doi:10.11959/j.issn.1000-436x.2015323

内容中心网络缓存隐私保护策略

朱轶[1,2]，糜正琨[1,3]，王文鼐[1]

（1. 南京邮电大学 通信与信息工程学院，江苏 南京 210046；2. 江苏大学 计算机科学与通信工程学院，江苏 镇江 212013；
3. 南京邮电大学 宽带无线通信与传感网技术教育部重点实验室，江苏 南京 210046）

摘 要：缓存隐私泄露是内容中心网络中的重要安全威胁之一，攻击者通过探测缓存可以获取合法用户的隐私信息。针对该安全问题，在隐私与非隐私内容区分的基础上，提出一种基于最近访问信息与回退机制的缓存隐私保护策略（CPPS-RVI&ECP），并与现有典型防御策略-随机 k 延迟（RFKD）对比，围绕隐私泄露率与网络命中率开展理论性能分析。该策略通过设置隐私标识，实现最近访问者的识别；通过随机缓存位置存入以及移出回退机制，降低了隐私泄露概率，且提升了网络性能。设定实验条件进行数值分析，结果表明，虽然 RFKD 有理想的隐私保护能力，但是它是以完全牺牲缓存的内容分发能力为代价的，而 CPPS-RVI&ECP 则通过合理设置回退概率，可以在保持较低隐私泄露率的同时，获得较高的网络命中率。

关键词：内容中心网络；缓存隐私探测；隐私保护策略；隐私泄露率；网络命中率

中图分类号：TN915.9 **文献标识码**：A

Cache privacy protection strategy in content centric networking

ZHU Yi[1,2], MI Zheng-kun[1,3], WANG Wen-nai[1]

(1. College of Communications & Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210046, China;
2. School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang 212013, China;
3. Key Laboratory of Broadband Wireless Communication and Sensor Network Technology, Ministry of Education,
Nanjing University of Posts and Telecommunications, Nanjing 210046, China)

Abstract: Cache privacy leak was one of the important security threats of CCN, the adversary could obtain the legitimate user's privacy information through probing cache visiting time. Aiming at this security problem, the privacy and non-privacy contents were dealt separately, then a cache privacy protection strategy based on recent visiting information and evicted copy up (CPPS-RVI&ECP) was proposed. In order to compare with the current typical defense strategy-random first k delay (RFKD), the theoretical analysis of privacy leak probability and network hit probability are further given. The CPPS-RVI&ECP identifies the recent visitor by setting privacy mark in interest packet, decreases the privacy leak probability by selecting replacing position randomly, and promotes the network performance by the mechanism of shifting evicted copy upstream. The numeric analysis results under the prescribed experimental conditions show that, whereas the ideal privacy protection ability of RFKD is obtained at the expense of sacrifice of cache contents delivery capability, the proposed CPPS-RVI&ECP can obtain low privacy leak probability and in the meantime maintain high network hit probability by setting reasonable upstream shifting probability.

Key words: content centric networking; cache privacy probe; privacy protection strategy; privacy leak probability; network hit probability

1 引言

随着Internet的快速发展，网络应用的主体正逐渐向内容服务转移，以主机为中心的传统IP网络结构已难以满足当前Internet的发展要求。自2006年起，国外学术界开展了多项关于未来网络体系结构

收稿日期：2015-05-30；**修回日期**：2015-10-28

基金项目：江苏省科技支撑计划（工业）基金资助项目（BE2013019）

Foundation Item: Jiangsu Provincial Science and Technology Support Program of Industrial Projects(BE2013019)

的研究项目，包括UC Berkeley RAD实验室提出的面向数据的网络架构（DONA, data-oriented network architecture）[1]、欧盟FP7的4WARD[2]以及发布/订阅式互联网路由范例（PSIRP, publish-subscribe internet routing paradigm）[3]、Palo Alto Research Center提出的内容中心网络（CCN, content-centric networking）[4]等，这些研究项目都采用了以内容为中心的网络架构思想，其中CCN的网络设计更具代表性，成为当前下一代互联网架构的研究热点。

缓存机制是 CCN 的核心特征，每个 CCN 节点都包含内容存储器（CS, content store），用于缓存数据分组，用户通过内容名寻址机制，就近获取所需数据分组。这一设计，可避免用户与内容源服务器之间链路性能不佳的问题，加快网络中其他用户访问缓存内容的响应时间，减轻网络的拥塞状况，提高网络资源的利用率。但是缓存机制作为一个公共、开放的数据交换平台，在提升网络性能的同时，也带来了隐私泄露的可能，现阶段 CCN 中由于缓存带来的隐私问题包括：缓存隐私泄露与内容隐私泄露[5, 6]。1）缓存隐私泄露，攻击者通过探测缓存中存储的内容，从而获知邻近用户对敏感内容的通信痕迹和访问行为信息，以达到邻居用户行为检测、隐私信息窥探等目的；2）内容隐私泄露，虽然 CCN 中已采用数字签名认证，对发布内容本身进行加密保护，但内容名未加密，并且与内容语义相关，攻击者可通过内容命名推断从缓存中获取敏感内容，并采用深度分组检测（DPI, deep packet inspection）对内容进行破解，实现隐私信息窃取。不同于 IP 网络，DPI 攻击仅能在网关或者网络重要节点处实施，CCN 中内容分散于网络各个节点缓存，且较长时间存储，因此 DPI 攻击更易于实现。

上述由于缓存所带来的隐私泄露问题严重威胁了 CCN 安全，本文在对现有缓存隐私保护策略分析的基础上，综合考虑了 CCN 的有效性和可靠性，提出一种基于最近访问信息与回退机制的缓存隐私保护策略（CPPS-RVI&ECP, cache privacy protection strategy based on recent visiting information and evicted copy up），通过合理设置回退概率，该策略可以在维持较低隐私泄露率的同时，获得较高的网络命中率。围绕 CPPS-RVI&ECP 的隐私泄露率与网络命中率，本文进一步开展了理论分析，并通过数值计算进行了策略性能评估。与前人工作相比，本文的主要贡献在于：1）所提出的 CPPS-RVI&ECP 策略兼顾了缓存隐私保护能力与 CCN 的缓存能力，避免了现有策略只考虑缓存隐私保护，而完全牺牲了 CCN 内容共享特征的问题；2）对 CPPS-RVI&ECP 及现有典型防御策略—随机 k 延迟策略的隐私泄露率进行理论研究，提出隐私泄露率近似公式，并加以评估。这一理论工作是现有 CCN 缓存隐私保护文献报道中所缺乏的。

2 缓存隐私探测

2.1 问题描述

内容获取时间测量，是 CCN 缓存隐私探测的主要手段[7, 8]。如图 1 所示场景，假设攻击者 A1 与合法用户 U1 为邻居用户，共存于一个接入路由器 R_1 范围之内，A1 通过测量对特定内容获取的往返时延（RTT, round trip time），即可推断 U1 是否最近请求过特定内容。攻击者首先测量从源服务器（source server）获取内容的往返时延 RTT_S（通过请求网络中未存的低流行度内容），再测量从最近路由（图 1 中 R_1）获取内容的往返时延 RTT_C（通过 2 次请求同一内容，第二次请求时，该内容已经存储于 R_1 上，测量第二次往返时延）。在完成以上准备工作后，攻击者根据目标探测内容进行请求，设测量获的往返时延为 RTT_A。

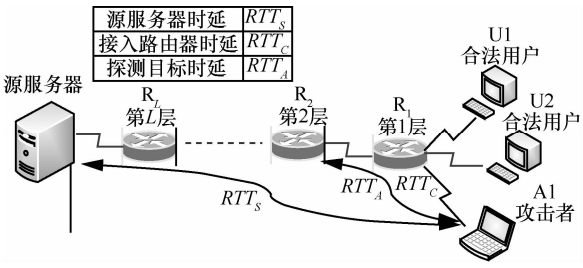


图 1 CCN 缓存隐私攻击示意

1) $|RTT_A - RTT_C| < \varepsilon$（$\varepsilon \to 0$），显然目标内容已经存在于最近路由 R_1 上，攻击者可以推断其邻居用户（如 U1）最近请求过该目标内容（此处，最近指 R_1 缓存更新时间之内）。

