面向管控的 Mainline DHT 网络测量与分析方法研究

田志宏[1,2], 张信幸[2], 楼 芳[1], 刘 渊[1]

1(中国工程物理研究院 计算机应用研究所, 四川 绵阳 621900)
2(哈尔滨工业大学 计算机科学与技术学院, 黑龙江 哈尔滨 150001)

摘要 作为最具有代表性的 DHT 网络, Mainline DHT 网络凭借其用户数量庞大、分布地域广、运行稳定, 正成为国际上结构化 P2P 网络研究和应用的热点。但由于 Mainline DHT 的异构性和复杂性, 使得很难对其开展行之有效的管控手段。以面向有效管控的 Mainline DHT 网络测量分析为目标, 在深刻理解 Mainline DHT 网络文件查询过程等相关细节的基础上, 提出并设计了基于伪装节点发布、主动扩散和被动监听策略相结合的高效采集方法, 通过获取节点分布、热门种子文件分布、客户端类型和端口分布等实际数据, 测量并分析了 Mainline DHT 的网络性质和流量特征, 为特定目标、区域管控等精细化、细粒度管控手段提供数据支撑及指导依据。

关键词 Mainline DHT; 网络测量; 主动扩散; 被动监听; 网络管控
中图法分类号 TP393 DOI 号 10.19363/j.cnki.cn10-1380/tn.2017.04.003

A Measurement and Analysis Study on Mainline DHT Network for Management and Control

TIAN Zhihong[1,2], ZHANG Xinxing[2], LOU Fang[1], LIU Yuan[1]

1(Institute of Computer Application, Chinese Academy of Engineering Physics, Mianyang 621900, China)
2(College of Computer Science and Technology, Harbin Institute of Technology, Harbin 150001, China)

Abstract As the most representative DHT network, Mainline DHT network has become a hot spot in the research and application of structured P2P network in the world because of its large number of users, wide distribution and stable operation. However, due to the heterogeneity and complexity of Mainline DHT, it is difficult to carry out effective management and control measures. For the effective control of the Mainline DHT network measurement analysis, based on a deep understanding of Mainline DHT network file query process and other related details, proposed and designed efficient acquisition method combining based on node distribution, diffusion and camouflage active passive listening strategies, through the acquisition of node distribution, file distribution, client type hot seeds port and distribution of the actual data, measurement and analyze the network properties and flow characteristics of Mainline DHT, to provide data support and guidance for specific objectives, regional control fine, fine-grained control means.

Key words Mainline DHT, network measurement, active spread, passive monitoring, network control

1 引言

随着网络技术和计算机技术的快速融合, 基于互联网的应用呈现出爆炸式的发展态势。P2P(Peer to Peer, 对等网络)技术的相关研究在国内外获得了广泛关注。由于 P2P 节点具有不依赖中心节点而是依靠网络边缘节点, 实现自组织与对等协作的资源发现和共享的优点, 而被广泛应用于文件分享、即时通信、协同处理、流媒体通信等领域, 以分布式资源共享和并行传输的特点, 为用户提供了更多的资源、更高的可用带宽以及更好的服务质量。

P2P 系统的体系结构发展至今, 已经经历了从中心索引服务器结构, 到非结构化的覆盖网络, 直至结构化的覆盖网络 DHT(Distributed Hash Table)的

通讯作者: 田志宏, 博士, 研究员, 博士生导师 Email: tianzhihong@hit.edu.cn。
本课题得到国家自然科学基金(61572153)、中国工程物理研究院发展基金(2014A0403020, 2015A0403002)、国防基础科研项目(JCKY2016212C005)资助。
收稿日期: 2016-06-07; 修改日期: 2016-11-09; 定稿日期: 2017-03-07

演变。在这些不同的体系结构中, DHT 由于存在无需中心索引服务器、 查找速度快、 网络开销小等优点, 在实际的大规模的 P2P 应用程序中被广泛使用。其中, Mainline DHT(MLDHT)网络由于用户数量庞大、分布地域广、运行稳定, 成为最具有代表性的 DHT 网络。很多著名的 P2P 客户端如 BitComet、µTorrent、BitSpirit、LibTorrent、Monotorrent、迅雷以及 Transmission 等流行 P2P 软件都实现了对 MLDHT 的支持[1]。据 Palo Alto 机构 2014 年 1 月的研究数据表明, 目前的 P2P 文件下载流量中有超半数来自于 MLDHT 网络, 占据约 6%的网络带宽[2]。

基于 MLDHT 的各类应用系统迅猛普及和发展, 不仅造成网络资源巨大消耗并引起网络拥塞, 同时也正成为盗版资源、反动信息、淫秽色情等内容传播的沃土。但是由于 MLDHT 具有大规模性、异构性和复杂性, 使得很难对其开展行之有效的管控手段, 传统的封堵技术也只能使得用户满意度下降, 并影响一些合理应用。目前学术界的研究焦点更多地关注网络结构的控制优化、内容搜索和定位以及数据索引和发布策略等方面[3], 面向有效管控的 MLDHT 网络准确测量与分析研究工作却少有人开展, 通过获取其节点分布、热门种子文件分布、客户端类型和端口分布等实际数据, 有利于更加深刻地了解 MLDHT 网络性质和流量特征, 并可为后续有效开展疏堵结合的管控技术提供数据支撑及指导依据。

综上所述, 为全面地测量 MLDHT 网络流量特征, 在深刻理解 MLDHT 网络文件查询过程等相关细节的基础上, 我们设计并开发了高效的 MLDHT 爬虫系统 ZCrawler, 通过对采集到的数据进行了深入分析, 初步描绘出 MLDHT 的全局网络概貌, 并给出了一系列测量分析结果。

