# 对 ICE 穿越 Symmetric NAT 技术的改进

刘胜辉[1],周 野[2]
LIU Sheng-hui[1],ZHOU Ye[2]

1.哈尔滨理工大学 软件学院,哈尔滨 150080
2.哈尔滨理工大学 计算机科学与技术学院,哈尔滨 150080
1.College of Software,Harbin University of Science and Technology,Harbin 150080,China
2.College of Computer Science and Technology,Harbin University of Science and Technology,Harbin 150080,China
E-mail:pjzhouye@163.com

**LIU Sheng-hui,ZHOU Ye.Improvement of technology of traversing through Symmetric NAT based on ICE.Computer Engineering and Applications,2010,46(3):109-111.**

**Abstract:** ICE(Interactive Connectivity Establishment) as a integrated solution can suit every kinds of NAT traversing.But in symmetric NAT case,there are still some disadvantages using the TURN method with not high efficiency.An improved ICE method is put forward based on ICE and concerning the pot prediction method,which is able to make ICE obtain more messages of addresses and traverse through most of Symmetric NATs using the way of UDP direct transfer.It will resolve the problem and enhance the efficiency of ICE.

**Key words:** Interactive Connectivity Establishment(ICE);Network Address Translation(NAT);Symmetric NAT

**摘 要:**ICE(交互式连通性建立)方案作为一种综合解决方案,适合各种类型的 NAT 穿越。但 ICE 方案针对 Symmetric NAT 全部采用 TURN 中继方式进行穿越,而 TURN 方式在传输效率上尚有不足。结合端口预测方案 P-STUN,对原有 ICE 方案进行了改进,使其获得更多的地址信息,能够对大部分 SymmetuicNAT 采用 UDP 直连方式穿越,解决了上述问题,有效提高了 ICE 针对 Symmetric NAT 穿越的效率。

**关键词:**交互式连通性建立;网络地址转换;对称网络地址转换
**DOI:**10.3778/j.issn.1002-8331.2010.03.032 **文章编号:**1002-8331(2010)03-0109-03 **文献标识码:**A **中图分类号:**TP393.02

## 1 引言

NAT(Network Access Translation)即网络地址转换,是 Internet Engineering Task Force(IETF)的一个标准[1]。NAT 是为解决 IP 地址紧缺的问题而被提出的,它驻留在构成公用 Internet 与专用局域网之间屏障的网关设备中,通过使用预设好的规则,修改 IP 数据包头的地址信息,并且跟踪这些转换以保持各个 Session 不变。NAT 技术可以使局域网内的多台主机共享一个外部地址访问 Internet,同时它可以隐藏局域网的内部 IP 地址,提供网络安全保障。因此得到了广泛应用。另一方面,随着近年 IP 网宽带业务的蓬勃发展,基于分组的多媒体通信也被广泛应用在视频会议、IP 电话等方面。在这些应用中,不仅需要在报文头部带有地址信息,在媒体负载中同样也需要带有地址信息,这要求每个对等程序都具有可路由的互联网公共地址,并且具有唯一的端口号。由于 NAT 是通过修改 TCP/UDP 报文的头部地址信息来实现地址的转换,如果使用内部地址或者是同一端口号,内部地址对局域网外的地址来说是不可路由的,应用就会因为媒体流传输通道不能建立而失败。因此穿越 NAT,在位于不同内部局域网的对等结点之间建立媒体流传输通道,对此类应用业务的发展有很大影响。

## 2 ICE 技术分析

为了解决穿越 NAT 的问题,业界出现了很多穿越技术,如 NAT/ALG 方式,MIDCOM 方式,STUN 方式,TURN 方式等等。交互式连通建立方式 ICE(Interactive Connectivity Establishment)是一个综合穿越方案,它非一种新的协议,它不需要对 STUN、TURN 或 RSIP 进行扩展就可适用于各种 NAT。ICE 是通过综合运用上面某几种协议,使之在最适合的情况下工作,以弥补单独使用其中任何一种所带来的固有缺陷。它充分考虑了内网主机所处的网络环境,利用穿越方案调度算法,使用最合适的一种或几种穿越方案对 NAT 防火墙进行穿越,具有自适应的能力,能够在任何网络状况下正常工作[2]。

STUN 协议中对 NAT 进行了分类,其中 Symmetric NAT 对内部主机的限制最严格,它会给每一个新的 Session 分配新的端口,而这个端口是无法通过 STUN 请求获得的[3]。一旦网络中存在对称 NAT,ICE 方案将会工作在 TURN 中继方式,那么穿越 NAT 收发数据需要服务器来中转,因此效率很低[4]。这里在 ICE 穿越方案中加入一种端口预测策略,这种策略可以对 Symmetric NAT 为新的 Session 分配的端口进行预测,如果预测成功,那么双方可以使用预测的端口进行通信,不需要使用

