文章编号:1001 - 9081(2006)02 - 0292 - 03

基于 P2P 的语言 IP 穿越网络地址转换和防火墙的统一模型

杨永火,何丕廉,崔晓源,孙学军
(天津大学 电子信息工程学院,天津 300072)
(yhyang2006@yahoo.com)

摘 要:从 P2P 网络出发,提出了一种新的语言 IP(Voice over IP,VoIP)穿越网络地址转换(Network Address Translation,NAT)和防火墙的统一模型。该模型利用分布式 P2P 网络的二层拓扑结构,通过最优路径建立算法(Optimal Path Establishment Algorithm,OPEA)以一种更有效的方式组织会话建立过程,使之能在各种情况下对 NAT 和防火墙的穿透问题提供最优解。与 STUN 等单一模型相比,具有更高的效率和健壮性。通过建立原型系统,在校园网环境中进行了模拟测试,证实了该模型的可行性以及提高服务质量的有效性。

关键词:P2P 网络;语音 IP;网络地址转换;防火墙;穿越
中图分类号: TP393.02 **文献标识码**:A

Unified model for VoIP traverse of NAT and firewall based on P2P networks

YANG Yong-huo, HE Pi-lian, CUI Xiao-yuan, SUN Xue-jun
(*School of Electronic & Information Engineering, Tianjin University, Tianjin* 300072, *China*)

Abstract: A unified model for VoIP traverse of NAT and firewall was presented based on P2P networks. This model exploits the two-tied distributed P2P overlay network to develop an Optimal Path Establishment Algorithm (OPEA), through which the optimal solutions of NAT/FW traverse in varied scenarios are got. It is more effective and more robust compared to other solutions such STUN. Its feasibility and effectiveness in providing QoS were demonstrated through the implementation of a prototype with corresponding experiments on the campus network.

Key words: P2P networks; Voice over IP; NAT; firewall; traverse

0 引言

当前,CS(Client/Server)模型受到了严峻的挑战。Internet 上每年产生的新信息达到 2×10^{18} 字节,但用户仅搜索到 8.0×10^{8} 个网页。服务器成了 Internet 中严重的瓶颈,而随着个人电脑性能的飞速提升和宽带网的逐步推广,大量的客户资源和网络带宽被闲置。在这样的背景下,P2P 模型得到了人们的广泛关注。在 P2P 模型中,每个用户既是资源的提供者也是资源的使用者,形成了一个完全无中心的分布式计算环境。P2P 模型在文件交换,大规模科学计算,搜索引擎等方面都体现出了巨大的优势,如 Napster[1]、SETI@home、Gnutella 等。

最近 P2P 模型被应用到了 VoIP 领域,也就是利用 P2P 网络提供高质量的多媒体服务,如 Skype[3] 等。P2P 模型在 VoIP 穿越 NAT 和防火墙以及提高多媒体服务质量方面都有巨大的优势。

本文利用二层分布式、自组织 P2P 网络的协同工作的特点,在会话终端 UAC(User Agent Client)加入 P2P 网络时注册相应的位置信息,而在会话建立时根据双方的位置信息,通过最优路径建立算法(OPEA),有效地组织会话建立过程和媒体通信方式。这样,在各种不同的网络拓扑结构下,提供了一种综合的足够灵活的方法,较好地解决了 All-NAT 与效率问题。最后,给出了实验原型系统的建立以及相应的语音服务质量的评估。

1 NAT 和防火墙穿越问题

几乎所有的企业在部署 VoIP 应用时都面临网络地址转换(NAT)[4] 及防火墙对语音 IP 的阻挡问题。普通个人用户通过宽带上网通常也处于 ISP 运营者的 NAT 和防火墙设备之后。所以,这个问题对企业用户和普通个人用户都有影响。

1.1 VoIP 穿越 NAT 面临的挑战

一个 NAT 设备允许一个企业为局域网上的设备分配私有的 IP 地址,这样一个公网 IP 地址就可以同时为多个只具有私有 IP 地址的终端服务了,从而在一定程度上解决了公网 IP 匮乏的问题。但是控制 Internet 上信息流向的路由设备仅仅能把数据传送到具有可路由 IP 地址(公网 IP 地址)的设备。所以,NAT 后的终端向 NAT 外的其他具有公网 IP 地址的终端发起呼叫是容易的,但是 NAT 后的终端无法接受来自局域网外的呼叫。另一方面,当前主流的 VoIP 通信协议(如 SIP[5])都把用于传送语音 IP 的会话双方的 IP 地址和端口封装在信令消息包的负载部分。这样如果会话终端向这些私有 IP 地址传送语音时就会遭到失败。

