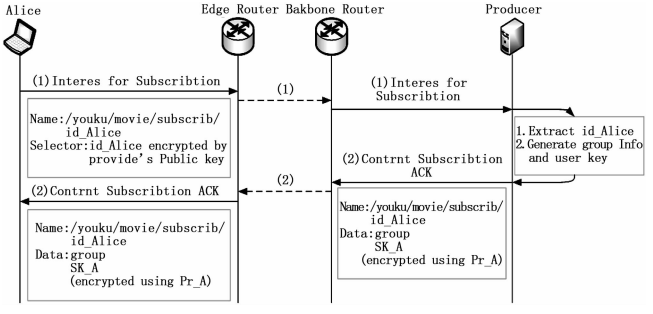

图 5　用户注册

2　ULBBE－AC 访问控制实例

为了进一步说明 ULBBE－AC 策略下的访问控制实施过程，本文以用户请求优酷网站下某个视频内容为例，详细说明 ULBBE－AC 方案的实施流程。在以下示例中，假设内容提供者非对称加密的公钥私钥对为 (P_C, Pr_C)，用户 Alice 与 Bob 在同一广播分组内，其非对称加密的公钥私钥对分别为 (P_A, Pr_A)、(P_B, Pr_B)，Alice 与 Bob 身份信息分别为 id_A、id_B，内容提供者为 Alice 与 Bob 生成的广播加密用户私钥为 $SK_A = g_A^{\gamma}$、$SK_B = g_B^{\gamma}$，内容提供者加密内容的对称内容密钥为 K。而且由于视频内容比较大，用户必须分块请求内容，包含解密密钥信息的启用块作为内容的一部分，在内容请求过程中，会作为一个单独的内容块分发给用户：

新用户注册：用户 Alice 想要请求根节点/youku/movie 下的某个视频内容，她首先发送一个名为/youku/movie/

subscribe/id_{Alice}的兴趣包向内容提供者进行注册。该注册兴趣包中携带着用户 Alice 的身份信息 id_A，并由内容提供的公钥 P_C 进行加密来保证用户身份信息的安全。内容提供者收到用户的注册兴趣包后，使用自己的私钥 Pr_C 解密获取到用户 Alice 的身份信息 id_A，同时根据订阅兴趣包中携带的 TraceRouteTag 确定用户在网络拓扑中的相对位置，并决定用户的分组信息，确定将用户加入 group1 广播组。随后，内容提供者根据用户 Alice 的身份 id_A，通过计算 $SK_A = g_A^{\gamma}$ 为 Alice 生成广播加密的用户私钥 SK_A，并将该私钥 SK_A 和分组信息使用 Alice 的公钥 Pr_A 加密，返回给 Alice。用户 Bob 注册过程与 Alice 相同，并假设用户 Bob 与 Alice 在同一广播分组内。

3 数据请求

Alice 完成注册后获得了用户私钥 SK_A，而且获知了自己被加入了 group1 广播组，此时，Alice 向内容提供者发送一个名为/youku/group1/zhanlang. mp4 的兴趣包，请求感兴趣的电影内容。内容提供者收到该兴趣包后，根据兴趣包名称中的分组信息，生成用户所在 group1 广播组的内容密钥 K 和启动块 Hdr。即提供者随机选择 $t \in Z_p$，计算 $K = e(g_{n+1}, g)^t \in G$ 以及 $Hdr = (g^t, (v \cdot \prod_{i \in S} g_{n+1-j})^t) \in G^2$ 得到广播加密会话密钥 K 以及广播头（启用块）Hdr。并使用生成的会话密钥 K 对内容 M 进行对称加密得到加密内容 C_M，即 $C_M = SymEnc(K, M)$。随后，提供者将加密的内容 C_M 和包含密钥信息的启用块 Hdr 发送给用户 Alice。由于 Alice 发送的内容请求兴趣包的名称中包含了 Alice 的分组信息，因此，按照名称精确匹配的原则，Alice 不会请求到其他用户组的加密内容。Alice 收到加密的内容后，进一步向内容提供者请求解密所需的启用块。收到启用块后，Alice 就可以结合启用块中的信息和广播加密私钥 SK_A，通过计算 $K = \dfrac{e(g_A, (v \cdot \prod_{A \in S} g_{n+1-j})^t)}{e(SK_A \cdot \prod_{\substack{j \in S \\ j \neq A}} g_{n+1-j+A}, g^t)}$ 获得内容密钥 K，从而通过计算 $M = SymDec(C_M, K)$ 获得内容 M。