**作者简介:**刘胜辉(1961-),男,教授,硕士生导师,主要研究领域为 CIMS,网络信息安全;周野(1983-),男,硕士研究生,主要研究领域为网络通信。
**收稿日期:**2008-08-05 **修回日期:**2008-11-03

TURN 方式转发数据,很明显在保证一定的预测成功率的前提下,加入这样的策略后提高了 ICE 穿越方案的效率。

## 3 ICE 改进方案

### 3.1 整体结构

ICE 方案结构图如图 1 所示,ICE 服务器位于公网,地址为 202.120.58.178,集成了 STUN 服务器,TURN 服务器和控制服务器的控制功能,控制服务器用来完成双方客户端地址信息的交互。ICE 服务器必须启动两个 socket 套接字,绑定两个端口进行监听,为端口预测提供必要的端口信息。

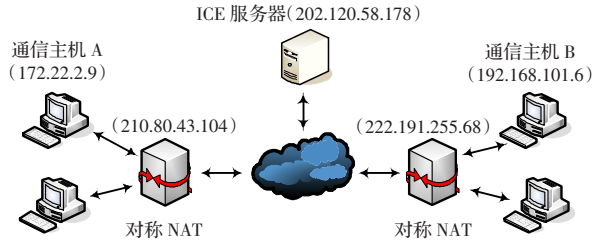


图 1 ICE 结构图

ICE 客户端双方处于 NAT 之后的私网中,客户端 A 本地地址为 172.22.2.9,A 的 NAT 地址为 210.80.43.104。客户端 B 本地地址为 192.168.101.6,NAT 地址为 222.191.255.68。

### 3.2 预测算法介绍

基于预测方法的 NAT 穿越技术 P-STUN[5]方案,是针对 STUN 技术对 Symmetric NAT 穿越的缺陷提出的。它利用 Symmetric NAT 端口分配规律,通过对 NAT 建立的新 Session 分配的新端口进行预测,对 Symmetric NAT 进行穿越。

P-STUN 方案中端口预测算法的基本思想就是:通过多次发送 STUN 请求,获得足够的预测信息,根据预测信息预测实际传输时将被分配到的端口。为了达到这个目的,必须获得 NAT 的端口分配策略,因此需要向不同的 IP 地址和端口发送 STUN 请求。所以,在端口预测时 ICE 服务器需要启动两个套接字来处理 STUN 请求。

端口预测算法如下:

(1)通信主机分别向 ICE Server 的不同 UDP 端口发送 STUN 请求,从得到的两次响应消息负载中可以得到被分配的外部地址 Address 和两次被分配得到的端口号:$P_{first}$ 和 $P_{second}$。

(2)根据两次被分配的端口号 $P_{first}$,$P_{second}$ 计算 Symmetric NAT 的端口分配间距 $\Delta P$:

$$\Delta P=P_{second}-P_{first}$$

(3)根据 $\Delta P$ 预测实际建立链接时将要被分配到的端口号 $P^{pre}$:

$$P^{pre}=P_{second}+\Delta P$$

### 3.3 ICE 算法流程

#### 3.3.1 地址收集

会话双方通过 ICE 服务器收集本机传输地址信息。需要搜集的地址信息包括本地传输地址(Local Transport Address),NAT 映射地址,P-STUN 预测地址,TURN 分配的中转地址。显然,搜集的传输地址越多,连通方式就越多,ICE 将工作得越好,这里加入端口预测方法,就是为了增加连通方式的搜集,从而提高 ICE 的穿越性能。但为了建立对等通信,ICE 通常要求至少保留中继方式(TURN 方式)来保证穿越成功,一旦连通双方处于 Symmetric NAT 之后,并且预测失败,就可以启用 TURN 中转的方式进行穿越。

主机 A 在确定本机使用的端口号之后,可以很容易获得本机该网卡上使用的 IP 地址 172.22.2.9:2020,为了保证预测端口的准确度,A 首先通过 TURN 请求查询出 ICE 服务器为其分配的 TURN 端口为 8801,然后通过 ICE Server 的 4589 端口查询它在 NAT 上的映射地址 210.80.43.104:3344;通过 4590 端口查询它的映射地址 210.80.43.104:3348。这样通过预测算法,A 主机可以预测出 NAT 下次为新的 Session 分配的端口 3352;地址搜集过程入图 2 所示。