2 MLDHT 网络文件查询机制

近年来, 由于文件分享的版权问题得不到很好的解决, 著名的海盗湾网站被迫关闭, MLDHT 网络凭借无中心服务器节点、用户自行组织路由管理等先天优势, 正逐步成为结构化 P2P 网络的主流[4]。

MLDHT 网络中的每个节点都有一个称为 ID 的唯一身份标识, 其长度为 160 位, 节点间的逻辑距离为 ID 经过异或(⊕)运算后的结果, 其值越小表示距离越近, 假设存在节点 a = 1011 和 b = 0111, 则 a 和 b 之间的距离为|1011 ⊕ 0111|= 12。每个节点维持一个由<IP 地址, 端口, ID >构成的三维列表(称为 K-桶), MLDHT 网络的路由表由二叉树结构存储, 二叉树的每个叶节点为一个 K-桶, 在系统初始化的时候, 路由表中只含有根节点, 且此根节点就是叶子节点。当节点收到路由查找请求, 它能够很快根据要求查找的 ID 到对应的 K-桶中寻找合适的节点信息。MLDHT 网络支持四种查询消息:

1) PING: 探测节点是否在线。

2) FIND_NODE: 查找距离目标节点最近的 k 个邻居节点, 一般 k=8。

3) GET_PEERS: 用于查询某哈希值所对应的节点集。该请求包含节点 ID 和 infohash 两个参数, infohash 为种子文件的 SHA1 哈希值, 长度与节点 ID 同为 160bit。该请求首先计算路由表中节点 ID 和 infohash 的距离, 并向距离 infohash 最近的节点发送请求, 被请求节点如果有对应 infohash 值, 则返回相应节点信息, 否则, 回复其路由表中距离该 infohash 最接近的 k 个节点信息。

4) ANNOUNCE_PEER: 向其他节点宣告, 正在某端口提供种子文件下载。

假设 MLDHT 网络中有 A、B 和 C 三个节点, 如图 1 所示, A 节点存有哈希值为 53 的种子文件, 文件的哈希值以及对应的节点集在 B 节点保存, C 节点请求下载文件。

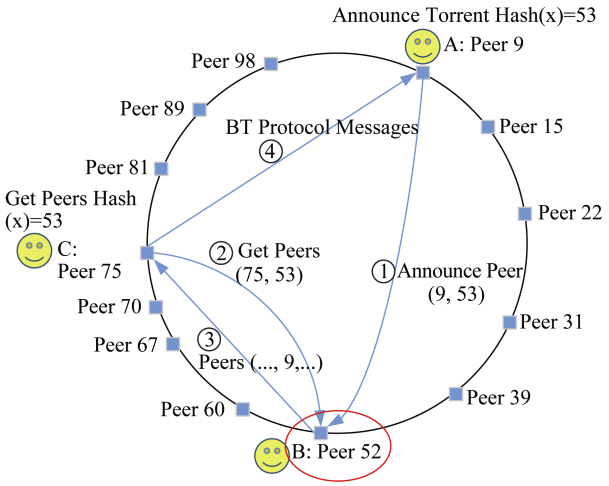

图 1 MLDHT 网络节点交互过程

首先, A 节点将文件哈希值存储到 B 节点并发布文件, 同时重复发送 GET_PEERS 消息来更多地获取 B 节点的近邻节点, 直到定位 B 节点。然后, A 节点发送 ANNOUNCE_PEER 消息给 B 节点, 通知它将共享该文件。B 节点将 A 节点的邻居节点信息存储于对应节点集中。

当 C 节点尝试下载该文件时, 需首先获取文件的哈希值, 并发送 GET_PEERS 消息定位 B 节点, 此时可能出现下述两种情况: 如被请求节点已知该哈希值, 且在对应节点集中存有节点信息, 则直接应

答该节点集; 如被请求节点不知该哈希值, 则将其路由表中距离该哈希值最近的几个节点应答给 C 节点。如此往复, 查询结果逐步逼近 B 节点, 直到最终定位 B 节点, 至此搜索结束, 接下来 C 节点和节点集中的节点建立连接关系, 开始文件下载过程。

3 ZCrawler 的设计与分析

ZCrawler 主要用于采集种子文件 infohash 和节点信息, 基于开源的 Transmission 客户端实现, 采用 C++编写, 总代码量 3 千余行。ZCrawler 的设计目标是: 对 MLDHT 网络的影响最小化、采集到的节点和种子文件数目最大化。

当前主流 DHT 网络爬虫工具大都为测量 DHT 网络结构而设计, 专职搜集 DHT 中的节点联系信息, 具体包括逻辑 ID、IP 地址以及 DHT 网络端口等。测量程序以基本的已知节点集合作为初始集, 通过主动测量的方式, 直接向其他节点不断发出路由查找请求得到更多节点信息[5]。而 ZCrawler 的设计初衷是面向有效管控的 MLDHT 网络测量与分析, 除节点信息之外, 还需兼顾种子文件的采集工作。

根据 MLDHT 网络查询机制可知, 节点通过在路由表中查找近邻节点的 ID, 并与种子文件的 infohash 进行距离对比, 最终完成文件定位。由此, 若 ZCrawler 构造大量伪装节点(Fake), 并设法污染其他 MLDHT 网络节点的路由表项, 使得其中含有 Fake 节点, 于是一旦其他网络节点发送 GET_PEERS 消息时, 只要 Fake 节点与查询目标的距离够近, ZCrawler 伪装的 Fake 节点就会收到该查询请求, 即可由此得到节点 ID 和种子文件 infohash。因此 ZCrawler 的核心设计思路是采取基于伪装节点发布、主动扩散和被动监听策略相结合的高效采集机制。

