

SIP 穿越 NAT 技术的研究

贺卿

(广东科学技术职业学院 广东 珠海 519090)

【摘要】:下一代网络 NGN 是基于分组技术的网络,能提供基于 IP 的语音、数据、视频等业务,VoIP 是其中典型代表之一,而 VoIP 所面临的技术难点之一就是如何有效地穿越各种 NAT。文章以会话初始化协议 SIP 作为研究对象,分析 SIP 穿越 NAT 的相关技术,对其中的 ICE 穿透方案进行改进,并以一个 VoIP 呼叫实例讲解改进后的流程。

【关键词】:SIP;NAT 穿越;STUN;TRUN;ICE

1. 问题背景

近年来,随着互联网技术和语音技术的不断发展,VoIP 已经占有相当比重的市场份额,成为当今电信业和计算机行业的热门话题。VoIP 是建立在 IP 技术上的分组化、数字化的传输技术,是下一代网络 NGN (Next Generation Network) 应用的典型代表。VoIP 的主要标准有 H.323, MGCP, H.248 和 SIP,其中,会话发起协议(Session Initiation Protocol, SIP)以其简单、灵活、可扩展性而成为应用越来越广泛的协议,被认为是 NGN 技术的核心协议。

穿越网络地址转换 (Network Address Translator, NAT)是 SIP 自提出起一直关注的问题。为了传输媒体流时产生的时延最小,SIP 被设计成端到端 (Peer-to-Peer, P2P)的通讯,具体来说,就是通过 SIP 协商后,最终需要 NAT 后的用户代理(User Agent, UA)直接给另一个 UA 发送媒体流。SIP 数据包中包含了会话建立以及会话内容传输需要的地址和端口信息,这些信息在穿越 NAT 时会由于映射或防火墙限制的原因变得无效,从而导致 UA 之间无法使用这些信息完成会话的建立和会话内容的传输,这就是 SIP 穿越 NAT 的问题。如果 UA 处于对称类型的 NAT 之后,问题会变得更加复杂。SIP 穿越 NAT 问题已成为 VoIP 业务开展的最大障碍之一。

2. SIP 相关协议及其 NAT 穿越技术

2.1 SIP 相关

会话(Session)是用户间的数据交换过程,很多互联网业务应用都需要会话的创建与管理功能,为此 IETF 起草会话发起协议 SIP,作为 IP 网络多媒体业务的核心协议。SIP 包括基础协议 SIP 和会话描述协议 SDP(Session Description Protocol)。SIP 用于建立、调整

和终止会话,而以基于文本的 SDP 媒体描述作为消息体嵌入到 SIP 数据包中,为媒体流的建立提供地址信息和媒体参数,使得呼叫建立的同时完成媒体通路的建立。

SIP 是基于客户机/服务器结构的,它包含两类组件:用户代理 UA 和网络服务器(Network Server)。SIP 协议消息分为请求和响应两类,请求是由客户机发往服务器,而响应由服务器发往客户机。下图为 SIP 请求消息数据包的格式。



图 1 SIP 请求消息格式

用户代理又分用户代理客户端(UAC)和用户代理服务器(UAS)。SIP 网络服务器分为代理服务器(Proxy)、重定向服务器(Redirect Server)、注册服务器(Register)。

SIP 呼叫流程支持三种方式:

点对点直接呼叫方式,即由 UAC 向 UAS 直接呼叫。

代理服务器方式,即由代理服务器代表 UAC 向

被叫发起呼叫。

重定向服务器方式,即由 UAC 在重定向服务器的辅助下进行重定向呼叫。

以下是代理服务器方式流程步骤说明:

1) 主叫 UA1 向代理服务器发送 INVITE 请求,代理服务器接收 INVITE 请求,发送 100Trying 表示正在处理,并发送 INVITE 请求通知被呼叫方 UA2;

2) 被叫 UA2 向代理服务器返回连接成功消息 180Ring / 200OK,代理服务器向主叫返回连接成功消息 180Ring / 200OK;

3) 主叫 UA1 返回 ACK 确认建立连接成功,代理服务器返回 ACK 给被叫 UA2 确认建立连接成功;