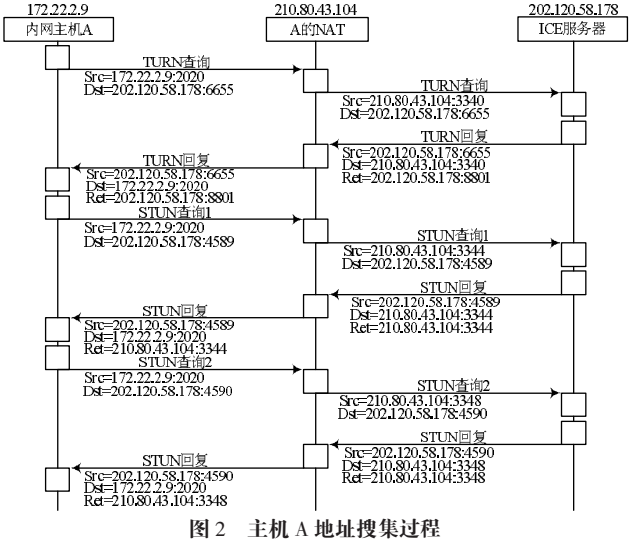


图 2 主机 A 地址搜集过程

主机 B 的地址搜集过程与 A 相似,双方具体地址信息如表 1。

表 1 地址搜集结果

| | A 的地址信息 | | B 的地址信息 | |
|---|---|---|---|---|
| | IP 地址 | 端口 | IP 地址 | 端口 |
| 本机 | 172.22.2.9 | 2020 | 192.168.2.6 | 34988 |
| 映射 | 210.80.43.104 | 3344 | 222.191.255.68 | 21873 |
| 预测 | 210.80.43.104 | 3352 | 222.191.255.68 | 21879 |
| TURN | 202.120.58.178 | 8801 | 202.120.58.178 | 8802 |

#### 3.3.2 连通性检查确定穿越方式

在地址收集之后通信双方根据收集的各种地址确定优先级并进行有效性检查。这些地址信息的优先级为本地地址>NAT 映射地址>P-STUN 预测地址>TURN 中转地址。

通信主机 A,B 双方依照对方地址的优先级依次向对方发送测试数据包进行连通性检查,与此同时收到测试数据包的一方向对方进行响应。对于 NAT 映射地址的检查,为了避免丢包,应多次发送测试数据包,A 发送的连通数据自然起到了 NAT 打洞的作用,B 检查时就可以连通了。这里以 B 为例,连通性检查时序如图 3 所示。

这里按照前面的优先级依次验证,如果预测的端口正确,则不需要进行 TURN 验证,如果端口预测方案失败,则启用 TURN 地址来保证穿越的成功。

#### 3.3.3 建立连接

穿越方式确定之后就可以直接使用确定的地址和端口进行通信了,这个通信的过程主要是指 UDP 数据,当然也可以指其他使用 UDP 的数据控制协议,比如 SIP。这样只要建立一个

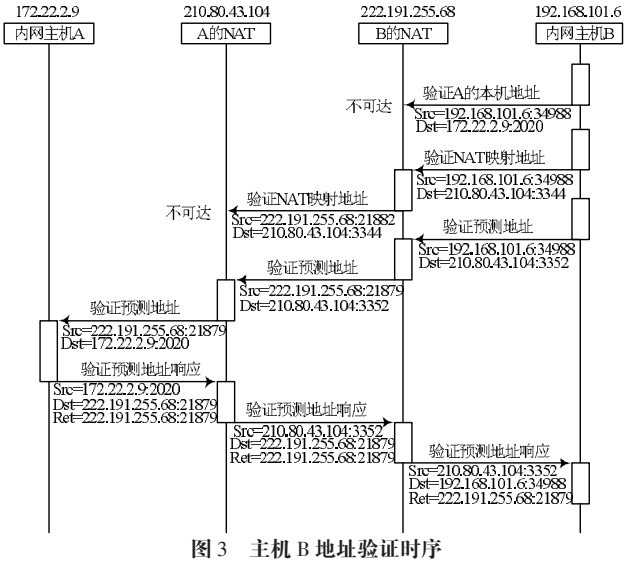


**图 3　主机 B 地址验证时序**

通信通道,其他的通信通道都可以使用已经建立的通道来进行扩展建立了。

## 4　验证结果与分析

在穿越过程中受其他应用程序同时运行的影响,Symmetric NAT 有可能在 ICE 工作过程中给其他 Session 分配了 ICE 地址搜集过程中预测的端口,从而导致预测失败。因此,改进后 ICE 方案效率的提高主要依赖于 P-STUN 端口预测算法预测的命中率。在低负载的情况下,建立 50 次连接,全部成功;高负载的情况下成功 48 次,成功率为 96%。实验结果表明改进后的方案可以有效地提高 ICE 方案的性能。改进后的 ICE 方案虽然增加了在地址收集过程的系统开销,但是在穿越成功以后由于采用了直连方式传输数据,对于 TURN 中转方式来说,数据传输性能有了很大提高,更加有利于平衡服务器负载。