每个 Fake 节点均需要一个端口号进行通讯, 而单 IP 地址最多有 2^{16} 个端口, 因此 ZCrawler 在每个 IP 地址上构建 65535 个 Fake 节点。在 ID 生成策略方面, 为避免 ID 空间分配不均衡而导致的 GET_PEERS 消息分布抖动, ZCrawler 并未采用 Fake 节点 ID 的全随机分配策略。由于 MLDHT 网络使用异或距离, 意味着 ID 的高位越不相同, 节点间距离就越远, 因此 ZCrawler 将 160 位地址空间的高 15 位设置为 000..00 到 111..11, 而余下的 145 位设置为随机值, 这使得 Fake 节点在任何时刻均能覆盖整个地址空间, 且与任一 infohash 的距离都不会超过 2^{145}, 尽可能地保证很大几率收到更多的 GET_PEERS 请求。

ZCrawler 主要包含两个工作线程, 线程 1 负责执行主动扩散策略, 具体利用 FIND_NODE 消息, 将 Fake 节点快速传播出去。由于 ZCrawler 并不真正承担文件共享的职责, 因而无需维护节点路由表, 因此其效率将远高于 MLDHT 客户端。给定初始节点集($V_1 \cdots V_i$), ZCrawler 依次向每个初始节点发送查询消息, FIND_NODE(Fake, V_k), k=1…i。其中 Fake 为待扩散的伪装节点。根据 MLDHT 网络协议设定, 接收该查询的 V_k 节点会将 Fake 加入其路由表, 并返回路由表中与 Fake 最近的 8 个近邻节点, ZCrawler 则将接收到的近邻节点加入初始节点集, 持续递归执行上述查询操作。

随着主动扩散程度加深, Fake 节点将驻留在大量的 MLDHT 网络节点中, 一旦 MLDHT 网络节点需要执行下载任务, 就有一定概率向 Fake 节点发送请求消息, ZCrawler 的线程 2 执行被动监听策略, 具体负责应答接收到的请求: 若收到某节点 A 的 FIND_NODE 请求, 则按协议约定, 选择距离查询目标最近的 8 个 Fake 节点予以应答, 进一步污染 A 节点的路由表, 使 Fake 节点与被查询目标的距离更为接近, 增大 A 节点向 Fake 节点发送 GET_PEERS 请求的几率。若收到 GET_PEERS 请求, 则提取用户 IP、端口、infohash 以及请求时间等字段并存储, 以便后续分析使用。ZCrawler 的功能结构如下图所示。

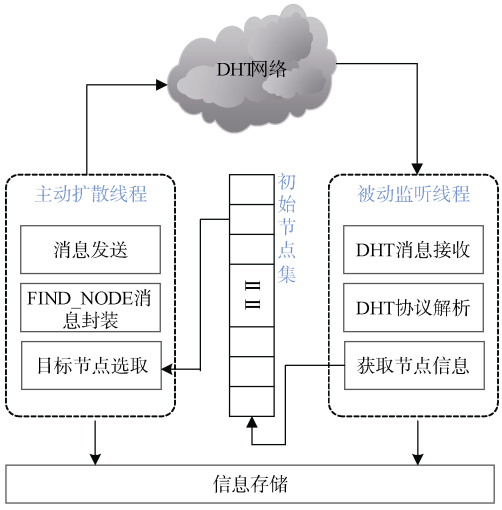

图 2 ZCrawler 功能结构图

4 MLDHT 网络测量结果分析

通过将 ZCrawler 部署在一台 Linode VPS 主机上(配置为: 1*CPU*2.83GHz、1G 内存、48GB 硬盘), 对全球 MLDHT 网络进行了为期 10 天的采集, 共采集到种子文件的 infohash 个数为 10,149,649, GET_PEERS 请求消息数量为 264,846,482; 共包含不同的 IP 地址数量为 28,666,196 条, 节点数量为

57,065,499 个, 分析结果如下。

4.1 ZCrawler 对 MLDHT 网络的影响分析

由于 ZCrawler 通过主动扩散策略向 MLDHT 网络中注入 Fake 节点, 但无节制的扩散势必对正常的网络通讯、查询响应时间等造成不可预估的影响, 因此, ZCrawler 采用限时限量的注入策略来保障主动扩散的稳定性, 期望不影响 MLDHT 网络的前提下, 尽可能多的采集到种子文件 infohash。在具体实现中, 每隔 10 秒, 轮询初始节点集, 向没有被回复过的节点再次发送 FIND_NODE 请求, 而当一个节点接受到超过一定数量(ZCrawler 设定为 8)的 GET_PEERS 消息后, 则永久停止针对该节点的主动扩散, 只执行被动监听动作。由图 3 给出的 ZCrawler 所爬取的种子文件 infohash 数的每日增长率曲线可知, 每小时平均增加消息数量约为千万量级。GET_PEERS 消息数每日增长率曲线如图 4 所示, 如图所示, GET_PEERS 消息数和 infohash 数保持了相同程度的变化率, GET_PEERS 消息数越多, 采集的种子文件 infohash 数也越大。第一天的增长率曲率非常明显, GET_PEERS 消息数量暴涨, 后面为使 MLDHT 网络的影响最小化, 采取限时限量注入的保障策略, 该曲线逐渐趋于收敛。

