基于会话的局域网P2P流量识别方法的研究

宫 博,王汝传
(南京邮电大学 计算机学院,江苏 南京 210003)

摘 要:随着P2P技术的发展,很多P2P软件采用了新的技术改善局域网用户的传输质量,导致P2P数据传输中出现了新的特征。针对STUN协议,在多元分类的基础上,提出了一种基于会话的P2P流量识别算法。首先介绍了STUN协议建立会话的消息格式,并描述了几种不同类型NAT建立地址映射的过程。算法采用多元组描述会话,建立二叉树结构对收发的数据包依次进行分析,识别P2P会话,最后以哈希表存储会话状态。在Linux环境下,以迅雷为例进行实验,结果表明采用本算法可以很好地识别P2P数据流。

关键词:识别;P2P;会话;NAT;STUN
中图分类号:TP301 **文献标识码**:A **文章编号**:1673-629X(2010)03-0005-04

Research on Method of Session-Based P2P Network Traffic Identification

GONG Bo, WANG Ru-chuan
(College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract: With the development of P2P technology, a lot of P2P applications introduced new technology to improve the transmission quality of the local area network, leading P2P data transmission in the emergence of new features. Presents a P2P identification algorithm based on session behavior characterization which targets STUN by multiple classification analysis. Firstly, STUN packet format for establishing a session is included to illustrate how all kinds of NATs acquire mapped address. Algorithm uses multi-group description of the session, the establishment of a binary tree structure on the analysis of data packets sent and received to identify P2P session, and uses the hash table to store session state. Finally, in Linux circumstance, many experiments on thunder are processed. The experiment results indicate that the algorithm can identify P2P traffic perfectly.

Key words: identification; P2P; session; NAT; STUN

0 引 言

近年来,由于文件共享类P2P软件的普及,大量网络带宽被占用,甚至产生网络拥塞,影响其他互联网业务的性能,运营商、企业网、学校等机构均受到这一问题不同程度上的困扰。高效并准确的识别和控制P2P流量是急待解决的问题。由于P2P软件的发展,早期一些简单的针对端口,IP地址进行测封的方式已经失效[1,2]。现有的应用方案大多基于P2P数据流的载荷分析,根据P2P协议特征库对应用层数据进行比较识别[3~5],但这种方式不可避免地要对用户数据进行扫描,有可能侵犯私人信息;更为重要的是,越来越多的P2P采取可变协议,数据包加密等方式传输数据,所以这种方式的局限性愈发明显。

各种网络环境受P2P数据流的影响程度并不相同,主干网设备完善,整流能力较强,产生拥塞的可能性很小。P2P数据流的冲击主要表现在末端子网内[6],出口转换点带宽的争用,比如企业网、校园网、住宅小区宽带等局域网产生的大流量P2P数据,不光造成局域网内拥塞,也会抢占子网内其他节点大量带宽,对电信运营商的业务产生严重影响。对上述这些局域网的P2P流量进行适当的控制,可以从很大程度上疏通整个网络性能的瓶颈,并减轻主干网的压力。

绝大多数局域网环境都使用了NAT设备[7],P2P

收稿日期:2009-07-20;**修回日期**:2009-10-12
基金项目:国家自然科学基金(60773041);江苏省自然科学基金(BK2008451);国家高科技863项目(2007AA01 Z404,2007AA01Z478);2006江苏省软件专项;南京市高科技项目(2007软资127);现代通信国家重点实验室基金(9140C1105040805);江苏高校科技创新计划项目(CX08B-085Z,CX08B-086Z);江苏省六大高峰人才项目
作者简介:宫 博(1981-),男,山东烟台人,硕士研究生,研究方向为基于网络的计算机软件应用技术;王汝传,博士生导师,研究方向为计算机软件、计算机通信、信息安全、无线传感器网络、移动Agent技术等。

软件传输数据，必然会通过 NAT 设备将私有地址映射到公网，文中针对 STUN 协议(RFC3489)所描述的四种 NAT[8]，分析它们传输 P2P 数据时的会话特征，在多元网络流量分类方式的基础上[9]，提出了一种基于会话的 P2P 流量识别算法。