2) $RTT_A > RTT_C$ 且 $RTT_A < RTT_S$，该目标内容不存在于最近路由 R_1 上，但存在于网络中（如 R_2 上），攻击者可以推断其邻居用户在一个较长时间内有请求该目标内容的行为，但是最近未请求过。

3) $|RTT_A - RTT_S| < \varepsilon$，目标内容从源服务器请求获得，攻击者推断其邻居用户在较长时间内未请求过该内容。

上述攻击行为可以有效探测一跳范围内邻居用户对目标内容的请求信息和通信行为，即使攻击者具有多个邻居用户，如果借助部分先验知识，攻击者也可以较准确地推断出用户身份。

2.2　现有解决策略与相关研究工作

CCN 改善了现有 IP 网络面向主机模型所带来的一系列问题，但其缓存机制在提升网络性能的同时，也带来了新的安全隐患。文献[7]较早详细阐述了 CCN 中存在的 3 类安全问题：缓存污染攻击、PIT 泛洪攻击与缓存/内容隐私探测，分析了安全问题产生的原因，并给出防御缓存隐私泄露的基本对策。针对时间测量攻击，文献[7]指出，若为请求的内容增加一个响应时延，且该时延至少等于传输路径上具有 k 个接入分支路由器与终端用户之间的往返时延，则攻击者将无法推断该内容历史请求者的身份，这一方法虽然有效地以 k-anonymity 方式保护了缓存隐私，但额外增加的时延抵消了 CCN 缓存机制所带来的性能改善，严重降低了网络性能。文献[8]对缓存隐私进行了理论建模与分析，提出了 random-cache 的方法，通过对于内容请求随机产生 k 个不命中响应，实现缓存隐私保护。文献[9]围绕 CCN 的隐私问题开展讨论，并与现有 Internet 加以对比，研究内容包括缓存隐私、内容隐私、命名隐私，就缓存隐私保护而言，除了涉及文献[6, 7]所提对策，进一步指出协同缓存与概率缓存，也是可行的隐私保护策略，但该文未提出具体的解决方案。文献[10,11]在文献[8]的基础上，提出 3 种改进策略：“用户—内容”状态识别、“接口（face）—内容”状态识别、“接口—内容—用户”状态识别。结合 CCNx 的仿真分析，该研究工作指出如果路由器维护每一内容的请求状态，会导致负荷过重，改进思路包括：1）仅维护路由器接口的请求状态，对于某一接口上到达的初次访问请求，设置额外的往返时延；2）将用户状态维护从路由器移动到接入点上，由接入点确定是否需要对请求产生额外时延。该工作虽然有效降低了路由负荷，但是隐私泄露风险提升。文献[12]也分析 CCN 的隐私风险，指出内容的隐私敏感性与内容流行度密切相关，内容的流行度越低，其隐私敏感性越高，因此可以有选择性地进行内容隐私保护，这一观点有助于更好折中网络性能和安全关系。文献[13]另辟蹊径，设计了一种内容名和内容本身的隐藏方法，将目标内容和内容名字进行混合，这一方法使攻击者探测难度增加，从而降低了隐私被攻击的风险；文献[14]侧重讨论了缓存探测方法和缓存特征时间测量，对隐私保护策略涉及不多，建议通过内容标记区分敏感内容，避免缓存该类内容来实现隐私保护，但具体策略没有给出。

以上为近年 CCN 缓存隐私问题的主要研究报道，类似于通信系统的有效性与可靠性之间的矛盾，CCN 的缓存隐私保护与内容分发能力也彼此矛盾，通过人为生成额外时延或者多次不命中，的确可以较理想地掩盖缓存中内容的存储痕迹，但缓存机制带来的网络性能改善优势也丧失殆尽。如何设计缓存隐私保护策略，在有效保护缓存隐私的同时，兼顾 CCN 的内容分发能力，是 CCN 研究者需要仔细考虑的问题。

总结现有 CCN 缓存隐私保护的主要策略，有如下几种方法。

1) 内容指定时延（CSD, content-specific delay）。对于每一个隐私敏感内容 C，路由器记录该内容的源服务器获取时间 γ_C，当有请求到达路由器，即使该内容存储于缓存内，路由器也延迟 γ_C 时间，再返回内容给请求者。该方法可以提供完美缓存隐私保护，但是 CCN 的缓存优势相应完全丧失。

2) 固定 k 延迟（FFKD, fixed first k delay）。为了避免隐私内容每次请求时都出现 γ_C 时延，FFKD 策略仅对隐私内容在缓存中的前 k_C 次请求设置 γ_C 额外时延（k_C 为固定值），该策略是 CSD 的改进，但是依然存在隐私泄露风险。如果攻击者获知 k_C 值，则可以根据攻击延迟次数推断出该内容已请求次数，从而得到缓存隐私信息。

3) 随机 k 延迟（RFKD, random first k delay），即文献[7]中提出的 random-cache 方法。该策略对隐私内容设置前 k_C 次随机请求时延，$k_C \in [0, N)$，且 k 值可以根据内容流行度动态调整，但该方法还是会带来较大时延，严重制约网络性能。

4) “用户—内容”状态识别（UCSR, user-content state recognition）。方法 4）~方法 6）均为文献[10, 11]所提出，文献中并未给予这 3 种策略合适名称，根据其工作原理，分别称之为 UCSR 策略、FCSR 策略以及 FCUSR 策略。其中 UCSR 策略要求边缘路由器记录访问用户名以及该用户所请求的内容名称，利用<用户名、请求内容名>历史数据，路由器可以识别用户是否首次请求该内容，对于首次请求的用户设置 γ_C 额外时延。该策略可以识别请求者

身份，因而可提供理想的隐私保护，但是实现难度高，边缘路由器难以维护所有访问者的历史请求信息。

5) “接口—内容”状态识别（FCSR, face-content state recognition）。为了降低边缘路由器的负载，FCSR 策略不要求路由器识别每一访问者，仅记录<访问接口、请求内容名>信息，当某一接口首次出现对新内容的请求，则为本次请求设置 γ_C 额外时延；而如果该接口有过请求目标内容的历史记录，将直接返回内容给请求者。FCSR 策略不会给路由器带来较大的压力，但是隐私保护能力差，当攻击者与合法用户存在于同一路由接口下，路由器无法区分出攻击者。

6) “接口—内容—用户”状态识别（FCUSR, face-content-user state recognition）。综合上述 2 种策略的优缺点，文献[10, 11]提出可以在边缘路由器下再设置一层接入点，由接入点记录、维护<用户、请求内容名>信息，边缘路由器记录、维护<访问接口、请求内容名>信息。对于接入点，判断请求用户是否首次请求目标内容，并将判断结果告知边缘路由器。边缘路由器对于接口首次出现新内容请求时，直接设置额外时延；对于有接口历史记录的请求，再去根据接入点判断结果，识别请求用户的身份。这一设置有效分解了边缘路由器的负载，但策略复杂度高，仍存在一定隐私泄露风险（攻击者与合法用户分属不同接入点以及不同接口）。

如何有效隐藏缓存隐私，究其原理，不难发现，隐藏缓存访问历史信息，关键在于攻击者初次请求时，路由器给予特殊处理，使其无法分辨缓存中是否存有该内容，因此如何判断用户对于特定内容的首次访问，变得至关重要；同时，为了避免路由器负载过重，区分隐私内容和非隐私内容也是一个关键点，路由器应仅对隐私内容施加保护策略。基于以上考虑，下面将分别讨论隐私内容标识以及基于用户访问信息与回退机制的隐私保护策略，并加以性能分析。

3 隐私保护策略设计

区分非隐私内容和隐私内容，是有效开展缓存隐私保护的第一步，本文中主要根据内容流行度加以区分。对于被大量用户所关注的高流行度内容，一方面所能泄露的隐私信息少，对攻击者而言，没有探测价值，另一方面此类内容访问用户数量大，攻击者难以推断具体请求用户身份，攻击难度大，因此内容请求流行度是区分隐私内容的参考基准[15]。