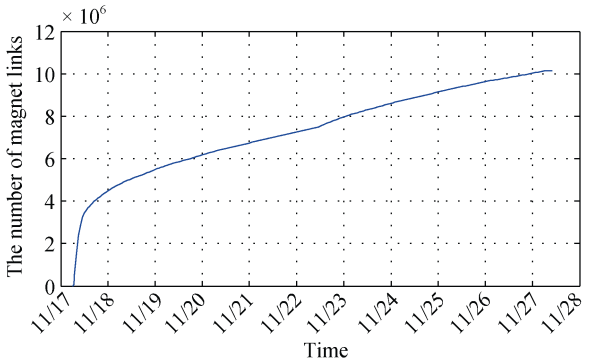

图 3 种子文件 infohash 数的每日增长率

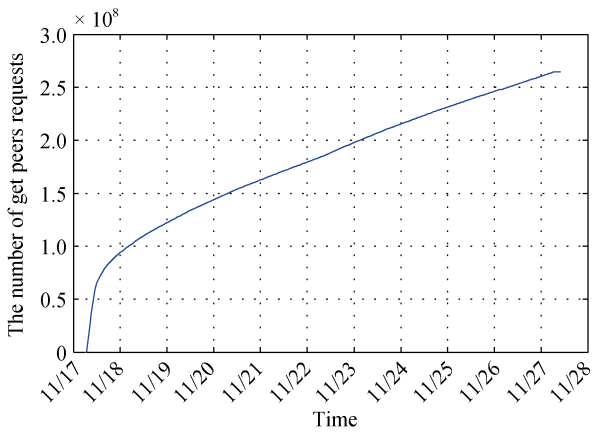

图 4 GET_PEERS 消息数的每日增长率

4.2 节点分布情况分析

如果能够描绘出 MLDHT 网络中节点的地理位置分布、热门种子文件的国家和地区分布以及各大洲的下载热度情况, 可以很好地为有关管理部门针对 MLDHT 网络作区域管控方案提供数据支撑和决策依据。为此, ZCrawler 利用 GeoIP[6]将所采集节点的 IP 地址自动转换为地理位置, 并依据文献[7]定位出城市代码列表。通过分析得出了图 5 所示的 247 个不同国家或地区的节点分布。根据节点的地理位置分布情况, ZCrawler 选取了前 20 个用户量最多的国家或地区, 来自欧洲或者亚洲国家或地区共有 7 个, 其中俄罗斯和中国大陆在 MLDHT 网络中起着关键性的作用, 其用户数量占比为总量的 35%。

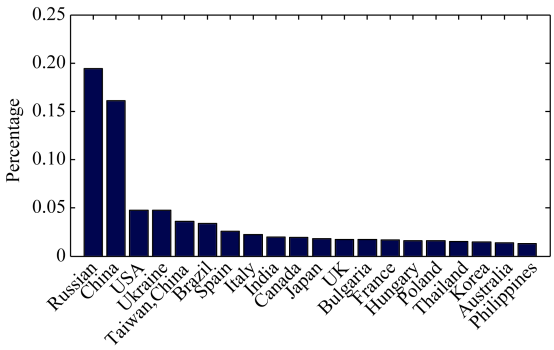

图 5 MLDHT 节点数最多的 TOP20 国家和地区分布

参照各国因特网用户数目, 图 6 描绘了 MLDHT 网络中各国家或地区用户与因特网用户的占比关系, 不难看出, MLDHT 在东欧非常流行, 占比为 40%, 其主要原因是客户端 Zona 在俄罗斯应用十分普遍而导致。另一个有趣的发现是, 图中有 9 个国家或地区的因特网用户数少于 100 万, 但其 MLDHT 所占比重却很高,明显的是保加利亚和梵蒂冈, 其总因特网用户数分别为 758 万和 480 万, 但 MLDHT 节点却分别

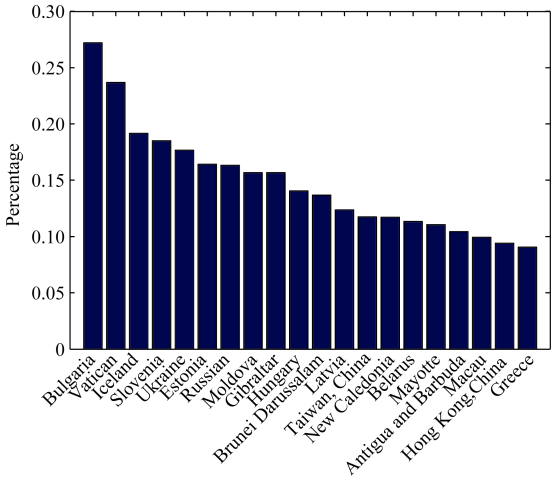

图 6 MLDHT 使用率最高的 TOP20 国家和地区分布

高达 190 万和 109 万, 由此表明, 即使在人口稀疏的地区, MLDHT 网络也十分流行。

参考文献[8], 将世界划分为六个大区: 非洲, 亚洲, 欧洲, 中东, 南美洲与大洋洲。各大区的的 MLDHT 用户分布情况在图 7 中展示, 在 MLDHT 用户数量上, 欧洲和亚洲占绝对优势, 共占 81.8%。图 8 给出了各大区 MLDHT 用户占因特网用户的比例, 从而反映出各大区的 MLDHT 使用热度, 在大洋洲和欧洲占比为 5%和 3.5%, MLDHT 的使用更为流行。这与实际情况一致, 欧洲拥有大量 MLDHT 节点, 且具有高使用比例; 大洋洲由于总体因特网用户数量基数较小, 但 MLDHT 用户比例很高, 占比 3.5%, 而亚洲则降到了第三位。

