一种利用 TURN 穿越对称型 NAT 方案的设计与实现

黄佳庆, 闵 江, 程文青
(华中科技大学 电子与信息工程系, 湖北省智能互联网技术重点实验室, 湖北 武汉 430074)

摘 要: 针对在 IP 上承载语音和视频的协议的控制通道/媒体通道无法穿越对称 NAT 与公网进行互通的问题, 设计并完成基于 SIP 协议上采用 TURN 技术的一种穿越对称 NAT 的方案: 利用 TURN 服务器的中转, TURN 客户端穿越对称 NAT, 与外部主机进行正常通信; 与 STUN 结合, 既可以穿越所有类型的 NAT, 又可降低 TURN 服务器的负载. 提供该模块的封装接口, 易于移植到其他类型的终端上. 本方案已成功应用于基于嵌入式 Linux 平台的 VoIP 网关中.

关键词: 网络地址转换; 对称型 NAT; 通过中继方式穿越 NAT; 基于 IP 的语音; 会话初始协议
中图分类号: TP393 文献标识码: A 文章编号: 1000-7180(2009)04-0255-05

Design and Implementation of a TURN Based Solution to Symmetric NAT

HUANG Jia-qing, MIN Jiang, CHENG Wen-qing
(Department of Electronics & Information Engineering, Huazhong University of Science & Technology, Hubei Provincial Key Laboratory of Smart Internet Technology, Wuhan 430074, China)

Abstract: The control/media channel carrying voice/video protocols based on IP faces the challenge in traversing symmetric NAT. This paper handles this issue, and designs and implements a TURN based solution to traverse symmetric NAT with SIP protocol. The TURN client traverses through the NAT to communicate with external host by the forwarding of TURN server. With the combination of STUN, this scheme can not only traverse all types of NATs, but also reduce the load of TURN server. This paper supplies the encapsulation interface of this module so that it can be transplanted to other types of terminals easily. This solution has been adopted successfully in the VoIP Gateway based on the embedded Linux platform.

Key words: network address translator (NAT); symmetric NAT; traversal using relay NAT (TURN); voice over Internet protocol (VoIP); session initiation protocol (SIP)

1 引言

NAT 是一个 Internet 工程任务组 (Internet Engineering Task Force, IETF) 标准, 用于允许专用网络上的多台 PC 使用专用地址段. 在 VoIP 的应用中, 必须解决 NAT 穿越问题[1-3].

现有的几种穿越方式, 如 NAT/ALG 和 MIDCOM 方式要求现有的 NAT/FW 设备需升级支持相应协议, 这对已大量部署的 NAT/FW 设备来说, 是很困难的. STUN (Simple Traversal of UDP Through Network Address Translators, UDP 对 NAT 的简单穿越方式)[4] 方式采用服务器/客户端模式, 无需 NAT/FW 升级, 但它无法穿越对称型 NAT (Symmetric NAT). 关于对称 NAT 型的穿越, 协议标准尚不成熟和完善, 这使得对对称型 NAT 的穿越, 存在较大难度. 胡宁等[5] 提出基于 H.323 的对

收稿日期: 2008-06-13
基金项目: 国家自然科学基金项目(60773193); 华中科技大学校基金项目(2008); 华中科技大学电信系基础研究基金项目(2008)

称 NAT 穿越.

文中依据通过中继方式穿越 NAT(Traversal Using Relay NAT, TURN)[6] 草案, 设计并实现了一种基于 SIP 协议能穿越对称型 NAT 的 NAT 穿越方案.

这种方式应用模型综合 STUN 和 TURN 两种不同的 NAT 穿越方式的优点. 既解决了 STUN 应用无法穿越对称型 NAT 的缺陷, 又降低 TURN 服务器的负荷.

2 NAT 穿越方案设计

本节在阐述中, 均将 STUN 与 TURN 结合考虑, 第 4 节服务器和客户端模块的实现中, 则重点阐述 TURN 部分.