为了更好界定隐私内容以及便于后续分析，现设定：1）CCN 网络源服务器可提供 M 个不同的内容，根据内容对应的流行度均匀划分成 K 个不同类别，即每一类包含 $m=\frac{M}{K}$ 个内容文件，每个内容的大小相同；2）采用 Zipf 分布描述网络边缘节点（第一层）到达请求的流行度，设 q_k 表示第 k 类内容的请求概率，即 $q_k=\frac{c}{k^{\alpha}}$，$c>0$，这里 α（$\alpha\geqslant 0$）代表了流行度分布的集中程度，α 越大，内容请求越集中于 k 较小的内容。

定义 1 隐私泄露信息量。定义为缓存中某一类内容潜在泄露信息量的大小，参考信息论中信息量的定义，对于第 k 类内容而言，其潜在泄露信息量 I_k 取决于该类内容的请求概率

$$I_k=\mathrm{lb}\frac{1}{q_k} \tag{1}$$

定义 2 隐私内容。设 I_{av} 为平均隐私泄露度，如式（2），对于第 k 类内容，当其隐私泄露信息量 I_k 大于 I_{av}，将其视为隐私内容；反之，则视为非隐私内容。

$$\begin{cases} I_{\mathrm{av}}=\sum\limits_{k=1}^{K}q_k\,\mathrm{lb}\dfrac{1}{q_k} \\ I_k \underset{\text{non-Privacy}}{\overset{\text{Privacy}}{\gtrless}} I_{\mathrm{av}} \end{cases} \tag{2}$$

基于上述隐私内容界定，路由器可以根据历史访问记录，统计最近时期内每类内容的请求概率，进而确定隐私类别，并针对隐私内容，实施保护策略。

CCN 缓存隐私的保护策略可以从 4 个方面独立开展设计：1）识别并记录请求的来源，以便区分合法用户与攻击者身份；2）增加时间不确定性，从缓存时间角度设计缓存策略，使攻击者无法确认攻击对象在最近一段时间内是否被请求过；3）增加空间不确定性，设计网络缓存策略从多个路由器中选择进行内容存储，攻击者虽然能确认攻击目标是否最近曾被访问，但无法确认历史请求的来源（来自于哪个接入路由器）；4）增加接入用户群体的不确定性，利用 k-anonymity 特性，使攻击者虽从时间、空间角度可以确认攻击目标的历史请求信息，但无法确认该请求来自于接入路由下的哪一个用户。分析以上 4 种设计思路，不难看出每一种方法均具备隐藏缓存隐私的能力，但具体设计中需要平衡可行性与有效性，若开销

太大或者严重降低网络性能，即使可获得完美隐私保护，也无实施价值。鉴于此，本文综合前 3 种设计思路，提出一种基于最近访问信息与回退机制的缓存隐私保护策略，该策略通过在兴趣分组头部设置隐私标识，标注最近访问用户，从而识别当前请求用户是否属于首次请求；通过随机回退机制增加内容在网络中的缓存时间，一方面在时间上增加模糊度，提升攻击者探测缓存隐私的难度，另一方面提高内容的网络命中率，改善网络访问性能。策略具体步骤如下。

1) 路由器针对隐私内容设置隐私标识，用于存储该类隐私内容的最近访问时间；用户在发送请求兴趣分组时，在兴趣分组的 nonce 字段内置入上次访问时间（获取时间）；当兴趣分组到达路由器时，路由器提取其中的 nonce 字段，将 nonce 中的时间与该内容隐私标识内的最近访问时间对比，如果基本接近，则判断兴趣分组发送者为上一次内容请求者，直接返回数据分组，且将隐私标识更新为当前访问时间；如果时间偏差较大，则判断兴趣分组发送者为新的请求者，路由器将隐私标识更新为当前访问时间，同时延迟 γ_C 时间（源服务器的获取时间）再发送数据分组给请求者。图 2 给出了最近访问用户识别及处理流程。

2) 当请求未被命中，且请求对象为隐私内容，路由器在获取该隐私内容后，不采用常规的 LRU（least recently used）策略将该内容置换到缓存队列首部，而是随机将该内容存入缓存中任意位置，同时存入位置至缓存队列尾部的所有内容顺序向后移动一位；若请求被命中，则不改变所请求隐私内容的存储位置。这一随机存入操作，是确保攻击者无法估计所请求内容在缓存中的停留时间。需要注意的是，非隐私内容依然采用 LRU 置换策略。

3) 当内容（包括隐私与非隐私）被移出当前路由器缓存队列时，以概率 p 回退上一层节点存储，存入上一层节点缓存的队列首部；以概率 $1-p$ 直接丢弃，如图 3 所示。