文献[4]定义了四种类型的 NAT:完全圆锥型(Full Cone)、地址限制圆锥型(Address Restricted Cone)、端口限制

收稿日期:2005 - 08 - 13 **基金项目**:天津市科技发展计划(04310941R);天津市应用基础研究计划(05YFJMJC11700)

作者简介:杨永火(1979 -),男,浙江丽水人,硕士研究生,主要研究方向:网络信息安全、网络多媒体技术、Web 检索与挖掘; 何丕廉(1942 -),男,天津人,教授,博士生导师,主要研究方向:网络多媒体、人工智能与计算机辅助教育、自然语言处理、Web 检索与挖掘; 崔晓源(1981 -),男,天津人,硕士研究生,主要要研究方向:网络信息安全、网络多媒体; 孙学军(1946 -),男,河北人,副教授,主要研究方向:计算机网络与通信.

圆锥型(Port Restricted Cone)和对称型(Symmetric)。前三种 NAT,映射与目的地址无关,只要源地址相同,映射就相同,而对称型 NAT 的映射则同时关联源地址和目的地址,所以穿越最为复杂。

1.2　VoIP 穿越防火墙面临的挑战

通常,企业为使内部的计算机不受外部网络的攻击,都部署了防火墙,主要目的是通过防火墙限制进入内部网的数据包。多媒体会话协议(如 SIP)的目标是建立 P2P 媒体流以减少时延。这样,终端必须随时侦听外来的呼叫,而防火墙却通常被配置来阻止任何不请自到的数据包通过。即使防火墙可以让最初建立呼叫时发往固定端口的数据包进入,其后的多媒体通信需要通过动态端口分配来传输数据包,而目前的防火墙一般仅允许事先打开特定的协议和端口,并不支持动态打开端口。也就是说为了允许多媒体数据包通过防火墙,网络管理员不得不打开防火墙上的所有端口,这样防火墙就失去存在的意义了。

2　P2P 统一穿越模型

目前关于 VoIP 的 NAT 和防火墙穿越问题有多种解决模型,如应用层网关(ALG)、虚拟专用网(VPN)[6]、隧道穿透、STUN[7]、TURN[8]等。它们都在一定程度上解决了 VoIP 穿越 NAT 和防火墙问题,但是它们的不足之处也是非常明显:ALG 需要升级或改动企业的 NAT 和防火墙的配置,这对于大多数已经部署完毕的企业网络来说是十分困难的;VPN 仅仅允许位于同一个 VPN 内的设备进行通信,无法实现与位于公众网上的终端之间的通信;隧道穿透模型和 TURN 模型中所有实时通信数据都必须经由单一 Server 中继,这会引起潜在的瓶颈,并且带来了较大的延迟和丢包率;STUN 模型只能解决完全圆锥型 NAT 问题。

基于 P2P 的统一穿越模型不需要企业升级或改造现有的网络,可以解决与所有 NAT 类型和防火墙后面的会话终端进行多媒体通信的问题,并且保证了实时通信对语音 QoS 的要求。

2.1　P2P 统一穿越模型的基本原理

P2P 网络的拓扑结构由最初的一个中心节点(如 Napster)到完全分布式(如 Gnutella),现在已经逐步发展到了一个由超级节点(Super Node,SN)和普通节点(Ordinary Node,ON)构成的二层分布式、自组织的拓扑结构(如 Skype)。在这样的网络拓扑结构中,所有参与会话的终端 UAC 根据其能力(包括网络连接状态,CPU 运算能力和可用的系统资源等)分为 SN 和 ON。通常,SN 是那些拥有公网 IP 地址,具有较强的 CPU,并且内存和带宽都比较大的终端。而 ON 必须在其中一个 SN 上进行注册。这样任何 ON 就可以通过与 SN 交换信息,再通过 SN 间互换信息,找到与之通信的的另一 ON,拓扑结构如图 1 所示。

在这样的 P2P 系统中,SN 同时扮演 Client 和 Server 的角色,而 ON 通常只做 Client。P2P 穿越模型的基本思想就是充分利用网络中存在的大量 SN 的计算能力和资源,为处于 NAT 和防火墙之后的 ON 提供一个交换信息的中间媒介,从而提高实时多媒体服务的质量。