1 STUN 协议

Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)，即 STUN，是为了实现透明的穿透 NAT，而定义的一套协议。它使处于内网中的主机具有取得能够得知它的 NAT 网关的 IP、NAT 类型的能力。STUN 协议将 NAT 分为四种类型：

I 完全透明 NAT(Full Cone NAT)：从相同的主机端口发出的数据都映射为同一个的 IP 和端口发往外网的目标主机端口，并且可以将外网其他主机发送给该映射后端口的数据转发给内网主机。

II 受限 NAT(Restricted Cone)：从相同的主机端口发出的数据都映射为同一个的 IP 和端口发往外网的目标主机端口，从目标主机任何端口发送给该映射后端口的数据都会转发给内网主机。

III 端口受限 NAT(Port Restricted Cone)：从相同的主机端口发出的数据都映射为同一个的 IP 和端口发往外网的目标主机端口，并且可以将目标主机端口发送给该映射后端口的数据交给内网主机。

IV 对称 NAT(Symmetric NAT)：数据包从同一个内网地址和端口发出，并且是同一个外网目标地址和端口，则将它们映射成同一个外部地址和端口；如果数据包从同一个内部地址和端口发送到不同外部目标地址和端口，则 NAT 将使用不同的映射，转换成不同的映射端口。

出于网络安全的考虑，除了 Full Cone NAT，必须先收到由内部地址发送的数据包的外部地址，才能通过 NAT 映射后的地址向该内部地址发送数据，即连接必须由内部地址发起。根据 STUN 协议的描述，除了 Symmetric NAT，内网中的主机都可以利用映射后的地址和端口，与其他主机进行双向连接，任何外网的主机只要将数据包发送到映射后的地址和端口，就可以被转发到内网主机上。而对于 Symmetric NAT 连接只能内部主机发起，因此这种 NAT 设备后的主机，只能与具备公网 IP 的主机进行通信，从理论上分析，减少了端对端的数量，可以减少 P2P 数据量；但实际上，具备高带宽数据发布的主机绝大多数是公网 IP，Symmetric NAT 只是过滤了传输能力较弱的内网主机，主干流量仍然存在，比如迅雷所采用的 P2SP 技术，可以汇集公网上具备资源的服务器提供给用户进行多点下载。

2 基于会话的 P2P 识别方法

为了描述 NAT 两侧主机间的关系，将源地址、端口，映射后的地址、端口与任一外网主机的地址和端口形成的组合称为一条会话，所有会话形成的集合称为会话集。定义表征会话的向量：

D(SA, SP, MA, MP, DA, DP, TL, TU)，其中：

SA：表示源 IP 地址

SP：表示源端口

MA：表示 NAT 映射后的 IP 地址

MP：表示 NAT 映射后的端口

DA：表示目的地址

DP：表示目的端口

TL：上一个数据包到来时间

TU：会话空闲时间

将描述会话集的向量矩阵进行适当的变换：将 SA 相同的向量放在一起，P2P 数据流表现出来的是长时间的一对多关系，即出现大量 SA 相同而(DA, DP)不同的会话；其他应用，比如 IE 浏览器同时打开数个网页，在某个较短的时间范围内也可能表现类似特征，但其与 P2P 数据流的区别在于不能长时间保持很小的 TU 值。Symmetric NAT 与非 Symmetric NAT 的不同之处在于：对于前者(SA, SP)相同的会话(MA, MP)必定相同，后者则不会出现这种情况，对于 Symmetric NAT 来说，(MA, MP)与(DA, DP)形成的子矩阵表现出一对一关系，如图 1 所示。