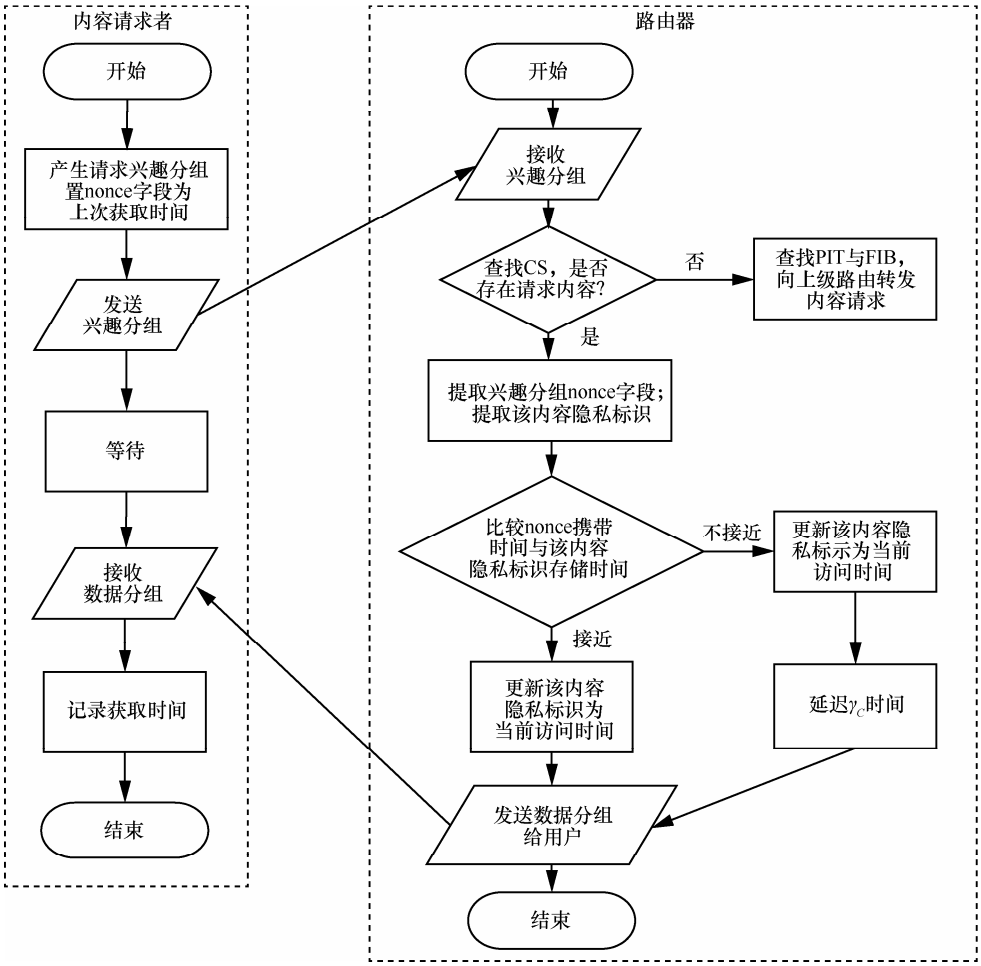


图 2　最近访问用户识别及处理流程

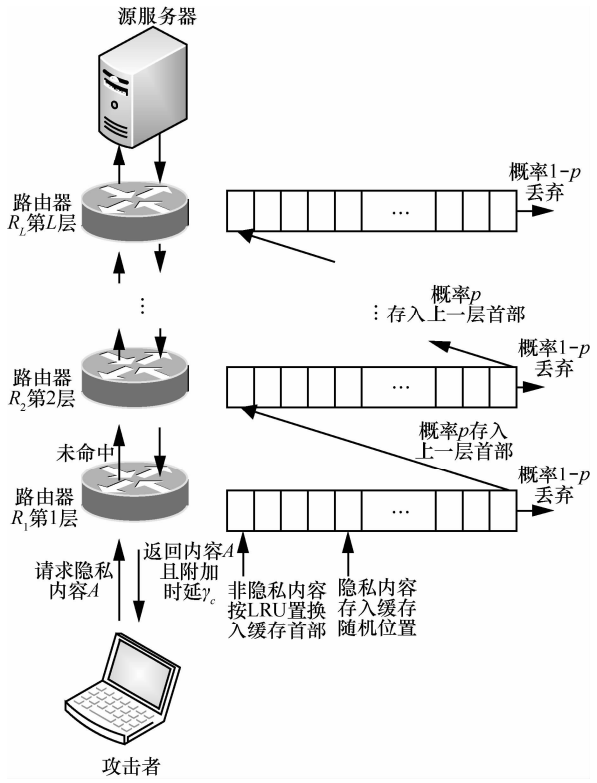


图 3　隐私内容置换及回退机制

以上 CPPS-RVI&ECP 策略设计，同时兼顾了内容隐私保护性与分发有效性。

通过设置隐私标识，比较路由器与兴趣分组内的内容最近访问时间，判断当前请求者是否为上一次内容请求者，从而实现请求者身份的识别。对于新的请求者，延迟 γ_C 时间，使其不能推断请求目标是否存在于缓存内。相比较 UCSR/ FCUSR 策略，本文识别方法无需记录所有用户状态，路由器的开销可控。

仅识别请求者身份，还不足以保护内容隐私，如攻击者估计出攻击目标在缓存中的停留时间，进而在该时间区间内多次请求攻击目标，如果发现出现延迟 γ_C 时间现象，必然是该次请求之前，有其他用户也请求了此内容，从而推断出邻居用户的访问行为。这一隐私泄露的核心原因，是攻击者可估计攻击目标在缓存内的停留时间，鉴于此，本文进一步设计了随机位置存入策略，降低上述隐私泄露可能。

相比较 LRU 策略，采用随机位置存入策略后，隐私内容命中率必然下降，为了改善访问有效性，本文提出内容移出回退机制，增加内容在网络内的停留时间，提高隐私内容在网络中的命中率。之所以采用概率回退，同样是为了避免攻击者估计出所请求内容在缓存内的停留时间。

4　理论性能分析

本节从隐私保护度与缓存利用率角度对 CPPS-RVI&ECP 及 RFKD 策略进行理论分析，隐私保护度评价指标选择隐私泄露概率，缓存利用率指标选择网络命中概率。之所以采用 RFKD 策略进行对比，是因为本文提出的 CPPS 设计目标侧重于在请求者身份区分基础上，增加网络不确定性，而 RFKD 是该类策略的传统代表；至于 UCSR/FCSR/FCUSR，仅仅侧重于请求来源识别，与本文设计目标有所偏离。

在第 3 节设定基础上，进一步假设：1）网络为 L 层路由器级联拓扑；2）合法用户与攻击者产生的请求兴趣分组均服从泊松分布到达，λ_N^i 为合法用户第 i 层节点的请求到达率，显然合法用户第一层节点第 k 类内容的请求到达率为 $\lambda_N^1 q_k$，$\lambda_A^i(k)$ 为攻击者第 i 层节点第 k 类内容的请求到达率（攻击行为通常针对某个特定类，对于未被攻击的内容类别 $\lambda_A^i(k)$=0）；3）合法用户 2 次连续对第 k 类内容请求的时间间隔为 τ_N^k，攻击者 2 次连续对第 k 类内容请求的时间间隔为 τ_A^k；4）第 i 层路由器的特征时间为 τ_i，即某内容从第 i 层节点缓存队列头部移动到尾部的平均时间（也可看作平均停留时间）；5）节点缓存大小相等，均为 C 个内容文件；6）CPPS-RVI&ECP 策略下第 k 类内容的隐私泄露概率为 $P_{\text{Leak}}^{\text{CPPS}}(k)$，RFKD 策略下第 k 类内容的隐私泄露概率为 $P_{\text{Leak}}^{\text{RFKD}}(k)$；7）CPPS-RVI&ECP 策略下第 k 类内容的网络命中率为 $P_{\text{Hit}}^{\text{CPPS}}(k)$，RFKD 策略下第 k 类内容的网络命中率为 $P_{\text{Hit}}^{\text{RFKD}}(k)$。表 1 列出了本文理论分析中涉及的主要符号定义。

4.1　隐私泄露概率

由 CPPS-RVI&ECP 策略可知，若攻击者对某隐私内容的 2 次连续请求之间，有合法用户也请求过该内容，则存在隐私泄露风险，攻击者通过发现隐私标识发生变化，从而获知有其他用户请求该类内容。考虑到隐私内容可能存在于网络不同层次的路由上，隐私泄露概率不同，可分为以下 2 种情况。

1) 对于第一层路由器，设隐私内容随机存入位置为 $j(1 \leqslant j \leqslant C)$，则该内容在第一层缓存内的平均停留时间为 $\tau_P^1 = \dfrac{\mathrm{E}[(C-j)\tau_1]}{C}$，这里 $\mathrm{E}[\bullet]$ 表示数学

表 1　　**主要符号定义**

符号	定义	符号	定义
M	源服务器提供文件数	λ_N^i	合法用户第 i 层节点的请求到达率
K	内容类别数	τ_N^k	合法用户 2 次连续对第 k 类内容请求的时间间隔
m	每一类包括的文件数	$\lambda_A^i(k)$	攻击者第 i 层节点第 k 类内容的请求到达率
q_k	Zipf 分布下，第一层第 k 类内容的请求概率	τ_A^k	攻击者 2 次连续对第 k 类内容请求的时间间隔
α	Zipf 的流行度参数	τ_i	第 i 层路由器的特征时间
L	CCN 网络层数	C	节点缓存大小
p	CPPS-RVI&ECP 中的回退概率	k_C	RFKD 对隐私内容设置额外时延的次数

期望，设 j 服从均匀分布。若该隐私内容是由攻击者所请求获得，且攻击者 2 次对该文件的请求间隔小于 τ_P^1，则第一层第 k 类隐私泄露概率 $P_{\text{Leak-1}}^{\text{CPPS}}(k)$ 为攻击者第二次请求到来之前，存在至少一次合法用户对该文件的请求的概率，如式（3）[注1][16~20]所示

$$\begin{aligned}P_{\text{Leak-1}}^{\text{CPPS}}(k)&=P\left\{\tau_N^k\leqslant\tau_A^k\,|\,\tau_A^k\leqslant\tau_P^1\right\}\\&=1-\mathrm{e}^{-\lambda_A^1(k)\tau_P^1}-\frac{m\lambda_A^1(k)}{m\lambda_A^1(k)+\lambda_N^1 q_k}\left[1-\mathrm{e}^{-\left(\lambda_A^1(k)+\frac{\lambda_N^1 q_k}{m}\right)\tau_P^1}\right]\end{aligned}\tag{3}$$

2）如图 4 所示，若隐私内容被移出第 $i-1\left(2\leqslant i\leqslant L\right)$ 层缓存，以概率 p 移入第 i 层路由器，且该隐私内容将以概率 p^{i-1} 在网络中停留 $\tau_P^1+\tau_2+\cdots+\tau_i$ 时间，则第 i 层第 k 类隐私泄露概率 $P_{\text{Leak-}i}^{\text{CPPS}}(k)$ 为攻击者 2 次对该文件的请求间隔小于该停留时间，且攻击者 2 次请求之间至少存在一次合法用户对该文件的请求的概率，如式（4）所示

$$\begin{aligned}P_{\text{Leak-}i}^{\text{CPPS}}(k)&=p^{i-1}P\left\{\tau_N^k\leqslant\tau_A^k\,|\,\tau_P^1\leqslant\tau_A^k\leqslant\tau_P^1+\sum_{s=2}^{i}\tau_s\right\}\\&=p^{i-1}\left\{\mathrm{e}^{-\lambda_A^1(k)\tau_P^1}-\mathrm{e}^{-\lambda_A^1(k)\left(\tau_P^1+\sum_{s=2}^{i}\tau_s\right)}-\frac{m\lambda_A^1(k)}{m\lambda_A^1(k)+\lambda_N^1 q_k}\cdot\right.\\&\qquad\left.\left[\mathrm{e}^{-\left(\lambda_A^1(k)+\frac{\lambda_N^1 q_k}{m}\right)\tau_P^1}-\mathrm{e}^{-\left(\lambda_A^1(k)+\frac{\lambda_N^1 q_k}{m}\right)\left(\tau_P^1+\sum_{s=2}^{i}\tau_s\right)}\right]\right\}\end{aligned}\tag{4}$$