2.1 总体方案

文中参考 STUN 草案以及 TURN 草案, 选择 STUN 与 TURN 结合的方式穿越所有类型的 NAT. 使用STUN 完成 NAT 是否存在以及 NAT 类型的检测, 并获知 STUN 服务器分配的绑定地址. 如果 NAT 设备为非对称 NAT, 则使用 STUN 进行穿越; 如果 NAT 设备为对称 NAT, 则使用 TURN 进行穿越. 这样既结合了 STUN 不会增加 NAT 和服务器负担的优势, 又使用 TURN 弥补了无法穿越 NAT 的缺陷. 该系统应用体系结构如图 1 所示.

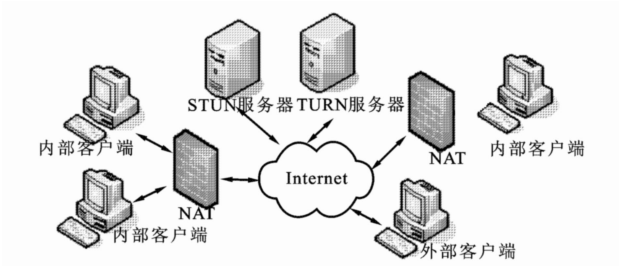

图 1 系统应用体系结构图

STUN 服务器和 TURN 服务器被放置在公网, 它们可以放在同一台主机中, 只要端口不冲突就可以. 在本系统中, 为了减轻运行 TURN 服务器的主机中继的负担, 将 STUN 服务器和 TURN 服务器分别运行在两台主机上. 而 NAT 内的客户端上, 运行有 STUN 客户端和 TURN 客户端.

2.2 TURN 服务器模块的设计

图2 为 TURN 服务器端模块图. TURN 服务器包含消息解析器、消息生成器, 将一次会话中用户名、密码、源地址、绑定端口以及生命期联系在一起的绑定模块, 还有数据转发模块.

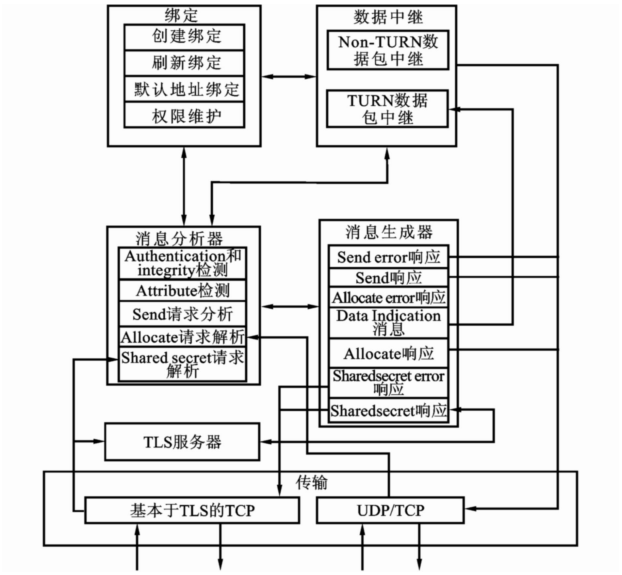

图 2 TURN 服务器模块

2.3 TURN 客户端模块的设计

图 3 为TURN 客户端模块图. TURN 客户端包含消息解析器、消息生成器以及发现模块. TURN 客户端的消息生成器负责 Allocate 请求、Send 请求的构造, 消息解析器负责解析来自于 TURN 服务器的应答并做出相应的处理.

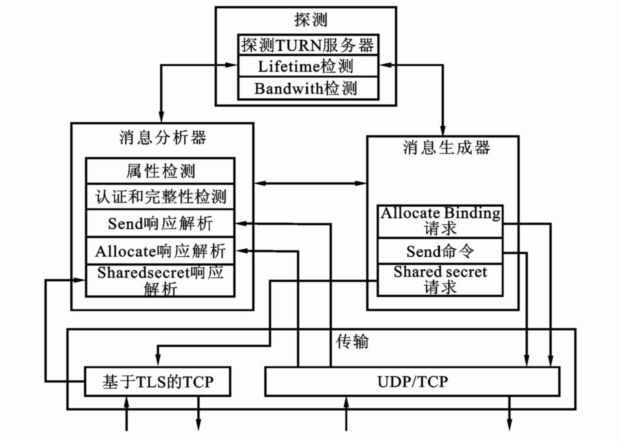

图 3 TURN 客户端模块

3 NAT 穿越方案实现

3.1 系统软件流程

图 4 是系统软件流程图. 内部客户机启动 STUN 客户端与公网上的 STUN 服务器交互, 从而获知 NAT 信息. 如果该客户机位于 NAT 之外, 则不做任何处理; 如果位于非对称 NAT 之内, 就使用 STUN 服务器返回的消息处理, 而如果位于对称 NAT 之内, 则启动 TURN 客户端程序, 并与公网上的 TURN 服务器交互. 建立 RTP 通道, 即可外部主