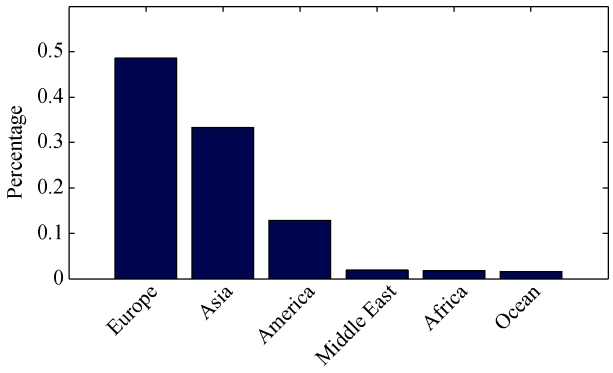

图 7 各大区的 MLDHT 用户分布情况

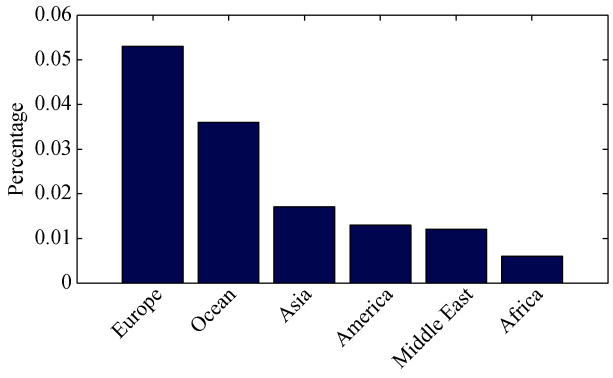

图 8 各大区 MLDHT 使用热度

4.3 客户端与端口分布情况

对 MLDHT 网络实施精细化管控, 需要全面了解其上承载的各种客户端及所使用端口的使用分布情况。GET_PEERS 消息中的字段“V”是 MLDHT 网络中客户端类型的唯一标识[9], 主流客户端如 µTorrent、LibTorrent 和 Monotorrent 等均予以支持。ZCrawler 采集到的数据中共包含 18 个不同类型客户端, 通过统计分析, 给出了如图 9 所示的客户端分布情况。其中使用µtorrent 客户端的占比超过半数, 共计 20,91,798 个节点, LibTorrent、Monotorrent 等客户端占比为 10%。而迅雷, BitComet 及 Zona 由于未设置“V”字段, 总占比约为 40%。

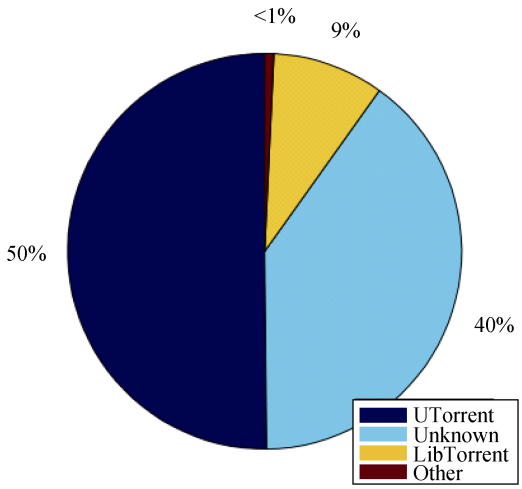

图 9 客户端使用分布情况

图 10 给出了 MLDHT 网络中端口分布情况, 16001(占比 4.5%), 49001(占比 3.4%)和 6881(占比 1%)是应用最广泛的端口号。其中, 16001、49001 分别是迅雷客户端和 Vuze 客户端的默认端口, 迅雷用户数量庞大, 这与我们的普遍认识一致。除了上述几个占比较高的端口之外, 剩余 91%的 MLDHT 节点大都使用随机端口, 其中µTorrent 客户端占据较大比例, 主要是由于µTorrent 客户端为防止运营商通过端口封堵, 而采取动态随机端口策略。

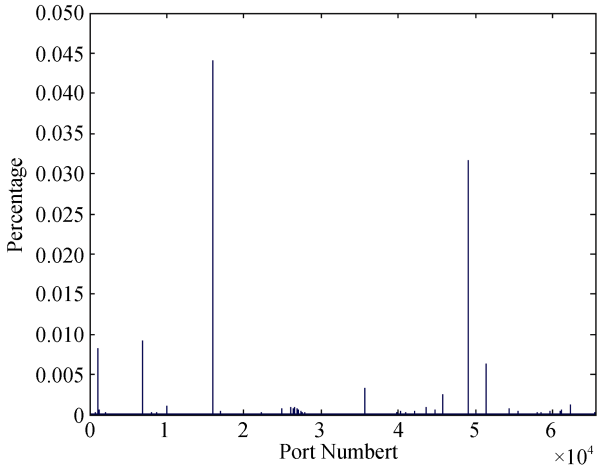

图 10 端口号使用分布情况

4.4 种子文件 infohash 分布情况

通过对种子文件的下载情况以及热度分析, 能直观地掌握当前网民文件下载趋势, 可进一步为特

定目标管控提供指导依据。定义种子文件 infohash 最长请求间隔为第一次和最后一次请求的时间差值。文件 infohash 最长请求间隔和请求数之间的对应关系如图 11 所示。不难看出, 文件 infohash 最长请求间隔越长, 其收到的请求数越多; 但是由于一些冷门种子的存在, 有节点会在不同的时间范围内对该种子文件进行反复请求尝试, 由此导致有些文件 infohash 尽管拥有较长的最长请求间隔, 收到的请求数却较少。