综上 2 种情况，CPPS-RVI&ECP 策略的第 k 类内容隐私泄露概率 $P_{\text{Leak}}^{\text{CPPS}}(k)$ 应为

$$P_{\text{Leak}}^{\text{CPPS}}(k)=P_{\text{Leak-1}}^{\text{CPPS}}(k)+\sum_{i=2}^{L}P_{\text{Leak-}i}^{\text{CPPS}}(k)\tag{5}$$

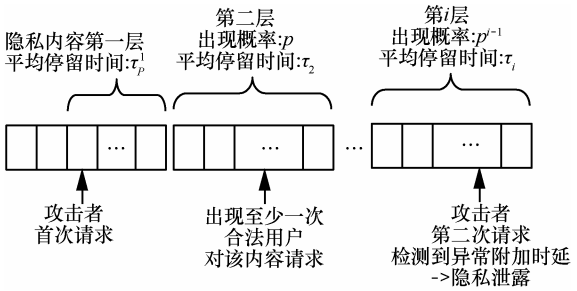


图 4　CPPS-RVI&ECP 第 i 层隐私泄露示意

对于 RFKD 策略，由策略规则可知，该策略对隐私内容设置前 k_C 次随机请求时延，则合法用户的命中率应为 k_C 次连续请求间隔小于第一层路由器的特征时间 τ_1 的概率，该命中率应等同于缓存中的该类内容存储概率（出现概率）。对于攻击者的请求而言，若无合法用户的存在，当 2 次请求之间的间隔 τ_A^k 大于 τ_1，则出现不命中事件；但合法用户的存在，导致即使 τ_A^k 大于 τ_1，攻击者也有一定概率命中内容，这部分命中概率即为隐私泄露概率。因此 RFKD 策略的第 k 类内容隐私泄露概率 $P_{\text{Leak}}^{\text{RFKD}}(k)$ 应为

$$P_{\text{Leak}}^{\text{RFKD}}(k)=P\left\{\tau_A^k>\tau_1\right\}P^{k_C+1}\left\{\tau_N^k\leqslant\tau_1\right\}\tag{6}$$

CPPS-RVI&ECP 策略与 RFKD 策略下，网络总的隐私泄露概率为

$$\begin{cases}P_{\text{Leak}}^{\text{CPPS}}=\sum\limits_{k\in\text{Privacy}}q_k P_{\text{Leak}}^{\text{CPPS}}(k)\\P_{\text{Leak}}^{\text{RFKD}}=\sum\limits_{k\in\text{Privacy}}q_k P_{\text{Leak}}^{\text{RFKD}}(k)\end{cases}\tag{7}$$

4.2　网络命中率

缓存隐私保护策略的引入，在提高缓存安全性的同时，又制约了缓存所带来的内容共享能力，本节分析无攻击出现条件下，合法用户的网络命中概率。由

注1 式（3）本质为内容请求服从泊松分布到达时，请求间隔的条件分布函数。在 CCN 建模分析中，计算特征时间并基于负指数分布计算请求的出现概率，较为常见。该建模方法在 LRU 策略研究中就已提出，见文献[16]；在 ICN/CCN 研究中，由意大利学者 G.Carofiglio 较早采用，之后研究者多引用文献[17, 18]研究工作，借助该分析手段，围绕 CCN 不同研究方面开展理论分析，如文献[19, 20]等。本文后续理论分析也均基于该建模分析方法。

文献[16~18]的分析可知，合法用户对同一文件 2 次连续请求之间的时间间隔 τ_N^k 若小于该类内容在网络中的平均停留时间，则不管第一次请求是否命中，第二次请求一定命中，因此 CPPS-RVI&ECP 策略下，考虑到非隐私内容采用 LRU 置换策略，新内容到达缓存将置入缓存队列头部，且移出缓存同样以概率 p 移入上一层路由缓存队列的首部，则非隐私内容第 k 类内容网络命中率应为

$$P_{\substack{\text{Hit}\\ k\in\text{non-Privacy}}}^{\text{CPPS}}(k)=P\{\tau_N^k\leqslant\tau_1\}+\sum_{i=2}^{L}p^{i-1}P\left\{\sum_{s=1}^{i-1}\tau_s\leqslant\tau_N^k\leqslant\sum_{s=1}^{i}\tau_s\right\}$$
$$=1-\mathrm{e}^{-\frac{\lambda_N^1 q_k}{m}\tau_1}+\sum_{i=2}^{L}p^{i-1}\left\{\mathrm{e}^{-\frac{\lambda_N^1 q_k}{m}\sum_{s=1}^{i-1}\tau_s}-\mathrm{e}^{-\frac{\lambda_N^1 q_k}{m}\sum_{s=1}^{i}\tau_s}\right\} \quad (8)$$

而对于隐私内容，新内容到达时候将随机存入缓存队列，因此隐私内容第 k 类内容网络命中率应为

$$P_{\substack{\text{Hit}\\ k\in\text{Privacy}}}^{\text{CPPS}}(k)=P\{\tau_N^k\leqslant\tau_P^1\}+pP\{\tau_P^1\leqslant\tau_N^k\leqslant\tau_P^1+\tau_2\}+$$
$$\sum_{i=3}^{L}p^{i-1}P\left\{\tau_P^1+\sum_{s=2}^{i-1}\tau_s\leqslant\tau_N^k\leqslant\tau_P^1+\sum_{s=2}^{i}\tau_s\right\} \quad (9)$$

式（9）中，τ_P^1 在第一层缓存内的平均停留时间。由上述分析可知，对于 RFKD 策略，当且仅当第一层路由器连续出现 k_C 个请求，满足 2 次请求间隔小于 τ_1，才会命中（命中事件从第 k_C+1 个请求开始），因此该策略下第 k 类内容网络命中率应为

$$P_{\text{Hit}}^{\text{RFKD}}(k)=P^{k_C+1}\{\tau_N^k\leqslant\tau_1\}=\left\{1-\mathrm{e}^{-\frac{\lambda_N^1 q_k}{m}\tau_1}\right\}^{k_C+1} \quad (10)$$

4.3 特征时间

由于在前文隐私泄露概率与网络命中率分析中，特征时间是分析关键，参考文献[16]中关于特征时间的定义，结合 CPPS-RVI&ECP 与 RFKD 策略的规则，可得出特征时间 τ_i 的定义如下。

定义 3 （特征时间-CPPS）。在 CPPS-RVI&ECP 策略下，文件从第 i 层路由器缓存队列首部移动到尾部平均所需的时间，记为 τ_i-CPPS，在不致混淆的情况下可简记为 τ_i，它满足

$$\begin{cases} m\sum\limits_{k\in\text{non-Privacy}}(1-\mathrm{e}^{-\left[\lambda_A^i(k)+\frac{\lambda_N^i(k)}{m}\right]\tau_i})+ \\ m\sum\limits_{k\in\text{Privacy}}(1-\mathrm{e}^{-\left[\lambda_A^i(k)+\frac{\lambda_N^i(k)}{m}\right]E\left[\frac{C-j}{C}\right]\tau_i})=C,i=1 \\ m\sum\limits_{k=1}^{K}(1-\mathrm{e}^{-\left[\lambda_A^i(k)+\frac{\lambda_N^i(k)}{m}\right]\tau_i})=C,1<i\leqslant L \end{cases} \quad (11)$$

其中，$\lambda_N^i(k)$ 为合法用户第 i 层节点第 k 类内容的请求到达率，$\lambda_A^i(k)+\dfrac{\lambda_N^i(k)}{m}$ 为有攻击时第 i 层第 k 类内容中某一特定文件的到达率。

证明

1) 对于第一层隐私内容，攻击请求服从参数为 $\lambda_A^1(k)$ 的泊松分布，合法用户请求服从参数为 $\lambda_N^1(k)$ 的泊松分布，则第 k 类中任一内容请求服从参数为 $\lambda_k=\lambda_A^1(k)+\dfrac{\lambda_N^1(k)}{m}$ 的泊松分布。