4) 媒体流 RTP/RTCP 协议通讯建立。

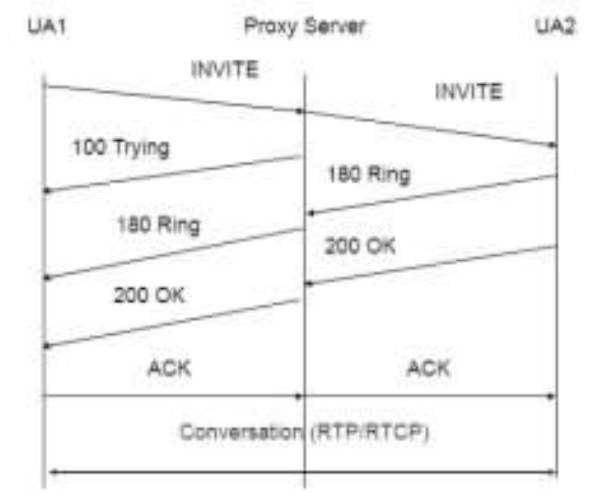


图2 代理服务器方式呼叫流程

2.2 NAT 的分类

NAT 仍是解决当前公用 IP 地址紧缺和网络安全问题的最有力手段,它主要有四种类型:完全圆锥型 NAT(Full Cone NAT),地址限制圆锥型 NAT (Address Restricted Cone NAT),端口限制圆锥型 NAT (Port Restricted Cone NAT),对称型 NAT (Symmetric NAT)。前三种 NAT,只要本地绑定的 UDP 端口相同,发出的目的地址不管是否相同,都使用同一个 Session,统称为 Cone 型 NAT。



图3 Cone 型 NAT

而对称型 NAT 的映射则同时关联源地址和目的地址,本地绑定的 UDP 端口相同,发出的目的 IP 地址

不同,则会建立不同的 Session。



图4 对称型 NAT

2.3 SIP 协议的 NAT 穿越技术

针对 NAT 问题目前有多种技术方案,典型的包括 ALG、MidCom、UPnP、隧道机制、STUN、TURN、ACM、ICE、SBC 等。每种方案都有其优缺点,其中 ALG, MidCom, UPnP 需要对 NAT 或者防火墙进行改造,而隧道机制执行效率低且增大了网络负载,STUN, TURN 和 ICE 需要对终端进行改造,应根据不同的接入方式和网络拓扑来应用不同的方案。

SIP 穿越 NAT 方案的基本要求是透明与高效。透明是指用户不需要关心网络拓扑结构和各种 NAT 类型,方案本身能适应各种网络环境;高效是说存储要求低,执行效率高,网络负载优,能在各种情况下对 NAT/FW 的穿越问题提供最优解。ICE 正是符合这样要求的一种良好的解决方案。

ICE (Interactive Connectivity Establishment) 提供的是一种框架,使各种 NAT 穿越技术可以实现统一。通过使用多种协议及网络连接机制,主要是使用 STUN (Simple Traversal of UDP Through NATs) 和 TURN(Traversal Using Relay NAT)两种协议,从而了解到客户端所在网络结构以及这些设备可以实现通信的各类网络地址。

SIP 应用 ICE 方案的基本算法是,呼叫流程两端 UA 都会去连接 STUN 和 TURN 服务器,并把得到的地址按优先级排列放在 SDP 消息中,然后两端相互收到并解析这个 SDP 消息,按照优先级尝试连接所给的地址,测试完所有的地址后,在可以互通的地址中选择优先级最高的进行通信。因此为了描述 ICE,实现上述算法,SDP 数据包中需添加一行信息如下:

a=alt: id 优先级: 从属 id 用户名 密码 IP 地址端口

其中 id 号定义为一个每次加一的序号数,优先级则从 1-0 递减,1 表示最高,从属 id 号表示这个地址是由测试连接哪个 id 号所代表的地址而得到的,这个一般会在测试连接 TURN 地址中用到,用户名和密码用于安全性认证,IP 地址和端口就是通过查询