基于 P2P 的统一穿越模型中,穿越过程可以分为登录注册和会话建立两部分。

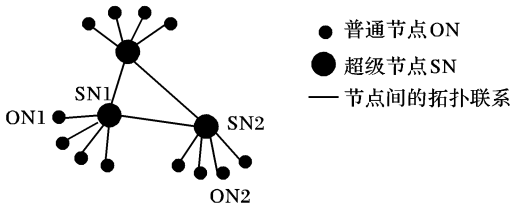

图 1　SN 和 ON 组成的二层结构的分布式 P2P 网络

2.2　登录注册

当会话终端 UAC 加入 P2P 网络时,它首先向 P2P 网络中的 SN 注册。注册的内容包含其位置信息,也就是终端是否具有公网 IP 地址、是否在 NAT 之后以及相应的 NAT 的类型、是否在防火墙之后等。在文献[7]中描述了一种通过终端向 STUN Server 发送一些探测性的数据包来获取位置信息的方法。在二层分布式 P2P 网络中,在 ON 登录注册时 SN 可以扮演 STUN Server 的角色。终端 UAC 处在公网上时,注册信息包含其公网 IP 地址及与 SN 通信的端口组成的接口;UAC 处在 NAT 之后时,注册信息包含其的私有 IP 地址和端口组成的接口、绑定的公网 IP 地址和端口组成的接口以及 NAT 类型信息;UAC 处在防火墙后面时,记录其与 SN 通讯的 IP 地址和端口组成的接口。

登录完毕后,终端定期向 SN 发送一些保持连接状态的数据包,以确保 NAT 绑定的地址仍然可用,同时定期刷新注册在 SN 上的信息以反映网络拓扑的变化。

2.3　会话建立

考虑这样的情景,如图 1 中所示,P2P 网络上的终端 ON1 想和终端 ON2 进行语音会话,它们分别注册在超级节点 SN1 和 SN2 上。

ON1 首先访问它所注册的超级节点 SN1,获取自己的位置信息,然后请求 SN1 通过超级节点间的搜索,定位 ON2 所注册的超级节点 SN2,从而获取 ON2 的位置信息。根据 ON1 和 ON2 的位置信息,终端 ON1 通过最优路径建立算法(OPEA)组织与终端 ON2 的最优会话方式。

OPEA 算法:

```
if ON1 不在防火墙后 && ON2 在公网上
  ON1 向 ON2 直接发起会话请求;
else if ON1 在公网上 && ON1 在 NAT 后
{
 ON1 向 SN2 发送反向连接的会话请求;
 SN2 指令 ON2 向 ON1 发起反向连接;
}
else if ON1 在 NAT 后 && ON2 在 NAT 后
{
 if ON2 在全锥型 NAT 后
   ON1 向 ON2 绑定的公网接口发起连接;
 else if ON1 在全锥型 NAT 后
 {
  ON1 向 SN2 发送反向连接的会话请求;
  SN2 指令 ON2 向 ON1 绑定的公网接口发起反向连接;
 }
 else if ON1 在受限型 NAT 后 && ON2 在受限型 NAT 后
 {
  ON1 向 SN2 发送反向试探的会话请求;
  SN2 指令 ON2 向 ON1 绑定的公网接口发送试探性数据包;
  ON1 向 ON2 绑定的公网接口发起连接;
  //发送试探性数据包是为了使受限圆型
```

```
  //的 NAT 能够通过 ON1 发起的连接请求
 }
 else
   通过 SN1 和 SN2 两路中继来建立通信;
   //与对称型 NAT 后终端的通信
 }
else
{
 通过 SN1 和 SN2 两路中继来建立通信;
 //与防火墙后终端的通信
}
```

在 OPEA 算法中,如果其中任一方处在防火墙后面,那么所有通信都通过两个超级节点继续转发,因为目前大部分防火墙都不允许在语音通信时动态分配端口,因此建立直接的通信途径是很困难的。虽然这样会造成一定的延迟,但是由于 P2P 网路中超级节点数量众多,利用这些超级节点进行多路径传输(Packet Path Diversity)可以缓解其他模型的中继方式所遇到的单一 Server 瓶颈问题,文献[9]表明,这样的系统可以提高两终端之间的多媒体服务质量。

3 实验与评估

根据上述的基于 P2P 的统一穿越模型,我们实现了一个该模型的原型系统,以证实模型的可行性及提高语音服务质量的有效性,该原型系统主要模块如下。

启动注册模块:当一个会话终端 UAC 启动时,以用户名和密码在 SN 上完成注册过程,然后发起 NAT 和防火墙的检测过程并在 SN 上进行相应的注册。

会话建立模块:实现了 OPEA 算法对 NAT 和防火墙的穿越。一般情况下传输层协议选择 UDP,如果 UDP 消息传送失败(如防火墙阻止 UDP 数据包),TCP 端口 80 被用做默认的传输接口。

语音传输模块:采用 G.729 编码方案和实时传输协议 RTP、RTCP 进行传输。

第一组实验中,两终端分别处于各种不同的位置上(公网、完全圆锥型 NAT、受限圆锥型 NAT、对称型 NAT 以及防火墙之后),共计 7 种组合情形,原型系统均能顺利建立会话,证实了模型的可行性。