2) 由于当 $i=1$ 时，隐私内容会随机插入缓存中的第 j 个位置，因此第一层区分隐私与非隐私内容。在时间区间 τ=E$\left[\dfrac{C-j}{C}\right]\tau_1$ 内，$1-\mathrm{e}^{-\lambda_k\tau}$ 为第 k 类中任一内容请求至少出现一次的概率，若相同内容的多次请求仅记录一次，则 $m\left(1-\mathrm{e}^{-\lambda_k\tau}\right)$ 为第 k 类的平均请求出现次数，$m\sum_{k\in\text{Privacy}}\left(1-\mathrm{e}^{-\lambda_k\tau}\right)$ 为隐私类的请求出现次数，同理，$m\sum_{k\in\text{non-Privacy}}\left(1-\mathrm{e}^{-\lambda_k\tau_1}\right)$ 为 τ_1 时间内非隐私类的请求出现次数。

3) 若 τ_1 时间内，第一层隐私与非隐私类请求次数恰好等于缓存大小 C，则某一文件在该区间开始时刻处于路由队列首部，该时间段结束时将有可能移动到路由队列尾部。

4) 对于 $1<i\leqslant L$ 时，隐私与非隐私内容都是存入缓存队列首部，因此不加以区分。此时，$m\sum_k\left(1-\mathrm{e}^{-\lambda_k\tau_i}\right)$ 为第 i 层所有类文件的平均请求次数，若该值等于 C，则 τ_i 满足某文件从缓存队列首部移动到尾部所需时间。式(11)得证。

可见特征时间本质上描述了：第 i 层某文件的 2 次请求间隔时间，等于 C 个不同文件请求的平均所需时间。此外，需要说明的是，以概率 p 移入上一层路由缓存，不影响存入位置，仅影响第 i 层节点第 k 类内容的请求到达率。

定义 4 （特征时间-RFKD）。在 RFKD 策略下，文件从第 i 层路由器缓存队列首部移动到尾部平均所需的时间，记为 τ_i-RFKD，在不致混淆的情况下可简记为 τ_i，它满足

$$m\sum_{k=1}^{K}\left[1-\mathrm{e}^{-\left[\lambda_A^i(k)+\frac{\lambda_N^i(k)}{m}\right]\tau_i}\right]=C,1\leqslant i\leqslant L \quad (12)$$

其物理意义同 τ_i-CPPS。特别地，当 $i=1$ 时，即得到RFKD策略计算隐私泄露率与网络命中率所

需的第一层特征时间 τ_1，此时，$\lambda_N^1(k)=\lambda_N^1 q_k$。

5　数值结果与分析

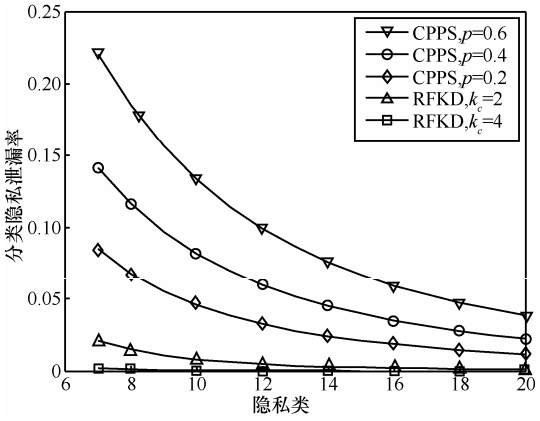
本节首先对本文策略和 RFKD 策略的隐私泄露率与网络命中率进行数值分析与比较，然后对 CCN 现有隐私保护策略的特性进行综合比较。数值分析工具为 Matlab。具体分析过程为：1）由式（1）、式（2）确定隐私内容类别与非隐私内容类别；2）基于式（11）、式（12）分别计算出 CPPS 与 RFKD 策略下的每层路由器的特征时间；3）将特征时间代入式（3）~式（7）分别计算出 CPPS 与 RFKD 策略的隐私泄露率（仅计算隐私类）；4）将特征时间代入式（8）~式（10）分别计算出 CPPS 与 RFKD 策略的网络命中率；5）更改网络参数设置，重复步骤 1）~步骤 4），并对结果进行对比分析。

参考文献[17, 21]关于 CCN 网络应用参数的设置，设定网络拓扑采用图 1 所示 L 层结构，$L=3$；CCN 可提供总的内容文件数 $M=20\,000$ 个，根据流行度分为 $K=200$ 个类别，每一类包含 $m=100$ 个内容文件，每个内容文件的平均大小为 10 MB；每个 CCN 节点缓存大小 $C=10$ GB；用户产生的内容请求服从参数为 $\lambda_N^1=1\,000$ content/s 的泊松分布，流行度模型采用 Zipf 分布。结合文献[22]对内容流行度分布的研究工作，Zipf 分布参数选取 $\alpha=0.8$ 以及 $\alpha=1.2$，其中 $\alpha=0.8$ 为 UGC（user generated content）业务的典型值、$\alpha=1.2$ 为 VOD（video on demand）业务的典型值。

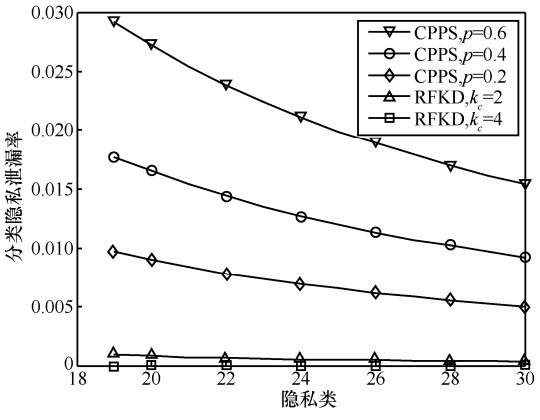
由于缓存隐私探测中，攻击者发送探测请求的时间间隔直接影响隐私探测效果，现定义攻击速率 v 为 $\lambda_A^1(k)=\dfrac{v\lambda_N^1 q_k}{m}$，即攻击者请求速率与合法用户请求速率的比值。

5.1　隐私泄露率分析

图 5 为 CPPS-RVI&ECP 与 RFKD 分类隐私泄露率对比，此时 v=0.01。根据式（2）给出的隐私内容界定条件，$\alpha=1.2$ 时第 7 类以后为隐私类，$\alpha=0.8$ 时第 19 类以后为隐私类。为了说明关键参数对策略性能的影响，对于 CPPS-RVI&ECP，取 p 等于 0.2、0.4、0.6，对于 RFKD，取 k_C 等于 2、4。由计算结果可见，CPPS-RVI&ECP 的隐私保护能力弱于 RFKD，且随着 p 的增加，内容回退存储概率增加，内容在网络中的停留时间变长，隐私泄露率相应提高。而 RFKD 的隐私保护能力很强，其隐私保护能力接近理想，在 k_C 等于 2 时，仅前几类隐私内容略有泄露可能，在 k_C 等于 4 时，几乎无隐私泄露。但同时注意到，CPPS-RVI&ECP 在回退概率 p 较小时，隐私保护能力与 RFKD 接近，如 p=0.2 时隐私泄露率与 RFKD 相差不大，可有效实现隐私保护。此外，图 5 也揭示了内容流行度分布对隐私泄露率的影响，随着 α 的提高，第一层到达的内容请求更集中于前若干类内容，这些类别的内容在网络中的存储比例增大，受到隐私探测时，更容易出现隐私泄露；而低流行度内容由于本身合法用户请求比例较低，内容在缓存中的出现概率不高，隐私泄露率相应下降。因此，$\alpha=1.2$ 的分类隐私泄露率普遍高于 $\alpha=0.8$ 的对应类别隐私泄露率。