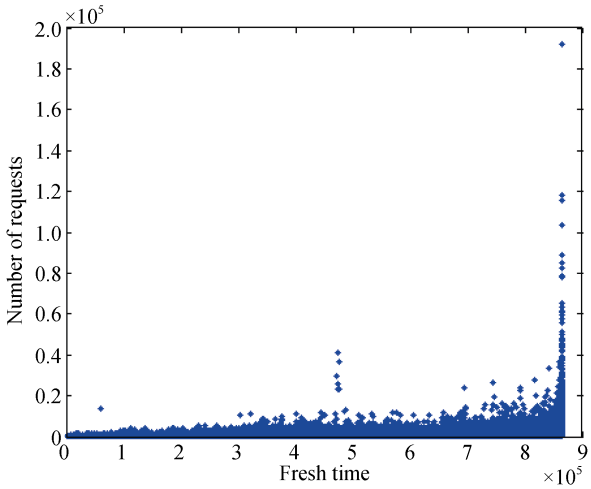

图 11 种子文件 infohash 最长请求间隔与请求数的关系

图 12 对每个文件 infohash 拥有的 MLDHT 节点数作了统计, 显然, 各 infohash 所拥有的 MLDHT 节点数大致符合 Zipf 分布, 约 11%的 infohash 占据了 95%的 MLDHT 节点, 约 46%的 infohash 只拥有一个 MLDHT 节点。

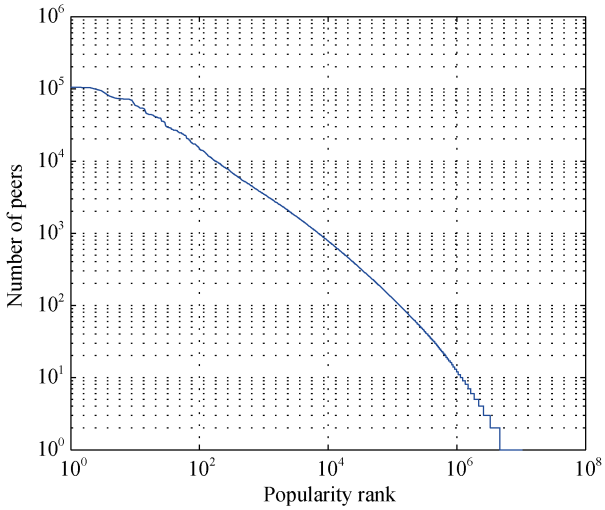

图 12 种子文件 infohash 对应的节点数分布

表 1 列出热度最高种子文件 infohash 的 TOP 10, 其中有 9 个属于 Zona 客户端, 由于 Zona 在东欧非常流行, 与前面的实验结论相互印证。

表 1 最热门的十个种子文件 infohash

种子文件 infohash	节点数	文件名	类型
2CCCE31684E7847A7A760B13653AD19104FB8D19	105159	zplayerswt_0.0.0.7.zip	Zona
CB70B29CD858B9C62ADE092CCC9D6A1909C48A6C	103922	zhtml_0.0.5.1.zip	Zona
2B377A244BC15837FEDB3C988D83EFF90214B423	93624	zplayerswt_0.0.0.7.zip	Zona
E1FAD8AD30C38A42A151B8C39215BE2BE4D7D264	79401	Zona1.0.3.2.jar	Zona
01CA132405BD9CD933D671939299DADF2A950EA9	73492	zplayerswt_0.0.0.6.zip	Zona
02DDA7BC8AF2922E154D3FA976B6426ABFF698C0	72894	update.exe	torrent
31705451C8F325D02AB0EB71CB63844C10B57D14	71924	zhtml_0.0.4.6.zip	Zona
A487016A73DA990480BDE5BBD7677E80A3CD0A4C	71255	zhtml_0.0.5.0.zip	Zona
0BC225789DBB5B0B74D3E2F94F31AC006C731FA0	68416	Zona1.0.3.0.jar	Zona
2EC4D16D55EB26CC10D97A428D0BD6D1B8646227	58554	zhtml_0.0.4.8.zip	Zona

4.5 infohash 转换效率测试

虽然 P2P 文件下载过程目前仅能通过流量控制或端口阻断来实施管控, 但 torrent 种子文件下载环节却可为细粒度管控 MLDHT 网络提供有利条件, 即通过阻断 torrent 文件下载过程, 间接达到阻止 P2P 文件下载的目的。ZCrawler 依靠发布伪装 Fake 节点采集到大量的种子文件 infohash, 接下来需要将 infohash 转换为种子文件 torrent, 方可执行真正的 P2P 文件下载过程。在 MLDHT 中, 通过种子文件 infohash 下载 torrent 文件的具体方式有两种: 一是借助第三方种子缓存网站(如 magnet.vuze.com、bt.box.n8080.com 等)提供的服务; 二是通过 PEX 协议(Peer-Exchange Protocol)进行转换。研究并分析 torrent 种子文件下载环节使得对 MLDHT 网络执行细粒度管控更有针对性。

ZCrawler 分别针对上述两种方式实现了 infohash 向 torrent 文件自动批量转换的功能模块, 对于第一种方式, ZCrawler 选取 5 个用户规模最大的种

子缓存网站(zoink.it、magnet.vuze.com、torrage.com、torcache.net 和 bt.box.n8080.com)作为测试目标。公平起见, ZCrawler 采用交叉验证方式, 种子文件 infohash 随机分为 5 组, 每组包含 200 个, 分别将五组同时提交给各种子缓存网站进行转换, 转换率如图 13 所示, 五个网站的平均转换率为 46.9%, 相比之下, magnet.vuze.com 转换率最高, 约为 41.5%, torcache.net 转换率最低。