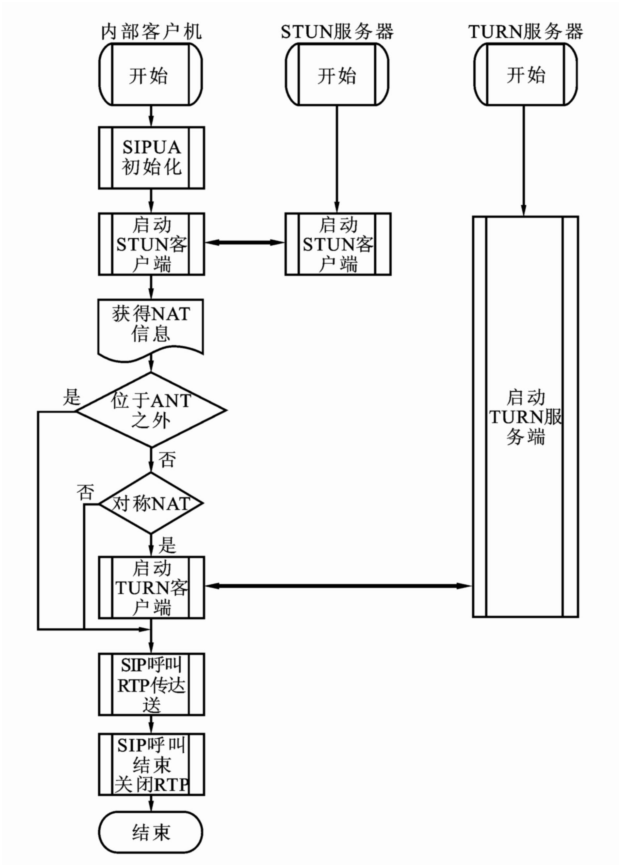

图 4　系统软件流程图

机进行通信. 需要结束通信时, 就关闭 RTP 通道.

3.2　TURN 服务器模块的实现

TURN 服务器首先设置其对外端口, 默认设置为 3478, 可以通过配置文件进行修改. 创建活动列表, 初始情况下活动表为空, 在后续接收到某类消息的触发下, 会添加或修改活动表. 程序启动时设置定时器, 并判断是否超时以及如果超时, 为哪一类超时. 如果为状态转换超时, 表示状态转换没有完成, 则主动将外部活动地址设置为下一个外部地址, 并发送 Set Active Destination 应答, 表示接受 TURN 客户端设置活动目的地址的请求. 这样, TURN 客户端与外部用户之间后续的数据包都不需要再进行封装, 而是直接进行转发. 这样将包的中继从应用层移至传输层处理, 降低服务器负荷. 如果是尚处于活动状态的列表超时, 则更新定时器, 允许它继续为活动状态. 否则, 删除绑定.

如果不存在超时, 则监听其传输列表上的端口. TURN 服务器当且仅当外部客户端在 TURN 服务器上建立了许可权限的时候, TURN 服务器才会接受来自外部客户端的 UDP 数据包或者 TCP 连接. 客户端是通过 TURN 服务器向指定的传输地址发送数据包来建立许可权限的. 文中仅考虑 TURN 的 UDP 实现, 故忽略 TCP 连接. 对接收到的包, 服务器判断其类型.

