

Kad 点对点网络中最佳结点标识选取研究

孙宁青

(广西工业职业技术学院, 广西 南宁 530003)

摘 要: Kad 网络是一种主流的文件共享对等网络(即 P2P network), 不法信息在其上的传播导致对其进行网络监管的需求也与日俱增. Kad 网络中广泛使用的节点标识 Kad ID 存在“Kad ID 别名”问题, 即单个节点具有多个 Kad ID. 为解决这一问题, 设计实现 Kad 网络节点信息爬虫—Kcrawler, 并提出了最佳节点标识概念, 以获得实际 Kad 网络中节点的多个候选标识之间的对应关系信息. 实验结果表明 {userID} 的稳定因子最大, 是最佳节点标识.

关键词: P2P 网络; Kad 网络; 爬虫; 节点标识

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2011)08-0126-03

A Study on Selection of Peer Identification in Kad Network

SUN Ning-qing

(Guangxi Vocational & Technical Institute of Industry, Nanning 530003, China)

Abstract: Kad network has become a main kind of file-sharing Peer-to-Peer(P2P) network, leading to the increasing demand of censoring it. In order to accurately determine the censoring object, the problem of optimal peer identification will be put forward. This paper tries to solve this problem. Kad network peer information crawler is designed and implemented to crawl peer information of multiple candidate identifications' relationship in real Kad network. Experimental results show that {userID} is the optimal peer identification.

Key words: peer-to-peer network; Kad network; crawler; peer identification

1 引言

eMule 网络^[1-2]是一种混合类型的文件共享对等网络(P2P network). 一般来说, 采用 Kademlia 协议的 eMule 网络称为 Kad 网络.

据统计, 被广泛应用的 Kad 网络为版权侵犯和不健康内容传播提供了温床, 对其进行监管是很有必要的. 为了对它实施有效监管, 必须准确地确定监管对象. 在 Kad 网络中, 节点是被指定了一定标识(例如: IP 地址)加入到 Kad 网络的物理机器. Kad ID 是 Kad 网络中节点的一种标识, 它是一个 128 位的随机整数, 可以由用户任意指定. 在 Kad 网络中, Kad ID 被普遍用于标识一个节点, 但一个节点可能对应多个 Kad ID, 这就是 Kad ID 别名问题^[3], 不难发现, Kad ID 并不是 Kad 网络的最佳节点标识. 本文就是在这样的背景下, 采用网络测量和数学方法,

力求对 Kad 网络的最佳节点标识问题进行分析 and 解决, 从而可以更准确地确定监管对象.

2 Kad 网络最佳节点标识

Kad ID 别名问题的存在导致有寻找更好 Kad 网络标识的需求, 本节提出了最佳节点标识和候选标识正常度的概念.

定义 1 最佳节点标识

假设节点存在候选标识集合 $S = \{x_1, x_2, \dots, x_n\}$, $\exists a \in (2^S - \{\Phi\}) \forall b \in (2^S - \{\Phi\}) \rightarrow SF_a = \max(SF_b)$, 则是集合 S 中的最佳节点标识.

选出集合 S 的最佳节点标识后, 为了对最佳节点标识与候选标识的关系是否正常进行归一化度量, 提出了最佳节点标识—候选标识 P 关系度量: 候选标识正常度 (Candidate Identifier Normality, CIN) 的定义.

定义2 候选标识正常度

$$CIN = \frac{y_1}{\sum_{i=1}^n y_i \times i + \sum_{j=2}^m z_{1/j} \times j} \quad (1)$$

式中, y_i 为最佳节点标识与候选标识 P 的 1 对 i 关系的不同 P 的数量(例如: $i = 1$ 表示最佳节点标识与 P 的 1 对 1 关系, $i = 3$ 表示最佳节点标识与 P 的 1 对 3 关系); $z_{1/j}$ 为最佳节点标识与 P 的 j 对 1 关系的不同最佳节点标识的数量(例如: $j = 5$ 表示最佳节点标识与 P 的 5 对 1 关系)。

$CIN \in [0, 1]$ 则反映了 Kad 网络中最佳节点标识—候选标识 P 关系的正常度, CIN 越大说明最佳节点标识与候选标识的一一对应关系比率越高, 正常度越高; 反之, CIN 越小则说明最佳节点标识与候选标识的一对多关系或者多对一关系比率越高, 正常度越低。