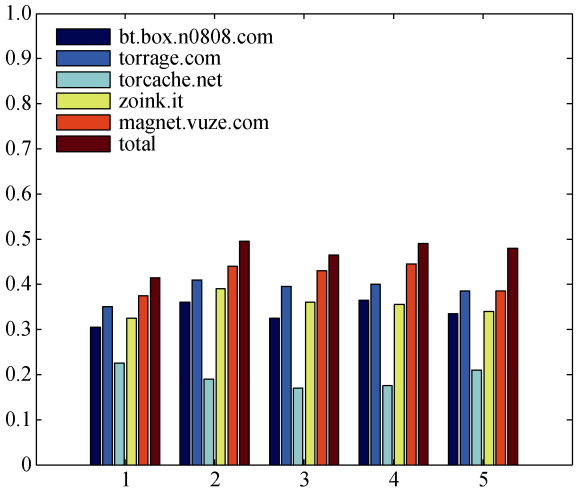

图 13 种子缓存网站转换率

将上述 5 组 infohash 分别用 PEX 协议进行自动转换, 平均转换率仅为 22.7%。此外, 用 PEX 协议自动转换过程中, 由于 MLDHT 网络节点查找产生一定时间损耗, 该方法较之于种子缓存网站的转换速度也略慢。根据文献[10]可知, 有 65%的节点都由于处于 NAT 或者防火墙之后而不能被连接, 这可能是导致 PEX 协议转换率低下的主要原因。

5 相关研究工作

DHT 网络测量与分析是当前的热点研究领域, 是进行协议设计、搜索优化等方面的基础, 许多工作面向改善 DHT 网络性能, 开展可用性测量等相关研究。当前, 基于 Kademlia 协议实现的 MLDHT、Kad 和 Vuze 是全球处于实用状态的最大的三个 DHT 网络[11]。

2009 年, 在世界最大的种子服务器海盗湾 Pirate Bay 被关闭之前, 文献[12]针对 Pirate Bay 所采集到的 460 万个种子文件进行了分析, 统计了用户地理分布情况和客户端类型的流行度, 但他们的研究具有一定局限性, 主要体现在数据采集方式不够合理, 当海盗湾被关闭之后, 其分析方法也就失去了数据源的支撑, 此外, 该分析针对英文版客户端, 从本文研究可知: 俄罗斯、中国等非英语地区也存在大量用户。

在 DHT 网络可用性研究方面, 有学者对 Vuze 和 Kad 网络进行了测量分析。文献[13]基于 Vuze DHT 网络实现了 Blizzard 爬虫系统, Blizzard 统计了 Vuze 客户端的版本分布、地理分布以及 IP 地址、端口分布等。文献[14]则设计了名为 ClearView 的 Vuze DHT 网络爬虫系统, ClearView 在 16 天内采集了超过 100 万个种子文件 infohash, 追踪到 790 万个不同 IP 地址的用户。但 ClearView 的采集仅能覆盖一定范围的节点, 而不是整个 ID 空间。文献[15]设计了一个适用于 Kad 网的 DHT 分析框架, 并因此提出了一些对 Kad 的改进建议, 为分析节点的搜索情况, 在框架中使用了爬虫来获取节点的路由表信息, 该爬虫基于路由表查询, 通过已知节点集, 并使用迭代式的方式来进行数据搜集。文献[16]和[17]的研究侧重 MLDHT 网络的安全性评估, 提出了一种向分布式系统 BitTorrent 中引入多个恶意构造的节点的攻击方法, 以达到控制整个覆盖网的目的, 该攻击可以被用于监控发布和搜索流量、隔离特定共享内容等, ZCrawler 的主动扩散策略借鉴了上述恶意节点的构造方法。文献[18]提出了一种基于抽样的 MLDHT 网络活跃用户的高效评估方法, 同时还指出了开源库 *libtorrent* 在爬取性能方面的不足, 与之相比, ZCrawler 侧重的测量维度更多, 但在 ZCrawler 的程序设计过程中借鉴了文献[18]所提出的一些提高爬取性能的思想, 例如: 去掉影响采集性能的校验(畸形包检查、可疑节点屏蔽等)、路由表查找等操作, 大幅度降低了数据处理开销, 提升了采集性能。

在 DHT 网络可控性方面研究较少, ZCrawler 面向有效管控, 通过获取其节点分布、热门种子文件分布、客户端类型和端口分布等实际数据, 给出 MLDHT 网络准确测量与分析。与前述方法相比, ZCrawler 的优势体现在: 1)基于伪装节点发布的设计思路决定了 ZCrawler 不再依赖路由表来查询节点信息, 提高采集效率; 2)ZCrawler 的节点 ID 选取策略具有空间全覆盖、均匀扩散的优点, 可在单台主机上完成, 对资源要求不高; 3)主动扩散和被动监听策略相结合, 在两个阶段分别利用 FIND_NODE 和 GET_PEERS 消息相互配合, 实现了节点 ID 和 infohash 的高效采集; 4)除节点信息之外, ZCrawler 还兼顾种子文件的采集工作, 对用户、地址、端口、infohash 的特性等方面都做了更为深入全面的统计和分析。

6 结论

以面向有效管控的 MLDHT 网络准确测量分析

为目标, 在深刻理解 MLDHT 网络文件查询过程等相关细节的基础上, 本文提出并设计了基于伪装节点发布、主动扩散和被动监听策略相结合的高效采集方法, ZCrawler 共接收到了来自全球 247 个不同国家与地区的节点, 发现中国和俄罗斯占用约 35%的 MLDHT 用户, 对 MLDHT 网络有非常大的贡献, 同时, 欧洲有 50%的因特网用户在使用 MLDHT 网络。还有一个有趣的趋势是 MLDHT 网络在人口稀疏的地区更加流行, 如保加利亚和梵蒂冈, 分别有大约 25%和 23%的用户使用 DHT 网络, 但他们的互联网人口仅分别为 758 万和 480 万。在 infohash 转换效率测试方面, ZCrawler 测试了两种方式将 infohash 转换为种子文件的效率, 并分析了造成转换率低的可能相关影响因素。接下来的工作重点将聚焦于 ZCrawler 的设计和优化, 设计网络测量部署模型, 实现部署代价和维护代价最小化, 并使得对网络的影响尽可能地小, 此外, 还将深入研究注入 Fake 节点的数量对于整个 MLDHT 网络在查询时间方面的影响程度, 并依此来获得 ZCrawler 在采集效果和网络影响之间的最佳平衡点。

致谢 衷心感谢各位评审专家对本文提出的宝贵意见。

参考文献

[1] R.Saunders, J.Cho, A.Banerjee, F.Rocha and J.V.Merwe, “P2P Offloading in Mobile Networks using SDN,” in Proc. the Symposium on SDN Research (SOSR '16), pp.34-48, 2016.