SA	SP	MA	MP	DA	DP	TL
192.168.0.2	6550	218.6.174.5	5166	61.130.71.13	8523	2
192.168.0.2	6551	218.6.174.5	8236	219.133.35.214	6940	17
192.168.0.2	6552	218.6.174.5	7160	208.184.19.154	7245	19
192.168.0.2	6553	218.6.174.5	15120	218.95.67.171	6675	33
192.168.0.2	6554	218.6.174.5	23140	61.152.43.216	7520	41
192.168.0.2	6555	218.6.174.5	9157	207.45.18.129	6269	53
192.168.0.2	6556	218.6.174.5	37150	216.74.156.142	8100	58
192.168.0.2	6557	218.6.174.5	6837	119.75.223.195	6420	85
192.168.0.10	2736	218.6.174.5	3525	203.208.33.100	80	23
192.168.0.10	2737	218.6.174.5	3525	121.194.0.203	25	754
192.168.0.10	2730	218.6.174.5	3525	218.24.38.219	80	6942
192.168.0.10	1642	218.6.174.5	5480	60.28.183.201	11296	350

(主机 192.168.0.2 正在使用 P2P 软件，而主机 192.168.0.10 正在浏览网页和升级软件)

图 1 某时刻会话集的子矩阵

从 TU 值可以看出，P2P 数据流量具有自相似性，但这不足以将其与普通的 HTTP，FTP 下载区分开来，要识别出 P2P 数据包需要对会话进一步细分。STUN 是简单的 C/S 协议，主机建立会话之前要向 STUN 服

务器提交绑定请求和共享私密请求,分别使用 UDP 和 TCP 发送。服务器收到绑定请求后,将其源地址和端口放在响应消息中发回给主机,这样主机就得到了 NAT 分配给它的(MA, MP)。绑定请求还可以携带一些附加参数,允许绑定响应发送到其他端口,也可以请求 STUN 服务器从不同的地址和端口发送绑定响应。这些格式的消息可以用来确定 NAT 的类型。共享私密请求目的是为了让服务器返回临时的用户名和密码,用于验证和检验消息的完整性。所有的 STUN 消息都包含 20 字节的包头,紧跟着是消息属性字段,如图 2 和图 3 所示。

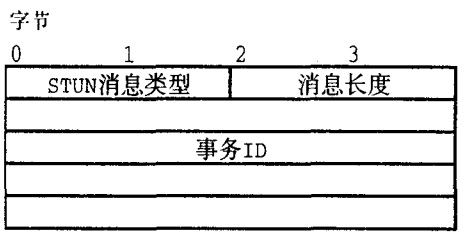

图 2　消息包头

消息类型:

0x0001:绑定请求

0x0101:绑定响应

0x0111:绑定错误响应

0x0002:共享私密请求

0x0102:共享私密响应

0x0112:共享私密错误响应

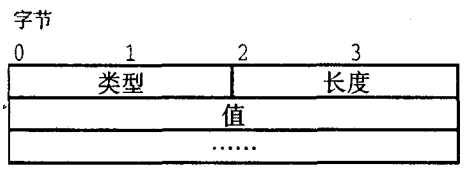

图 3　消息属性

类型:

0x0001:MAPPED-ADDRESS 表示映射过的地址和端口

0x0002:RESPONSE-ADDRESS 表示绑定响应应该响应的目的地址和端口

0x0003:CHANGE-REQUEST 主机请求 STUN 服务器使用不同的地址或端口发送响应

0x0004:SOURCE-ADDRESS 表示 STUN 服务器发送响应的地址和端口

0x0005: CHANGED-ADDRESS 针对 CHANGE-REQUEST,表示响应发出的 IP 地址和端口号

0x0006:USENAME 用于消息完整性检查

0x0007:PASSWORD 用于共享私密响应

0x0008:MESSAGE-INTEGRITY 包含 STUN 消息的散列值

0x0009:ERROR-CODE 绑定错误响应和共享私密错误响应

0x000a:UNKNOWN-ATTRIBUTES 默认的错误响应

0x000b:REFLECTED-FROM 对应包含 RESPONSE-ADDRESS 属性的绑定响应,包含请求的源地址,用于防止 DDOS 攻击

上述消息格式精确描述了主机和 STUN 服务器间的请求和响应报文,在实际应用中选择哪些报文是由各个软件自行决定的,但建立会话之前有些报文是必需的,并且顺序也是固定的,可以利用这一特征识别在 P2P 数据开始传输之前识别出其会话。这些报文可分为三步:

I 主机向 STUN 服务器发送绑定请求,CHANGE-REQUEST 和 RESPONSE-ADDRESS 属性置空,服务器发送绑定响应报文,主机收到后检查 MAPPED-ADDRESS 属性值,将其与本地 IP 地址和端口比较,确定使用了 NAT。

II 主机再次发出绑定请求,设定 CHANGE-REQUEST 属性中的"改变 IP"和"改变端口"标志,如果收到绑定响应,说明使用的是 Full Cone NAT。如果没有收到响应,则继续发送一个绑定请求,目的地址是步骤 I 绑定响应消息中的 CHANGED-ADDRESS 属性值,收到响应后,与步骤 I 得到的响应比较 MAPPED-ADDRESS 属性值,如果不相同说明是 Symmetric NAT,相同则进行步骤 III。

III 继续发送绑定请求,只设定 CHANGE-REQUEST 属性中"改变端口"标志,如果收到绑定响应,则说明使用的是 Restricted Cone,否则是 Port Restricted Cone。P2P 会话识别流程如图 4 所示。

该算法的设计思想是:将整个识别流程转化为从二叉树根结点开始,寻找叶结点的过程。当新的会话发送第一个 UDP 数据包时,就检查其是否为 STUN 协议的绑定请求,然后依次按照 STUN 协议的消息格式检查后续数据包,达到叶结点时结束,如果根结点是某种 NAT,则绑定成功,该会话将用来传输 P2P 数据,该识别过程的时间复杂度是 O(1),记录(SA, SP, MA, MP)作为关键字存放在哈希表中,从(MA,MP)通过的流量就是 P2P 流,当(SA,SP)与(MA,MP)的映射关系结束时,(MA,MP)传输的不再是 P2P 数据,则应将其从哈希表中删除。NAT 每次发送数据包时,在记录(MA,MP)的哈希表中查询源地址;接收数据包时,在记录(MA,MP)的哈希表中查询目的地址,若找到匹配项,就证明它是一个 P2P 数据包,这一系列操作的时间复杂度仍是 O(1)。