如果接收到的包不是 UDP 包, 则服务器结束该连接. 如果接收到的包是 UDP 包但不是 TURN 类型, 则查看源地址是否与内部五元组匹配. 如果匹配, 则表示这个包来自 TURN 客户端, 并且该客户端之前已经向 TURN 服务器发送过 Send 请求, 并成功登记, 所以此时将负载发送该客户端对应的活动远端. 如果不是来自内部五元组, 则查找允许表, 查看它是否为活动五元组. 如果是, 则表示这个包来自与外部用户, 并且该外部用户已通过内部 TURN 客户端的通信允许, 于是 TURN 服务器直接将数据包转发至内部 TURN 客户端. 如果源地址与活动五元组不匹配, 则将数据包放在 Data Indication 中, 发送给内部 TURN 客户端. 如果接收到的包是 UDP 包且为 TURN 类型, 则依据类型不同进行相应处理.

在该方案的实现中, 使用 C++ 作为编程语言, 服务器和客户端都使用统一的类来实现. 所有的类都继承于类 Mobject, 它包含一个对计数器的引用, 以决定何时将对象从堆中移出.

3.3　TURN 客户端模块的实现

当 SIP UA 通过 STUN 交互发现自己处在对称 NAT 内时, 启动 TURN 客户端. TURN 客户端返回分配的地址以及数据包供其他模块使用.

TUNR 客户端启动后, 首先发送初始 Allocate 请求, 用于向 TURN 服务器索要分配的绑定地址和端口. 如果对方已经是活动目的地, 即当前正在通信的用户, 则表示 TURN 客户端已经针对该外部用户向 TURN 服务器发送过 Send 请求和 Set Active 请求且被成功应答, 可直接发送消息. 否则, 需要创建 Send 请求. 如果尚未将正在通信的外部用户成功设置为活动目的地, 则要发送的数据包作为 Send 请求的负载来发送. 接着判断是否为活动目的地, 如果不是则发送 Set Active Destination 请求. 接着对接收到的 TURN 应答进行相应处理. 如果为 Data Indication, 则将负载内容拷贝到缓存, 以供其他模块(SIP 模块、RTP 模块) 使用. 如果为 Set Active Destination 应答, 则设置活动目的地址. 如果为 Allocate 应答且绑定未刷新, 则设置绑定刷新为真. 之后将负载均拷入缓存.

TURN 客户端为了不停地刷新与 TURN 服务器之间的绑定, 需要额外起一个线程来完成这个工作. 该线程不断创建 Allocate 后续请求, 并携带新的生命期字段, 以刷新绑定. 两个线程之间通过 flag 置位来进行交互.

客户端使用 C++ 作为编程语言开发,为方便移植,提供用 C 封装的接口. 例如函数 void turn_start(char * turnServer_Addr, char * turn_username, char * turn_passwd, int turn_lifetime); 它向 TURN 服务器发送绑定请求,并获得分配的地址和端口.

3.4 系统消息流程

本方案应用在使用 SIP 作为信令传输协议的 VoIP 网关中,但可以推广到基于其他协议的终端上. 图 5 为整个系统整体的消息流程图. 为了获知是否存在 NAT 以及 NAT 的类型,用户代理客户端 A 会首先向 STUN 服务器发送请求. 如果获知位于 NAT 之内,则开始与 TURN 服务器进行交互.