3 Kad 网络爬虫

为了通过实验验证上述最佳节点标识的有效性, 我们设计了网络爬虫 Kcrawler, 以此来获得实际 Kad 网络中节点的多个候选标识关系信息。设计 Kad 网络爬虫的挑战是网络规模大和节点震荡带来的多个瞬态快照的堆叠现象, 为尽量减少节点震荡所带来的影响, 并使获得的节点信息具有良好的抽样随机性。设计了采用了独特的随机采集方式的爬虫, 即对 Kad 网络做随机探测, 不固定 k 位前缀, 且只采集部分节点信息。其优点有: 采集的节点规模可调(典型值为 $20 \times 10^3 \sim 100 \times 10^3$); 采集一次的时间适中(100×10^3 节点耗时约 100 s); 采集随机目标节点, 比区域采集获得的节点更具有代表性。缺点是不能获得全部节点信息。

Kcrawler 系统框架由三个模块: 节点采集器、节点信息收集器和写数据库模块组成。

Kcrawler 系统的工作流程如下, 通过模拟一个 Kad 网络正常节点(任意生成一个 Kad ID 作为本地的 Kad 网络标识), 加入 Kad 网络, 经过一段时间的稳定期后(例如加入网络大概 45 分钟后), 开始随机采集。进行如下三个阶段(分别对应系统框架的三个模块)的操作。

阶段1: UDP 节点采集阶段(节点采集器)

(1) 从本地维持的非平衡二叉树路由表中读取联系人信息到 `std::map` 中;

(2) UDP 发包线程遍历 `map`, 从中选取没有发过 UDP 包的联系人, 向其(IP: UdpPort)发送随机

生成的查询, 同时置 UDP 访问状态为已访问;

(3) 收到 UDP 回包后的处理。UDP 监听线程将对应一次查询的 UDP 回包中的联系人信息去重后放入 `std::map`;

(4) 转到(2)循环一直到爬到的最大节点数达到阈值为止;

阶段2: TCP 探测补充信息阶段(节点信息收集器)

(5) TCP 发包线程遍历 `map`, 试图和(IP: TcpPort)建立 TCP 连接并发送异步 Tcp hello 包以获取 `userID` 等信息;

(6) TCP hello 回包(可能不能和部分(IP: TcpPort)建立 TCP 连接, 从而没有 TCP 回包)后的处理。TCP 监听线程根据(IP: TcpPort)在 `map` 中查找对应的项, 置相应联系人的 `userID` 等为返回的值;

阶段3: 写数据库阶段(写数据库模块)

(7) 遍历 `map`, 将结果存入数据库的节点信息表 `PeerInfo`。

4 实验结果及分析

应用 Kcrawler 在如下配置的机器上进行了数据采集。硬件环境为: 4 核 Intel i3 处理器, 2.5 GHz 主频, 内存 32 GB, 网络带宽 1 000 Mb/s, 局域网环境。软件环境为: Windows Server 2008 Standard, SQL Server 2008。

表1对本文设计和实现的 Kcrawler 和当前的几个主要爬虫: Saroiu^[4], Cruiser^[5], D-Crawler^[6-8], 的采集性能进行了比较。Kcrawler 采集 2 万个节点, 平均耗时需时 18 s 左右, 仅消耗 2 Mb/s 左右的带宽, 就达到了近 1 200 节点/s 的采集性能。为了进一步加快数据采集速度, 我们让 Kcrawler 在两台机器(服务器和 PC 各一台)上持续运行了 7 天, 然后将数据库进行合并, 共进行了 280 次随机采集, `PeerInfo` 表共获得约 300 万条去重节点信息记录, 其中可以建立 TCP 连接节点信息记录有约 110 万条, 采集数据汇总见表 2。

表1 P2P 采集器性能比较

P2P Crawler	Crawl Duration	Crawled Peers	System Configuration
Saroiu	168hours	1.2×10^6	1PC
Cruiser	7minutes	1.3×10^6	7clients, 2 server
D-Crawler	13minutes	$1.5 \times 10^6 \sim 3 \times 10^6$	2clients, 1 server
Kcrawler	18seconds	20×10^3	1PC

在验证了 Kcrawler 的性能后, 我们选择了 {KadID}, {IP}, {userID}, {KadID, IP}, {IP, userID},

$\{\text{Kad ID}, \text{userID}\}$, $\{\text{Kad ID}, \text{IP}, \text{userID}\}$ 作为候选节点标识, 使用第 2 节所述的方法进行验证, 得到 $\{\text{userID}\}$ 为最佳节点标识。