第二组实验测试模型提高语音服务质量的效率。我们采用国际电信联盟(ITU)最近提出的 ITU-T E-Model 来评估语音质量,该模型综合考虑了网络中各种可能对语音质量产生影响的因数,包括端到端的网络延迟、丢包率、编码模式和播放策略等,因此被广泛的应用在语音质量的评估上。根据我们的评估需求,可通过如下公式计算最后的语音服务质量 MOS 值(e 代表端到端的延迟,d 代表丢包率):

$$MOS = 1 + 0.035R + 7 \times 10^{-6}R(R - 60)(100 - R) \quad (1)$$

$$R = 94.2 - I_e - I_d \quad (2)$$

$$I_e = \gamma_1 + \gamma_2 \ln(1 + \gamma_3 e) \quad (3)$$

$$I_d = 0.024d + 0.11(d - 177.3)F(d - 177.3) \quad (4)$$

式(3)中的参数 $\gamma_i(i = 1,2,3)$ 与具体的编码模式关联,我们选取的编码模式为 G.729,所以相应的三个参数值分别为 10、47.82 和 18。式(4)中的 $F(x)$ 为二值函数,$x < 0$ 时函数值为 0,反之为 1。语音服务由低到高的 MOS 值的范围为 1 分到 5 分。

按照 ITU-T 对 G.729 编码方案的设定,分别在 P2P 穿越模型中两终端直接建立会话和通过两个 SN 中继方式建立会话下传播 4kbit/s 的数据流。同时,为比较方便,测试了其他模型中通过单 Server 中继方式传输的性能。试验的结果如图 2 所示。

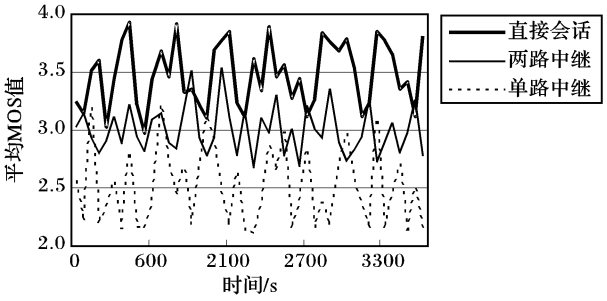

图 2 P2P 统一穿越模型语音质量试验

从图 2 可以看出,P2P 统一穿越模型中的直接会话和两路中继的平均 MOS 值都明显高于普通的单路中继方式。分组传播路径的性能差异性使得在 P2P 网络中做多路传输的语音服务质量比单 Server 中继有更出色的表现。

4 结语

基于 P2P 统一穿越模型充分利用了网络中参与节点的计算能力和资源,不需要对现有企业或 ISP 网络做任何的升级和改造,实现了 VoIP 对 All-NAT 和防火墙穿越。通过 OPEA 算法有效的组织会话,提供了一种负载均衡的解决方案,从而在最大程度上保证了服务的可靠性和效率。

但是 P2P 统一穿越系统所面临的最大挑战就是安全性问题。虽然可以在超级节点引入相应的连接认证机制,但是对超级节点的恶意的有计划的攻击,尚无有效的防范措施,这是该模型将来研究的方向。

参考文献:

[1] Napster. http://www.napster.com/[EB/OL],2005.

[2] Gnutella Protocol Specification[EB/OL]. http://www.clip2.com/GnutellaProtocol04.pdf,2005.

[3] Skype, http://www.skype.com[EB/OL].

[4] SRISURESH P, HOLDREGE M. IP Network Address Translator (NAT) Terminology and considerations[S]. RFC 2663, August 1999.

[5] HANDLEY M, SCHULZRINNE H, SCHOOLER E, *et al*. SIP: Session Initiation Protocol[S]. RFC 3261, Jun. 2002.

[6] GLEESON B, LIN A, HEINANEN J, *et al*. A Framework for IP Based Virtual Private Networks[S]. RFC 2764, IETF, February 2000.

[7] ROSENBERG J, *et al*. STUN - Simple Traversal of UDP Trough NATs[S]. Internet Draft, IETF, Oct. 2001.

[8] ROSENBERG J, MAHY R, HUITEMA C. Traversal Using Relay NAT (TURN)[S]. Internet Draft, IETF, Nov. 2001.

[9] LIANG YJ, STEINBACH EG, GIROD B. Multi-stream voice over ip using packet path diversity[A]. IEEE Multimedia Signal Processing Workshop (MMSP01)[C]. 2001. 555 - 560.

[10] The e-model, a computational model for use in transmission planning [S]. ITU-T Recommendation G.107, March 2003.