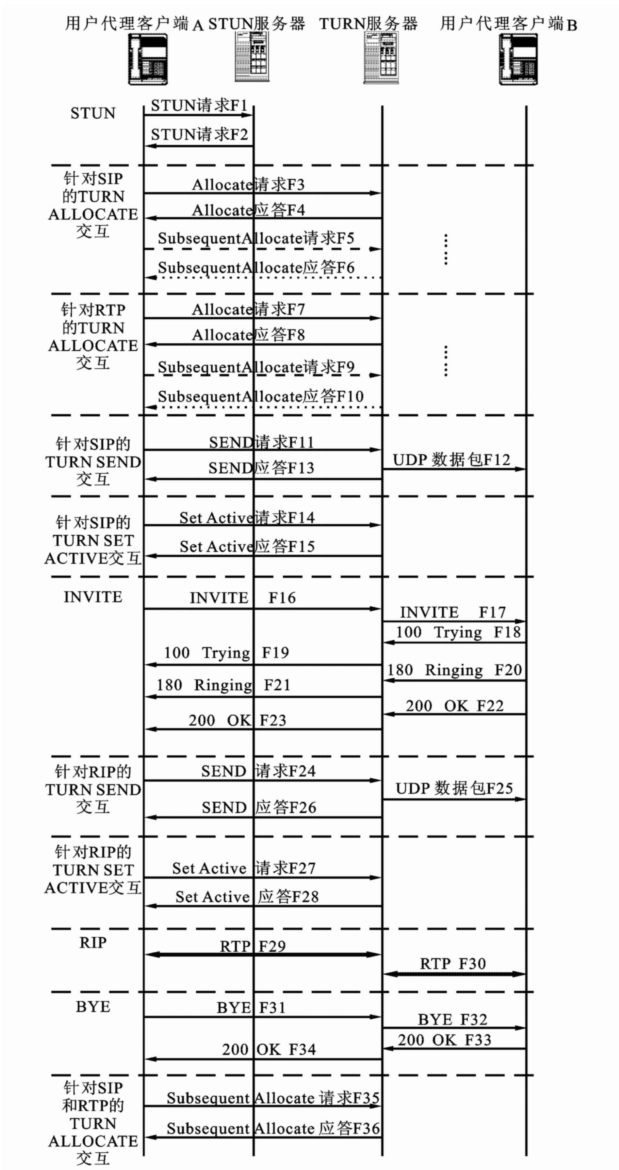

图 5 整体消息流程图

为了与 NAT 之外的用户代理客户端 B 之间完成 SIP 信令的正常通信,用户代理客户端 A 先向 TURN 服务器依次发送针对 SIP 和 RTP 的 Allocate 请求,要求服务器为客户端 A 分配用于信令传输和媒体流传输的端口. 在端口被成功分配之后,A 向 TURN 服务器发送以用户代理客户端 B 的 IP 地址和 SIP 端口为目的地的 Send 请求. 在 TURN 服务器向 A 返回成功的 Send 应答后,A 通过 TURN 服务器穿越对称 NAT,向 B 发送 INVITE 请求以建立 SIP 会话. 在收到 200 OK 成功应答后,A 向 TURN 服务器发送以 B 的 IP 地址和 RTP 端口为目的地的 Send 请求,接着发送同样目的地址的 Set Active 请求,以激活与 B 之间免封装的 RTP 交互.

在此期间,A 仍要不停地向 TURN 服务器发送 Subsequent Allocate 请求,以维持绑定. 在发送 BYE 消息后,A 与 B 之间结束 SIP 以及 RTP 会话. 最后,A 向 TURN 发送 lifetime 为 0 的 Subsequent Allocate 请求,以移除绑定.

4 测试结果与分析

测试环境如图 6 所示.

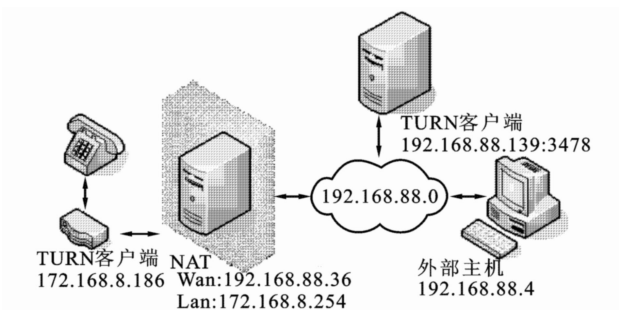

图 6 测试环境

使用装有双网卡的主机作为对称 NAT,集成有 VoIP 功能的嵌入式板上运行有 TURN 客户端程序,并连在 NAT 的 LAN 下,NAT 的 WAN 和 TURN 服务器、外部主机均连在 192.168.88.0 网段.

NAT 的 WAN IP 为 192.168.88.36,LAN IP 为 172.168.8.254,使用 iptables[7] 将其配置成对称 NAT,WAN 口连接 192.168.88.0 网段.

TURN 服务器的 IP 为 192.168.88.139,使用 3478 作为 TURN 服务的对外端口.

TURN 客户端的 IP 为 172.168.8.186,通过 HUB 连在 NAT 的 LAN 口. 它的 FXS 端口上连接有普通电话机.

外部主机的 IP 为 192.168.88.4,运行着一个基于 PC 的 SIP 电话.