[2] A.Banerjee, J.Cho, E.Eide, J.Duerig, B.Nguyen, and R.Ricci, “Phantomnet: Research infrastructure for mobile networking, cloud computing and software-defined networking,” Mobile Computing and Communications, vol. 19, no. 2, pp. 28–33, 2015.

[3] M. Varvello and M. Steiner, “Traffic localization for dht-based bittorrent networks,” in Proc. 10th International IFIP TC 6 Networking Conference. Valencia, pp.40-53, May 2011.

[4] R.Tietzmann and L.G.Furini, “Sharing without laws: an exploration of social practices and ad hoc labeling standards in online movie piracy,” Internet Policy Review, Vol.5, no. 2, June 2016.

[5] A.Malatras, “State-of-the-art survey on P2P overlay networks in pervasive computing environments,” Journal of Network and Computer Applications, Vol.55, no. 2, pp.1–23, September 2015.

[6] Y. Lee, H. Park, Y. Lee, “IP Geolocation with a Crowd-sourcing Broadband Performance Tool,” Acm Sigcomm Computer Communication Review, Vol.46, no. 1, pp.12-20, 2016

[7] “ISO 3166 Country Codes,” MaxMind, Inc. http://dev.maxmind.com/geoip/legacy/codes/iso3166, 2016.

[8] “Internet World Stats Usage and Population Statistics,” http://www.internetworldstats.com/stats.htm, 2016.

[9] M. Scanlon, J. Farina, M. T. Kechadi, “Network investigation methodology for BitTorrent Sync: A Peer-to-Peer based file synchronisation service,” Computers & Security, Vol.54, pp.27-43, August 2015.

[10] R. Jimenez, F. Osmani, and B. Knutsson, “Connectivity properties of Mainline BitTorrent DHT nodes,” in Proc. 9th International Conference on Peer-to-Peer Computing, Seattle, Washington, USA, pp.9-17, 2010.

[11] S. Wolchok and J. A. Halderman, “Crawling BitTorrent DHTs for fun and profit,” in Proc. of the 4th USENIX conference on Offensive technologies. Washington pp.1-8, August 2010.

[12] “The Pirate Bay Tracker Shuts Down for Good, ” http://torrentfreak.com/the-pirate-bay-tracker-shuts-down-for-good-091117, NOVEMBER, 2009.

[13] C.Zhang, P.Dhungel, D.Wu, K.W.Ross, “Unraveling the BitTorrent Ecosystem,” IEEE Transactions on Parallel and Distributed Systems, Vol.22, no.7, pp.1164-1177, July 2011.

[14] S. Wolchok, O.S. Hofmann, N. Heninger, E.W. Felten, J.A. Halderman, C.J. Rossbach, B. Waters and E. Witchel, “Defeating Vanish with Low-Cost Sybil Attacks against Large DHTs,” in Proc. 17th Network and Distributed System Security Symp. (NDSS), SanDiego, pp.1-20, January 2010.

[15] P.Danielis, J.Skodzik, V.Altmann and L.Lender, “Dynamic search tolerance at runtime for lookup determinism in the DHT-based P2P network Kad,” in Proc. Consumer Communications and Networking Conference (CCNC), pp.9-12 Jan. 2015.

[16] J. Timpanaro, T. Cholez, I. Chrisment, and O. Festor, “Bittorrent's mainline dht security assessment,” in IFIP International Conference on NTMS, pp.1-5, Feb. 2011.

[17] I. S. Garcia, “Exploring Mainline DHT: an experimental approach [Master thesis] ,” KTH Royal Institute of Technology, Swedish, November 2010.

[18] L.Wang and J.Kangasharju, “Measuring large-scale distributed systems: case of bittorrent mainline DHT,” in Proc. 13th International Conference on P2P, pp.1-10, Helsinki, 2013.

田志宏 于 2006 年在哈尔滨工业大学计算机科学与技术专业获得博士学位。现任中国工程物理研究院计算机应用研究所研究员。研究领域为计算机网络与信息安全。研究兴趣包括: 计算机取证、主动防御。Email: tianzhihong@hit.edu.cn

张信幸 于 2014 年在哈尔滨工业大学计算机科学与技术专业获得硕士学位。现在百度在线网络技术有限公司任研发工程师。研究领域为计算机网络与信息安全。Email: zxx_hit@163.com

刘渊 于 2000 年在中国工程物理研究院研究生部计算机应用专业获得硕士学位。现任中国工程物理研究院计算机应用研究所研究员。研究领域为计算机网络与信息安全。研究兴趣包括: 入侵检测、网电对抗。Email: lyisme@caep.cn

楼芳 于 2007 年在四川大学计算机应用专业获得硕士学位。现任中国工程物理研究院计算机应用研究所高级工程师。研究领域为计算机网络与信息安全。研究兴趣包括: 网络评估、内网威胁。Email: louf108@caep.cn