(a) $\alpha=1.2$

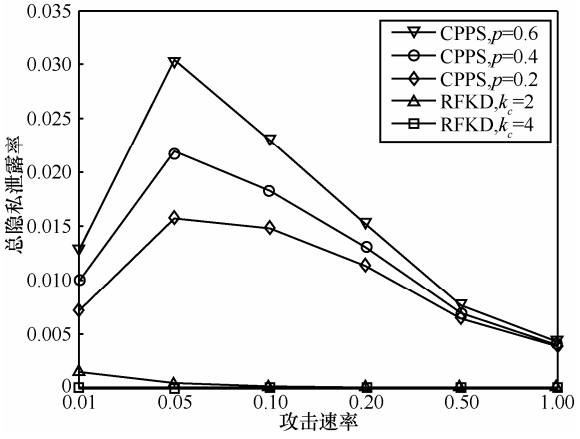


(b) $\alpha=0.8$

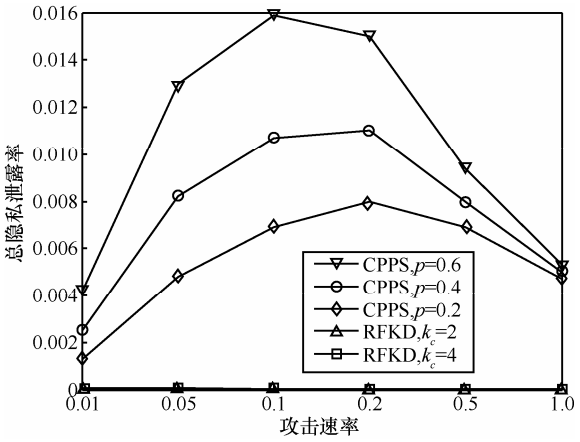
图 5　分类隐私泄露率（CPPS 与 RFDK）

图 6 给出了攻击速率对网络总隐私泄露率的影响，攻击速率反映了攻击者对探测内容所发送 2 次请求之间的时间间隔，而探测效果直接受制于该时间间隔的设置。若该时间间隔过小，比如小于路由

器的特征时间，攻击者的命中率会提高，但是所命中的内容都是由攻击者之前请求所获取，所以隐私探测效果较差；若该时间间隔过大，攻击者的探测请求到达路由器时，合法用户所请求的内容可能已经移出缓存，因此也不能获得较高的隐私泄露率。由上分析可知，攻击速率过大和过小，如 v=1 或 v=0.01，都不能使攻击者获得其想要的隐私探测效果；而攻击速率恰好取某个速率区间时，攻击效果最佳。由图 6 可见，在本文设定仿真条件下，对于 CPPS-RVI&ECP，若 $\alpha=1.2$，攻击速率 v=0.05 左右，隐私泄露率最大；若 $\alpha=0.8$，攻击速率 $v\in[0.1,0.2]$ 范围附近，隐私泄露率最大。



(a) $\alpha=1.2$



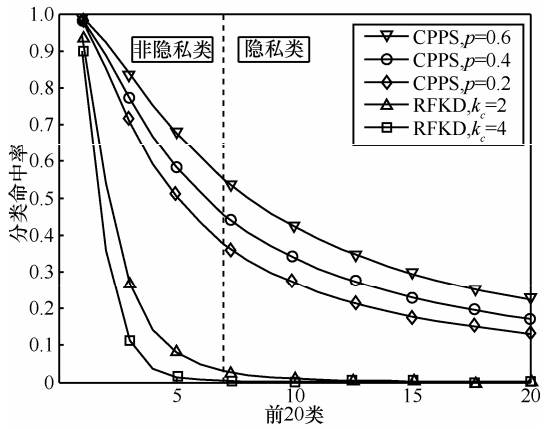
(b) $\alpha=0.8$

图 6 攻击速率与隐私泄露率

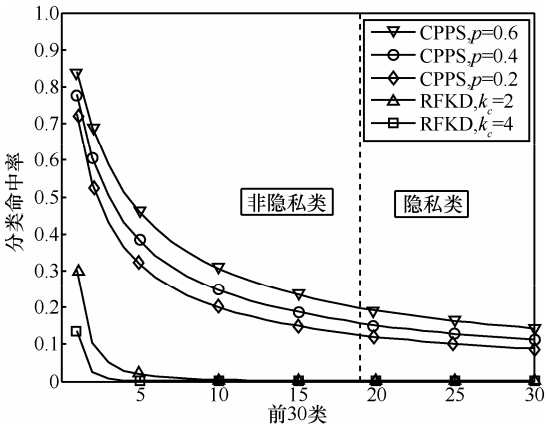
从总体隐私泄露率看，RFKD 通过随机设置前 k_C 次请求的获取时延，基本获得了理想隐私保护。CPPS-RVI&ECP 的隐私泄露体现在：攻击者 2 次请求之间，有合法用户也请求了该内容，攻击者通过察觉隐私标识的变更，发现合法用户的请求行为；由于回退机制的存在，导致内容在网络中的停留时间增加，攻击者 2 次请求之间合法用户的请求出现概率也相应增大。因此，CPPS-RVI&ECP 的总体隐私泄露率也随着回退概率 p 的增加而提高，但同样可看到，当 p 值较小时，CPPS-RVI&ECP 的总体隐私泄露率处于一个较低水平，即使在攻击者选择最优攻击速率范围时，p=0.2 的隐私泄露率为 0.015 ($\alpha=1.2$)、0.006 5 ($\alpha=0.8$)，也体现了较好的隐私泄露抑制能力。

5.2 网络命中率分析

图 7、图 8 分别给出了 CPPS-RVI&ECP 与 RFKD 分类命中率与网络总命中率对比。从上一节分析可知，RFKD 隐私保护能力很理想，但是这一隐私保护优势是完全牺牲了缓存的内容分发能力。从图 7 可见，RFKD 策略下，除了少数最流行内容，其他内容类别的命中率几乎为零；从图 8 可见，随着 k_C 的增加，RFKD 隐私保护能力增强，网络总命中率同时相应下降，即采用 RFKD 策略，CCN 网络的



(a) $\alpha=1.2$



(b) $\alpha=0.8$

图 7 分类命中率（CPPS 与 RFKD）

缓存能力几乎无法体现，剥夺了缓存特征，CCN 网络也丧失了存在的理由。对于 CPPS-RVI&ECP，不管是分类还是总体网络命中率，都明显优于 RFKD 策略，且隐私类别的内容也具有一定的网络命中率。随着 p 的增加，CPPS-RVI&ECP 网络命中率相应提高，但即使仅取 p=0.2，也可获得较满意的网络命中性能。

需要说明的是，RFKD 总体网络命中率主要来自于第一类和第二类内容，在 $\alpha=1.2$ 时，由于内容请求集中第一类和第二类，这 2 类命中率较高，因此总体网络命中率 30%左右。

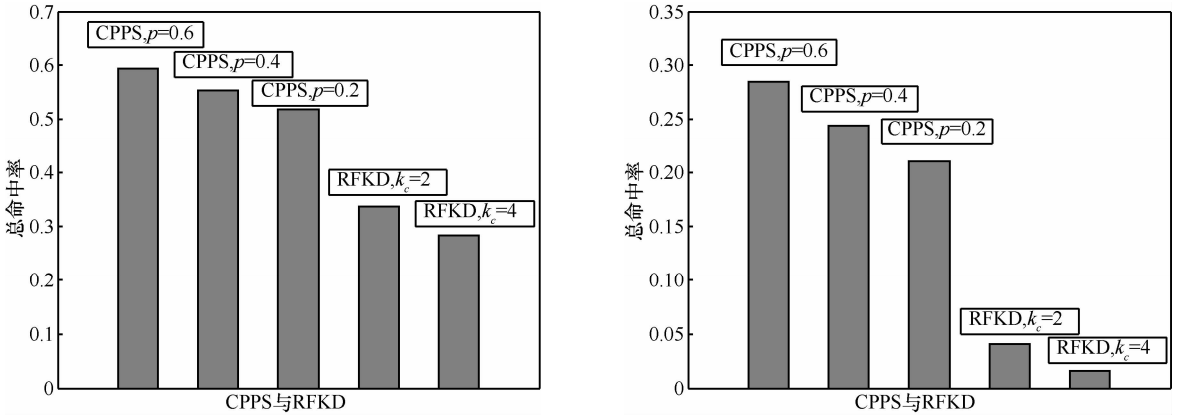
5.3　隐私保护策略比较

CCN 现有缓存隐私保护策略特性的综合比较如表 2 所示。其中，CSD、FFKD 和 RFKD 都是通过严重牺牲 CCN 的缓存能力而获得隐私保护的能力，其设计原则不符合 CCN 的网络特征；UCSR 和 FCUSR 部分沿用原有 IP 网络设计思路，仍需设置用户地址（用户名），以便准确识别请求来源，且需要网络设备维护大量信息，不适用于大规模网络；FCSR 采用接口来源识别，虽然降低了设备维护的信息量，但是隐私保护能力弱。本文提出的 CPPS 策略在保持较强缓存能力的前提下，具有较高的隐私保护性能，且实现难度不高，适于大规模网络应用。