3　试验结果

试验环境是:一台安装 Linux 虚拟路由器的 PC 作为 Full Cone NAT,连接一台装有迅雷的 PC 机,并安装

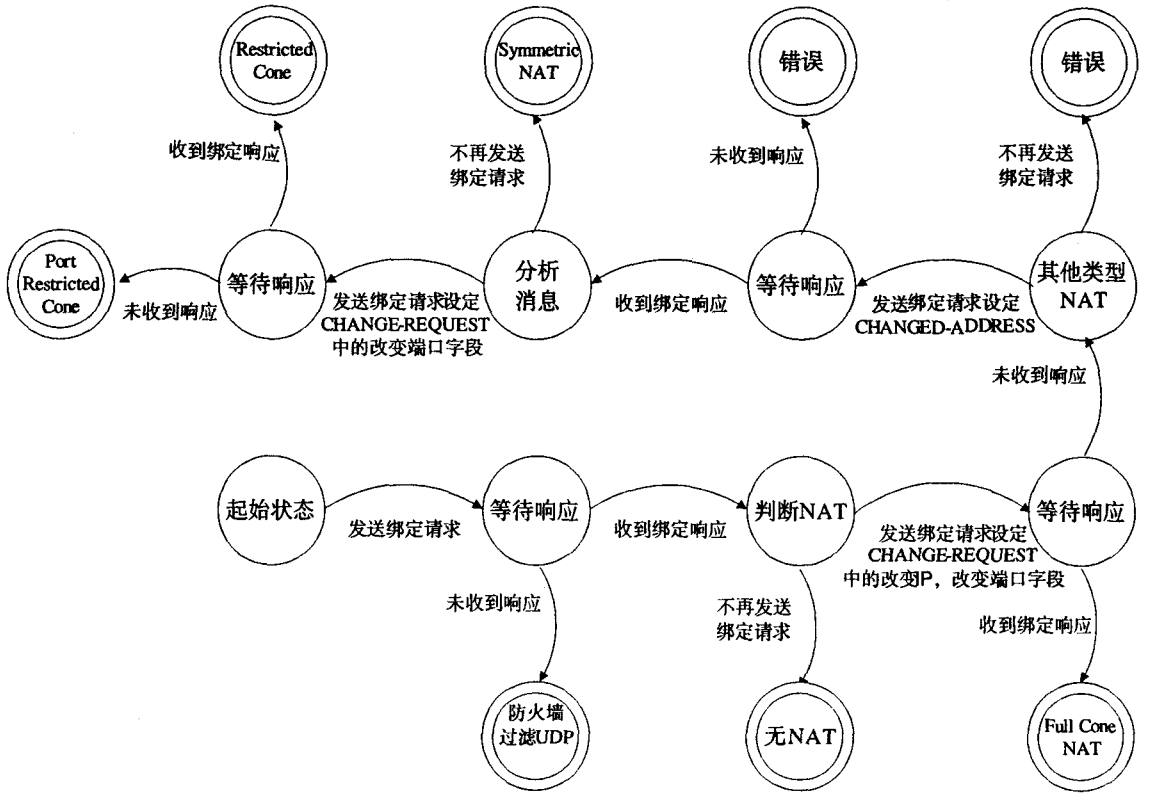

图 4 P2P 会话识别流程

sniffer 收集迅雷进程收发的数据包进行统计。由于迅雷是 P2SP 软件，所以在虚拟路由器中利用 Iptable 工具设置了访问规则，屏蔽了迅雷的资源服务器 IP，让其完全作用在 P2P 机制下，迅雷的 P2P 下载是基于 STUN 协议的。在虚拟路由器上利用 Netfilter 提供的 5 个拦截点设置分析函数，通过对话的分析识别 P2P 流量。

实验中，由虚拟路由器分析函数收集到的 P2P 流量是 2.41G，40432453 个 P2P 数据包，而由主机应用层收集到的迅雷总流量是 2.4G，40425188 个数据包，识别率达到 99.98%。

4 结束语

文中提出了基于会话表的 P2P 识别方法，具备很高的识别率和良好的时间复杂度，它专门针对 STUN 协议，适用存在 NAT 的局域网环境。由于现有的 P2P 软件种类繁多，并非完全遵照 STUN 协议实现 NAT 穿透，有的则利用其他协议实现，比如 ALG，MIDCOM，TURN 等。要识别更多的 P2P 软件需要研究其他协议格式，采用多个识别函数并行分析，将在后续的论文中阐述。

参考文献：

[1] Karagiannis T，Broido A，Faloutsos M，et al. Transport layer identification of P2P traffic[C]//Li Jiangtao，Jiang Yongling. Proceedings of the 4th ACM SIGCOMM conference on Internet measurement. Survey of P2P traffic identification and engineering technology. Taormina，Sicily，Italy：[s. n.]，2005.

[2] 李 君，王 攀，孙雁飞，等. P2P 业务流量识别、分析和控制研究[J]. 计算机工程，2006，32(11)：122－124.

[3] Sen S，Spatscheck O，Wang Dongmei. Accurate，scalable in－network identification of p2p traffic using application signatures[C]//Proceedings of the 13th international conference on World Wide Web. New York，NY，USA：[s. n.]，2004：512－521.

[4] 陈宝钢，张 凌，许 勇，等. 基于 P2P 应用的网络流量特征分析[J]. 计算机应用，2007，27(3)：531－533.

[5] 石 萍，陈贞翔，荆 山，等. 基于对等特征的 P2P 流量识别方法[J]. 中国教育网络，2007(2)：36－38.

[6] 刘 琼，徐 鹏，杨 海，等. Peer－to－Peer 文件共享系统的测量研究[J]. 软件学报，2006，17(10)：2131－2140.

[7] Srisuresh P，Holdredge M. IP Network Address Translator (NAT) Terminology and Considerations[S]. RFC 2663，IETF，1999.

[8] Rosenberg J，Weinberger J，Huitema C，et al. STUN － Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)[S]. RFC 3489，IETF，2003.

[9] 李双庆，左建勋，路 遥. 基于 ABV 的 BT 流量识别与分类[J]. 计算机应用，2007，27(6)：166－167.