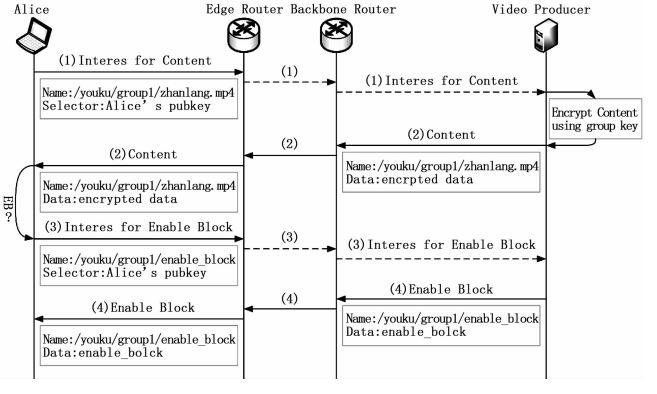

图 6 数据请求（Alice）

Bob 完成注册后，同样向内容提供者发送一个名为/youku/group1/zhanlang. mp4 的兴趣包请求，由于同广播分组的 Alice 此前请求过该数据，所以 Bob 的请求（兴趣包与启动块）可在临近边缘节点处得到满足。Bob 收到启动块 Hdr 和加密的内容 C_M 后，结合自己的私钥 $SK_B = g_B^{\gamma}$ 和启动块 Hdr 中的密钥信息，通过计算 $K = \dfrac{e(g_B, (v \cdot \prod_{B \in S} g_{n+1-j})^t)}{e(SK_B \cdot \prod_{\substack{j \in S \\ j \neq B}} g_{n+1-j+B}, g^t)}$，获得内容密钥 K，进而解密获取内容。

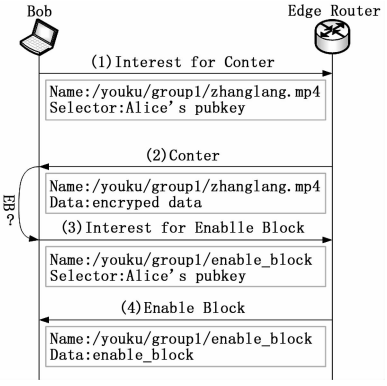

图 7 数据请求（Bob）

4 仿真分析

本节通过搭建 ns－3 仿真环境，利用 ndnSIM V2. 3 仿真工具，对基于位置分组和随机分组两种策略从缓存利用率角度进行性能仿真，并从分类命中率和内容访问时延的两个方面对方案进行对比分析。其中 ndnSIM V2. 3 所运行的高性能计算平台具有 10 核 CPU，其型号为 Intel（R）Xeon（R）E7－4830，CPU 单核的主频是 2. 20 GHz，计算平台内存为 256 GB，采用 CentOS 6. 5 操作系统。

参考文献［10－11］的分析条件设置，设内容提供者可提供的内容文件包括 50 类（分类规则根据内容请求的热度，即流行度），且设定内容请求的热度从第 1 类到第 50 类依次降低，每一类内容包含 1 000 个大小为 50 MB 的内容文件，每个内容在网内传输与存储时被分割成大小为 1 M 的内容块。路由器节点的 CS 大小设为 200 GB，使用最近最少缓存置换策略，各路由器之间使用带宽为 100 Mbps 的链路连接，并设链路传输时延为 10 ms。进而，设用户发出兴趣包所请求的内容类别服从参数 $\alpha_N = 1.2$ 的 Zipf 分布，边缘路由器每个接口接收到兴趣的到达概率服从参数为 10 内容块/秒的泊松分布。仿真所用拓扑如图 8 所示，16 个用户被平均分为 4 个组，图 8（A）为随机分组（RGBE－AC）场景，此时每个边缘路由器下有四个处于不同分组的用户；图 8（B）为基于拓扑位置分组（ULBBE－AC）场景，现将处于同一路由器下的四个用户分入相同组。