6　结束语

本文兼顾 CCN 的缓存隐私保护与内容分发能力，提出一种基于最近访问信息与回退机制的缓存隐私保护策略，该策略通过设置隐私标识识别当前用户在最近时间内对该内容的请求行为；通过随机回退机制，使内容在网络中的停留时间模糊化，也改善网络的访问性能。设定实验条件进行数值分析，结果表明，虽然 RFKD 有理想的隐私保护能力，但是它是以完全牺牲缓存的内容分发能力为代价的，而本文提出的 CPPS 策略虽然隐私保护能力略弱于 RFKD，但通过合理设置回退概率，选取较小的 p 值，可以在保持较低隐私泄露率的同时，获得较高的网络命中率。

此外，本文设计的隐私保护策略，攻击者需要较准确估计出攻击目标在网络中的停留时间，才可



(a) $\alpha=1.2$　　(b) $\alpha=0.8$

图 8　网络总命中率（CPPS 与 RFKD）

表 2　　CCN 现有主要隐私保护策略对比

策略名称	隐私保护	缓存能力	来源识别	设备维护信息	实现难度
CSD	完美	无	无	无	易
FFKD	弱	差	无	固定延迟次数	易
RFKD	强	差	无	随机延迟次数	易
UCSR	完美	强	用户	用户访问状态	很难
FCSR	弱	强	接口	接口访问状态	中等
FCUSR	较强	强	用户+接口	用户+接口访问状态	难
CPPS	较强	较强	数据分组最近访问时间	缓存现有存储内容的访问时间	中等

能有效探测用户隐私。而通过随机位置置换以及设置回退概率，本文策略可保证隐私内容的网络停留时间具有较强随机性，攻击者有效实施攻击的难度较大。因此，从 CCN 安全性角度而言，本文策略的安全性较高，在现有各种策略中，其各个维度的特性表现均衡。

本文工作主要围绕缓存隐私保护策略本身开展讨论，接下来的工作是进一步研究如何检测缓存隐私探测行为，这方面主要考虑 CCN 缓存隐私探测具有一定的时域特征，可以通过该类特征进行直接或者变换域分析。此外，CCN 隐私安全性中，除了缓存隐私，还存在内容隐私泄露问题，关于 CCN 内容的隐私保护，也是未来的研究内容。

参考文献：

[1] KOPONEN T, CHAWLA M, GON C B, et al. A data-oriented (and beyond) network architecture[A]. Proceedings of the ACM SIGCOMM 2007 Conference[C]. Kyoto, Japan, 2007. 181-192.

[2] European Union. Project FP7 4WARD[EB/OL]. http://www.4ward-project.eu, 2010.

[3] European Union. Project PSIRP[EB/OL]. http://www.psirp.org, 2010.

[4] JACOBSON V, SMETTERS D K, THORNTON J D, et al. Networking named content[A]. Proceedings of the 5th International Conference on Emerging Networking Experiments and Technologies[C]. Rome, Italy, 2009. 1-12.

[5] VASILAKOS A V, LI Z, SIMON G, et al. Information centric network: research challenges and opportunities[J]. Journal of Network and Computer Applications, 2015, (52): 1-10.

[6] FOTIOU N, POLYZOS G C. ICN privacy and name based security[A]. Proceedings of the 1st International Conference on Information-Centric Networking[C]. ACM, 2014. 5-6.

[7] LAUINGER T. Security & Scalability of Content-Centric Networking[D]. TU Darmstadt, 2010.

[8] ACS G, CONTI M, GASTI P, et al. Cache privacy in named-data networking[A]. Distributed Computing Systems (ICDCS), 2013 IEEE 33rd International Conference[C]. IEEE, 2013. 41-51.

[9] CHAABANE A, DE CRISTOFARO E, KAAFAR M A, et al. Privacy in content-oriented networking: threats and countermeasures[J]. ACM SIGCOMM Computer Communication Review, 2013, 43(3): 25-33.

[10] MOHAISEN A, ZHANG X, SCHUCHARD M, et al. Protecting access privacy of cached contents in information centric networks[A]. Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications security[C]. ACM, 2013. 173-178.

[11] MOHAISEN A, MEKKY H, ZHANG X, et al. Timing attacks on access privacy in information centric networks and countermeasures[J]. IEEE Transactions on Dependable and Secure Computing, 2015 (online first).

[12] LAUINGER T, LAOUTARIS N, RODRIGUEZ P, et al. Privacy risks in named data networking: what is the cost of performance[J]. ACM SIGCOMM Computer Communication Review, 2012, 42(5): 54-57.

[13] ARIANFAR S, KOPONEN T, RAGHAVAN B, et al. On preserving privacy in content-oriented networks[A]. Proceedings of the ACM SIGCOMM Workshop on Information-Centric Networking[C]. ACM, 2011. 19-24.

[14] LAUINGER T, LAOUTARIS N, RODRIGUEZ P, et al. Privacy implications of ubiquitous caching in named data networking architectures[R]. Technical Report TR-iSecLab-0812-001, iSecLab, 2012.

[15] 葛国栋, 郭云飞, 刘彩霞, 等. 内容中心网络中面向隐私保护的协作缓存策略[J]. 电子与信息学报, 2015, 37(5):1220-1226.
GE G D, GUO Y F, LIU C X, et al. A collaborative caching strategy for privacy protection in content centric networking[J]. Journal of Electronics & In for motion Technology, 2015, 37(5):1220-1226.

[16] LAOUTARIS N, CHE H, STAVRAKAKIS I. The LCD interconnection of LRU caches and its analysis[J]. Performance Evaluation, 2006, 63(7): 609-634.

[17] CAROFIGLIO G, GALLO M, MUSCARIELLO L, et al. Modeling data transfer in content-centric networking (extended version)[EB/OL]. http://perso.rd.francetelecom.fr/muscariello, 2011.

[18] CAROFIGLIO G, GALLO M, MUSCARIELLO L. On the performance of bandwidth and storage sharing in information-centric networks[J]. Computer Networks: The International Journal of Computer and Telecommunications Networking, 2013, 57(17): 3743-3758.

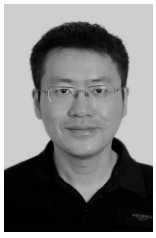
[19] WANG G, HUANG T, JIANG L I U, et al. Modeling in-network caching and bandwidth sharing performance in information-centric networking[J]. The Journal of China Universities of Posts and Telecommunications, 2013, 20(2): 99-105.

[20] WANG K, CHEN J, ZHOU H, et al. Modeling denial‐of‐service against pending interest table in named data networking[J]. International Journal of Communication Systems, 2014, 27(12): 4355-4368.

[21] MANGILI M, MARTIGNON F, PARABOSCHI S. A cache-aware mechanism to enforce confidentiality, trackability and access policy evolution in content-centric networks[J]. Computer Networks, 2015, (76): 126-145.

[22] FRICKER C, ROBERT P, ROBERTS J, et al. Impact of traffic mix on caching performance in a content-centric network[A]. Computer Communications Workshops (INFOCOM WKSHPS), 2012 IEEE Conference[C]. IEEE, 2012. 310-315.

作者简介：



朱轶（1977-），男，江苏镇江人，南京邮电大学博士生，江苏大学副教授，主要研究方向为下一代互联网架构、异构网络融合、绿色通信与网络仿真等。

糜正琨[通信作者]（1946-），男，浙江上虞人，南京邮电大学教授、博士生导师，主要研究方向为未来网络理论与技术、自组网络（SON）技术、异构网络集成及业务融合。E-mail: mizk@njupt.edu.cn。

王文磊（1966-），男，江苏南京人，博士，南京邮电大学教授，主要研究方向为未来互联网体系结构、云计算与网络虚拟化、绿色通信网和网络仿真等。