STUN 和 TURN 服务器得到的。

3. 方案改进

3.1 ICE 方案的局限

ICE 方案作为最为全面的一种解决 NAT 穿越方案,其设计思想是综合使用 STUN 和 TURN 这两种穿越技术,最大限度地利用 STUN,当 STUN 无法作用的时候才使用 TURN,这样就能避免单独使用 STUN 不能穿越某些 NAT 的弊病和最大限度的减少 TURN 的使用。但是 ICE 还是有很多缺陷,首先如果很多通话在对称型 NAT 下,ICE 实际上就是使用 TURN,这就仍然避免不了 TURN 造成的语音延时问题。另外,ICE 中得到和测试地址的连通性过程过于麻烦,由于发送 SIP 信令之前就去拿地址,所以影响还不是很大,但是当测试地址是在用户拿起听筒准备讲话的时候,网络情况很差,测试时间很长,那么用户说的话很可能要很长时间才能传到会话的发起方,而发起方的测试过程也会造成对端用户要过一段时间才能听到主叫方的声音。

3.2 ICE 方案的改进

解决测试时间过长的问题可以有一种改进,因为测试的过程只是为了找一个可以连通的地址,ICE 设计的时候是测试所有的地址,可以改进为测试到一个可以互通的地址就产生应答信息,并且发送语言流,两端都是如此。因为按照优先级顺序测试的,所以可以保证连通的那个地址一定可以互通的地址中优先级最高的。

对于 TURN 带来的语音延迟和丢包可能性增大的问题,这是 TURN 技术的自身缺陷,要解决这个问题只有不使用 TURN 而采用其他方法来穿越 STUN 所不能穿越的对称型 NAT。改进的新方案需要在 SDP 中加入如下附加属性:

```
a=alt: id 优先级:用户名 密码 IP 地址端口
a=nat: symmetric
a=direction: <role>
```

第一行和 ICE 非常类似,含义也相同,所不同的是取消了 TURN 相关的部分,包括取 TURN 地址和从属 id 号。

第二行是新方案中需要的,如果本方发出的 SDP 消息中包括这行语句,则表示对端处于对称型 NAT 之后,由于只有一方处于这种 NAT 之后,所以只可能通话双方中一方的 SDP 消息含有这条属性行。

第三行和 SDP 协议 Connect Oriented Media 字段一样,加入连接属性,其中,role 的值包括:passive(接

收一个连接)、active(发送一个连接)和 both(既可接收也可发送一个连接)。

3.3 新方案对称型 NAT 的穿越

如何处理对称型 NAT 是新方案和 ICE 显著不同的地方,假设 A 处于对称型 NAT 而 B 处于 Cone 型 NAT,下图是一个应用新方案后的 VoIP 系统测试过程:



图5 对称型 NAT 下的测试过程

VoIP 业务呼叫前,A 和 B 连接公网上 STUN 服务器获取映射地址,从图中看出 B 从 STUN 得到的地址是 192.0.2.1:10234。当 B 呼叫 A 时,B 先去连 A 的物理地址,不通,然后再去连接 STUN 地址,因为 A 端是对称型 NAT,所以这个也无法通过,当 B 收不到回应时,它就意识到 A 端处于对称型 NAT 之后,那么它将会在自己的 SDP 消息加入如下信息:

```
c=IN IP4 192.168.2.1
m=audio 23456RTP/AVP 0
a=alt: 41.0:peerpassword192.168.2.123456
a=alt: 50.8:peerpassword192.0.2.110234192.0.2.110235
a=nat: symmetric
a=direction: passive
```

知道 A 是对称型 NAT 之后,B 所能做的就是等待 A 发起连接,此时 B 是连接的被动方面 A 是主动方。当 A 收到 B 的应答,它首先会检查 B 的地址连通性,因为 B 在 Cone 型 NAT 之后,所以 B 的 STUN 地址可以连通,A 会在给 B 的应答消息中增加 SDP 部分信息如下:

```
c=IN IP4 192.0.1.10:8076
m=audio 1010RTP/AVP 0
a=direction: active
```

B 收到应答消息后就会在本地建立一个地址映射表,通过地址映射表的信息,B 就可以把媒体流信息穿过 A 的 NAT 到达 A,这样双方媒体通信就建立起来了。

4. 结束语

(下转第 73 页)