测试过程中, 对称 NAT 之内的电话与外部的 SIP 电话多次通话, 均正常. 在 TURN 服务器的终端显示上, 可以看到有数据的转发过程.

从结果中可以看到, 通过 TURN 服务器的中转, TURN 客户端与外部主机之间通信正常. 说明通过 TURN 服务器/客户机成功完成了对称 NAT 的穿越.

5　结束语

文中采用 TURN 技术设计并实现对称 NAT 的一种穿越方案, 该方案与 STUN 结合, 可以穿越所有类型的 NAT, 并测试系统的功能以及稳定性. 结果表明方案设计和实现的正确性和有效性.

参考文献:

[1] Internet Engineering Task Force. RFC 1631. The IP network address translator(NAT)[S]. USA: ISOC, 1994.

[2] Internet Engineering Task Force. RFC 2663. IP network address translator(NAT) terminology and considerations [S]. USA: ISOC, 1999.

[3] Internet Engineering Task Force. RFC 3261. SIP: session initiation protocol[S]. USA: ISOC, 2002.

[4] Internet Engineering Task Force. RFC 3489. STUN – simple traversal of user datagram protocol(UDP) through network address translators(NATs) [S]. USA: ISOC, 2003.

[5] 胡宁, 张德运, 胡国栋. 一种 H.323 通信穿越对称 NAT 的方法[J]. 微电子学与计算机, 2005, 22(3): 81– 83.

[6] Internet Engineering Task Force. Draftrosenberg– midcom – turn– 07. Traversal Using Relay NAT(TURN)[S]. USA: ISOC, 2005.

[7] Suehring S, Ziegler R L. 何泾沙, 译. Linux 防火墙[M]. 3 版. 北京: 机械工业出版社, 2006.

作者简介:

黄佳庆　男, (1972–), 博士, 副教授. 研究方向为网络通信、P2P、网络编码、多播.

闵　江　女, (1984–), 硕士研究生. 研究方向为嵌入式系统、VoIP 网络通信技术、多媒体网络通信.

程文青　女, (1964–), 博士, 教授. 研究方向为媒体网络通信.

(上接第 254 页)

表 2　RS232 接口正常和受损时的注入监测电压的上下界(置信水平 90%)

	正常	受损
发送端口	< 126.7 V	> 243.2 V
接收端口	< 128.6 V	> 239.3 V

4　结束语

RS232 接口受电磁脉冲干扰受损的主要原因在于, 通过耦合夹钳在 RS232 数据传输线上产生的感生电流在端口上产生高压, 该高压作用于接口的集成电路, 在高于一定电压阈值时激发低阻通路, 电流瞬间增大, 注入到低阻通路上的功率以及能量也急剧增大, 在高于热损阈值时, 造成接口电路受损. 通过 Logistic 回归模型计算得出置信水平为 90% 的 RS232 接口正常工作以及受损时的电磁脉冲幅度上下界. 该结论对评估 RS232 接口在某电磁脉冲幅度作用下的可靠性提供了依据.

参考文献:

[1] 米切尔• 麦迪圭安. 电磁干扰排查及故障解决的电磁兼容技术[M]. 刘萍, 译. 北京: 机械工业出版社, 2003: 51 – 63.

[2] 蔡仁钢. 电磁兼容原理、设计和预测技术[M]. 北京: 北京航空航天大学出版社, 2003: 42– 62.

[3] 林国荣. 电磁干扰及控制[M]. 北京: 电子电子工业出版社, 2003: 155– 162.

[4] 孙传友. 测控系统原理与设计[M]. 北京: 北京航空航天大学出版社, 2003: 103– 117.

作者简介:

高　晶　女, (1983–), 硕士研究生. 研究方向为指挥自动化.

孙继银　男, (1952–), 教授. 研究方向为虚拟现实与多媒体技术.

赵星阳　男, (1980–), 博士研究生. 研究方向为指挥自动化.

柴焱杰　男, (1978–), 博士研究生. 研究方向为指挥自动化.

王　波　男, (1984–), 硕士研究生. 研究方向为网络应用.

时　零　女, (1983–), 助理工程师. 研究方向为卫星导航技术.