表 2 采集数据

采集时间	7 day
随机采集次数	280
采集节点总数	3×10^6
可建立 TCP 连接节点信息记录数	1.1×10^6

$\{\text{userID}\}$ 做为最佳节点标识可以在如下场景中应用: Kad 网络的用户跟踪; Kad 网络用户行为分析等。本节为证明这点, 采用 Kcrawler 对 Kad 网络用户的共享文件信息进行了为期 7 天的探测, 共获得用户拥有的文件条数约 530 万条, 然后分别采用 $\{\text{KadID}\}$, $\{\text{IP}\}$, $\{\text{userID}\}$, $\{\text{Kad ID}, \text{IP}\}$, $\{\text{IP}, \text{userID}\}$, $\{\text{Kad ID}, \text{userID}\}$, $\{\text{Kad ID}, \text{IP}, \text{userID}\}$ 作为标识对用户所拥有的文件进行了统计, 实验结果如图 1 的“箱线图”所示。由图可见, $\{\text{userID}\}$ 在短期 (只有 7 天) 的测量中也能对应的最多的文件数量, 故采用 $\{\text{userID}\}$ 作为节点标识可以更准确地探测用户所拥有的文件情况。从而证明了 $\{\text{userID}\}$ 是集合 $\{\text{KadID}, \text{IP}, \text{userID}\}$ 中最佳的节点标识。

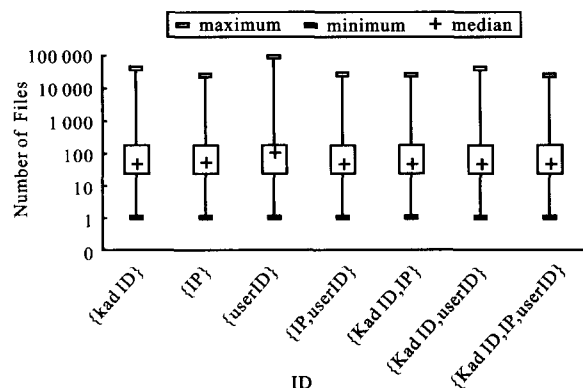


图 1 标识对应文件数量箱线图

5 结束语

本文设计并实现了采用随机采集方式的 Kad

网络节点信息爬虫: Kcrawler; 然后采集了实际 Kad 网络的候选标识: Kad ID, IP, userID 之间对应关系的节点信息, 通过计算和实验验证得出 $\{\text{userID}\}$ 是 Kad 网络的最佳节点标识, 为 Kad 网络的研究奠定了基础。Kad 网络的研究受到越来越多的关注, 更进一步的研究工作包括: Kad 网络共享内容的获取及其分类, Kad 网络完全拓扑图的采集等。

参考文献:

- [1] Merkur. eMule[EB/OL]. [2011-05-13]. <http://www.eMule-project.net>.
- [2] 彭凯, 邓天平. 基于市场机制的 P2P 流媒体网络节点选择算法研究[J]. 微电子学与计算机, 2009, 26(3): 97-101.
- [3] Steiner M, En-Najjary T, Biersack E W. Analyzing peer behavior in kad[R]. London: Institut Eurecom, 2007.
- [4] Subhabrata Sen, Oliver Spatscheck, Dongmei Wang. Accurate, scalable in-network identification of P2P traffic using application signatures[C]// WWW 2004. New York: ACM Press, 2004: 512-521.
- [5] Yoram Kulbak, Danny Bickson. The eMule protocol specification[R]. Israel: The Hebrew University of Jerusalem, 2005.
- [6] Saroiu S, Gummadi P K, Gribble S D. A measurement study of peer-to-peer file sharing systems[C]// Proc. of the Multimedia Computing and Networking (MMCN). London: IEEE Press, 2002.
- [7] Stutzbach D, Rejaie R, Sen S. Characterizing unstructured overlay topologies in modern P2P file-sharing systems[C]// Proc. of the 5th ACM SIGCOMM Conf. on Internet Measurement. Berkeley: ACM Press, 2005.
- [8] Stutzbach D, Rejaie R. Improving lookup performance over a widely-deployed DHT[C]// Proc. INFOCOM 2006. Barcelona: IEEE Press, 2006: 185-192.

作者简介:

孙宁青 男, (1963-), 副教授. 研究方向为计算机应用技术。

(上接第 125 页)

- [6] Stephen G Batsell, Nageswara S Rao, Mallikarjun Shankar. Distributed intrusion detection and attack containment for organizational cyber security[EB/OL]. [2011-05-22]. <http://www.ioc. oml. gov/projects/documents/containment. pdf>.
- [7] Adam Berger, Stephen Della Pietra, Vincent Della Pi-

etra. A maximum entropy approach to natural language processing[C]// Computational Linguistics. University of Amsterdam, Netherlands, 1996.

作者简介:

张焱 男, (1983-), 博士研究生. 研究方向为计算机网络、信息安全。