用户请求内容时，按照“/｛prefix｝/group｛x｝/｛content _ class｝/｛content name｝”的原则构造兴趣包名

称。其中，兴趣包名称中的/group｛x｝/组件直接体现出用户所在的广播加密分组信息。

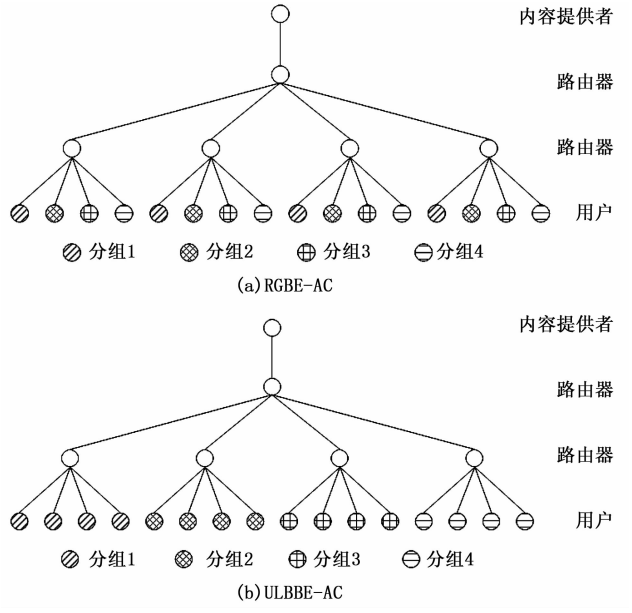

图 8　两种分组方案

4.1　内容命中率

网内命中率是用来评估用户的请求在网内的命中情况（如果内容从内容提供者处获取，则为网内非命中情况），它可以直接反映出网内缓存副本的利用率，显然，网内命中率越高则说明网内缓存的利用率越高，网内副本的冗余度越低。从图 9 所示的命中率仿真结果中可以看出：RGBE－AC 场景下的网内命中率为 18.15%，ULBBE－AC 场景下的网内命中率为 37.69%。相比于 RGBE－AC，ULBBE－AC 有更高的网内命中率，这一提升充分说明 ULBBE－AC 的分组方式更适合 NDN 网络，能更好地利用 NDN 的网内缓存，降低网内加密内容副本的冗余量，改善网络性能。

4.2　内容请求时延

内容请求时延同样是反映 NDN 网络性能的重要指标，该指标定义为网内每一跳获取时延的数学期望值。图 10 给出了 RGBE－AC 与 ULBBE－AC 分组场景下的分类请求时延，如图所示，随着类别编号的增加，两个场景下的内容请求时延均增大，这一现象实质上是佐证了低流行度内容由于请求过少，导致网内缓存不足，必须大概率去内容提供者处去获取。而进一步对比 RGBE－AC 和 ULBBE－AC，可以看到，针对流行度较高的内容，ULBBE－AC 中的内容请求时延比 RGBE－AC 要低，这是由于 ULBBE－AC 方案下，同一位置组中的用户属于同一个广播组，经过广播加密的内容在该组内合法用户共享，因此网络中内容的副本冗余量小、缓存利用率高，用户的请求易于在缓存中直接命中所请求的内容，从而获得较低的请求时延。而对于低流行度内容，由于用户对其较低的请求概率，导致

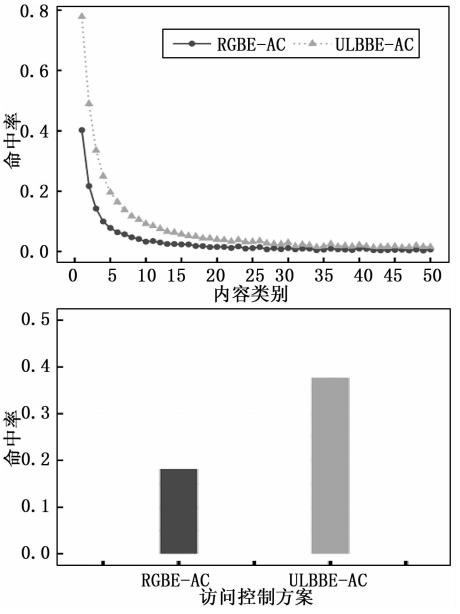

图 9　ULBBE－AC 和 RGBE－AC 命中率对比

网络中存在的内容副本较少，两种方案下，用户都需要到内容提供者处请求内容，因此，随着内容流行度的降低，两种策略下内容的请求时延趋于一致。

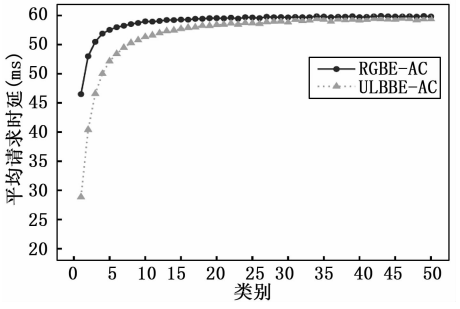

图 10　ULBBE－AC 和 RGBE－AC 命中率对比

5　结束语

本文提出了一种基于用户位置分组的广播加密访问控制方案，解决了基于广播加密的访问控制方案中用户分组问题，通过修改兴趣包结构提取传输路径设备信息，内容提供者将临近区域用户分入相同组内，实现分组优化。ndnSIM 仿真结果显示，相比较随机位置分组，ULBBE－AC 可以实现较高的缓存利用率，降低了用户请求内容的时延。

未来，将围绕广播加密的动态密钥生成与分发开展研究，设计更为灵活的 NDN 广播加密接入控制机制。

参考文献：

[1] Jacobson V，Smetters D K，Thornton J D，et al. Networking named content [A]. In Intl. conference on Emerging networking experiments and technologies [C]. ACM，2009，1－12.

（下转第 244 页）