判别分析进行研究,主要对二维主成分分析和二维线性判别分析的人脸识别算法进行研究并提出相应的改进算法并进行仿真。我们采用在图像矩阵的行和列两个方向上同时进行特征提取的改进算法,即有基于加权(2D) 2 PCA 人脸识别算法,这种算法能够消除图像行、列各自的相关性,减少特征数量,减小存储空间,提高识别速率。

四、基于视频监控的人脸识别系统的设计与实现:

该系统划分成几个模块:视频采集模块、用户注册及库模块、人脸识别模块

1.视频采集模块

该模块安装高清摄像头进行视频采集,在开发平台上,利用 Visual C++辅助 OpenCV 开源库,利用 OpenCV 视频采集函数进行编程实现。主要利用的采集函数有 CvCapture、CvCaptureFromCAM、CvReleaseCapture、CvQueryFrame。

2.用户注册及库模块

我们采用 AdaBoost 人脸检测算法来建立人脸识别库。

3.人脸识别模块

本模块是最关键模块,也就是识别出进入系统的人的身份。主要就是通过高清视频采集视频,利用 AdaBoost 人脸检测算法检测到人脸,确认检测到的人脸大小、位置,利用 CamShift 跟踪算法对检测到的人脸进行追踪,对追踪到的人脸图像进行处理,采用分块加权的 (2D)2PCA 算法提取人脸特征;然后根据分类规则进行比对,从而辨别出人的身份。

结论

随着计算机技术、传感器技术和仿真技术高速发展,人脸检测与识别技术具有越来越广泛的应用价值和重要的理论研究价值,已成为图像处理、人工智能、模式识别等领域中研究最为热门的课题之一,也相信在未来会发展的更好!

参考文献:

- [1]周杰、卢春雨《人脸自动识别方法综述》(《电子学报》)
- [2]周激流《人脸正面模式自动识别的方法的研究》(《四川大学学报》)
- [3]王耀南《计算机智能信息技术及其应用》(湖南大学出版社)
- [4]边肇祺、张学工《模式识别(第二版)》(清华大学出版社)
- [5]施卫斌《关于人脸识别技术在城市轨道交通的应用与研究》(《电子世界》)

(上接第 65 页)

本文提出的 SIP 穿越 NAT 的方案,是 ICE 完整解决方案的技术改进。ICE 方案中使用了 STUN 和 TURN,但是 TURN 对语音延迟等 VoIP 的关键问题带来很大影响,改进方案借鉴 ICE 的设计思想,即把多个优势互补的穿越方法综合运用以消除单个使用所带来的缺陷,对 ICE 扩展 SDP 协议的方法进行修改,从而避免了 TURN 的缺陷。

VoIP 系统中,终端如何有效地穿越各种 NAT 是一个关键问题,解决好这个问题,将会促进 VoIP 业务的应用和推广。本文提出的这种方案还可以作为 VoIP 以外的其他 SIP 协议高级应用(即时消息、游戏、视频监控等)的参考和借鉴。

参考文献:

- [1] K. Egevang and P. Francis, "Rfc 1631: The ip network address translator(nat)," [S] 1994.

- [2] J. Rosenberg and R. Mahy et. al., "Session Traversal Utilities for NAT(STUN)," [S] RFC 5389, IETF, October 2008.
- [3] J. Rosenberg, R. Mahy, and P. Matthews, "Traversal using relays aroundnat (TURN): Relay extensions to session traversal utilities for nat (stun)," [S] RFC 5766 (Review Copy), IETF, February 2010.
- [4] J. Rosenberg, R. Mahy, and jdrosen.net, "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols," [S] RFC5245, IETF, April 2010
- [5] 魏立峰等。一种媒体流穿越 NAT 的算法设计与实现,[J]《计算机工程》,2009 年 12 月
- [6] 刘春燕等。基于端口探测的 SIP 穿透 NAT 的设计与实现,[J]《计算机工程》,2008 年 9 月
- [7] 刘杨等。基于 ICE 方式的综合性 SIPNAT 解决方案设计与实现,[J]《小型微型计算机系统》,2006 年 5 月