另外需要说明的是,为了降低预测算法的复杂度,简化了对 Symmetric NAT 的类型细分。在算法中,默认 NAT 将按照一定的间距 $\Delta P$ 来分配端口号,而实际情况中,NAT 也可以按照事先设定的分配表来为每个请求分配端口号,这样前后两次分配的端口号不存在线形关系。在这种情况下,预测算法有可能失败。之所以在 P-STUN 中没有区分这种情况,一方面是因为目前绝大多数 Symmetric NAT 路由器是按照一定的固定间距来进行端口分配;另一方面也是为了简化预测算法,提高算法的命中率。

## 5　结束语

在原有 ICE 方案的基础上,结合端口预测方法 P-STUN 对 ICE 穿越方案进行了改进,在没有明显增加 ICE 方案复杂性的前提下,有效提高了针对 Symmetric NAT 的穿越效率,从而提升了 ICE 整体性能。

## 参考文献:

[1] Athans M.Command and control theory:A challenge M to control science[J].IEEE Trans on AC,1987,32(4):286-293.

[2] Rosenberg J.Interactive Connectivity Establishment(ICE):A methodology for Network Address Translator(NAT) traversal for the Seddion Initiation Protocol(SIP)[S].2003-07.

[3] Rosenberg J,Weinberger J,Huitema C.RFC 3489 STUN-Simple Traversal of User Datagram Protocol(UDP) Through Network Address Translators(NATs)[S].2003-03.

[4] Rosenberg J,Huitema C,Mahy M.Traversal Using Relay NAT (TURN)[Z].2003.

[5] 王止戈,彭宇峰,张苏灵,等.一种基于预测的 Symmetric NAT 穿越解决方案[J].计算机工程,2005,31(11):122-123.

(上接 104 页)

表 1 是该文结果和文献结果的全文的 DRDM 值 $d$ 和全文扭曲度 $APPD$ 的比较,分块大小均为 15×15。从比较结果可以看出,该文的算法视觉效果比文中提到 Min Wu[2]和 LU[4]的实验结果,以及基于 Min Wu[2]的经典算法提出改进的 Yang[7]和 XI[8]的实验结果都要理想,在客观上证明了该算法的视觉优越性。

**表 1　该文结果和文献结果的比较**

| | 该文结果 | WU[2] | LU[4] | Yang[7] | XI[8] |
|---|---|---|---|---|---|
| $d$ | 0.106 | 0.944 | 0.182 | 0.316 | 0.85 |
| $APPD$ | 0.275 | 0.390 | 0.730 | 0.440 | 0.46 |

## 4　结语

结合汉字笔画结构特点与可翻转性准则、DRDM 准则,提出了一种新的基于汉字结构隐藏的文本水印算法,该算法有效利用了汉字结构的独特特点,选定了具有最佳翻动性的标准模块,在全图中搜索标准模块来嵌入水印,实现了数据隐藏与内容认证。该算法在目前两大视觉评价准——DRDM 准则与像素翻转引起的扭曲度准则计算下都达到最优。体现出了汉字的结构特点在分块翻转方案中的独特优势。如何将可翻动像素模型应用到纸张方式上,实现抗打印、复印、扫描的二值文本认证水印技术,扩大版权保护的范围和能力,是以后研究的方向。

## 参考文献:

[1] Awan I,Gilani S A M,Shah S A.Utilization of maximum data hiding capacity in object-based text document authentication[C]//IEEE Proc IIH-MSP,2006.

[2] Wu M,Liu B.Data hiding in binary images for authentication and annotation[J].IEEE Trans Multimedia,2004,6(4):528-538.

[3] L Haiping,W Jian,Kot A C,et al.An objective distortion measure for binary document images based on human visual perception[C]//16th International Conference on Pattern Recognition,2002,4:293-242.

[4] Lu H,Kot A C,Cheng J.Secure data hiding in binary document images for authentication[J].Proc ISCAS'04,2004,3:806-809.

[5] 吴建国,俞庆英,吴海辉.汉字笔画若干数据的统计方法研究与应用[J].安徽大学学报,2005(5):14-20.

[6] Yang Huijuan,Kot A C.Pattern-based data hiding for binary image authentication by connectivity-preserving[C]//Proc IEEE Transactions on Multimedia,2007,9(3):475-485.

[7] Yang Huijuan,Kot A C.Data hiding for binary images authentication by considering a larger neighborhood[C]//IEEE International Symposium on Circuits and Systems,27-30 May 2007:1269-1272.

[8] XI Yan-hua,ZHANG Min-rui.Fragile Watermarking Based on Smoothness for Document Image[C]//Proc IEEE I-4244-1035-5/07,2007:249-252.