基于 STUN 协议的 NAT 穿透技术通讯效率优化研究

杨富钧，孙芊，高佳宁，刘美，廖雪花*

四川师范大学计算机科学学院，四川成都 610101

摘要: NAT（Network Address Translator）技术虽然解决了 IP 地址短缺的问题，但该技术会阻碍主机之间进行 P2P（Peer-to-Peer）通信，NAT 穿透就是根据设备的映射规则，通过技术手段找出一种能让外部数据报通过 NAT 设备的方法，从而建立稳定的 P2P 连接。为了保证 P2P 网络内的节点完成高质量通信，本文对整个 P2P 通信过程展开研究，针对 NAT 类型检测过程复杂繁琐和穿透过程成功率较低等问题，提出一种基于 STUN（Simple Traversal of UDP Through NATs）协议穿透的优化策略。该策略通过重新划分 NAT 类型、改进 NAT 类型检测方法、引入网络状态检测算法和优化通信流程等措施，保障 P2P 网络中各节点之间顺畅、高质量完成通信。实验结果表明，本文提出的基于 STUN 协议的 NAT 穿透策略具有更低的资源消耗、较强的抗干扰能力和较高的穿透成功率，避免服务器出现性能瓶颈，为整个通信过程提供高质量网络服务。

关键词: P2P; NAT 类型检测; STUN; 网络状态检测算法; NAT 穿透

DOI: 10.57237/j.cst.2023.02.005

Research on Optimizing the Communication Efficiency of NAT Penetration Technology Based on STUN Protocol

Yang Fujun, Sun Qian, Gao Jianing, Liu Mei, Liao Xuehua*

School of Computer Science, Sichuan Normal University, Chengdu 610101, China

Abstract: NAT (Network Address Translator) technology solves the problem of IP address shortage, but this technology can prevent P2P (Peer-to-Peer) communication between hosts. NAT penetration is the technical means to find a way to allow external datagrams to pass through the NAT device according to the mapping rules of the device, thus establishing a stable P2P connection. In order to ensure that the nodes in a P2P network complete high-quality communication, this paper investigates the entire P2P communication process and proposes an optimisation strategy based on STUN (Simple Traversal of UDP Through NATs) protocol penetration to address the problems of complex and tedious NAT type detection process and low success rate of the penetration process. By reclassifying NAT types, improving NAT type detection methods, introducing network state detection algorithms and optimising the communication flow, the strategy ensures smooth and high-quality communication between nodes in a P2P network. The experimental results show that the STUN protocol-based NAT penetration strategy proposed in this paper has lower resource consumption, stronger

*通信作者: 廖雪花, 191716312@qq.com

收稿日期: 2023-02-28; 接受日期: 2023-04-15; 在线出版日期: 2023-04-25

anti-interference capability and higher penetration success rate, avoiding performance bottlenecks in the server and providing high-quality network services for the whole communication process.

Keywords: P2P; NAT Type Detection; STUN; Network State Detection Algorithm; NAT Penetration

1 引言

近几年来，中国互联网技术蓬勃发展，上网人数急剧攀升，各种通讯设备的人均持有量也大幅增加，原本稀缺的IPV4网络地址变得更加无法满足各种设备的上网需求。为了从根源上解决 IPV4 地址短缺问题，国际互联网工程任务组（The Internet Engineering Task Force, IETF）提出了解决方案 IPV6 协议。受到替换成本、花费时间、复杂程度等因素的制约，IPV4 的替代方案 IPV6 离大规模普及还有相当长一段时间[1]。在这个过渡过程中，网络地址转换（Network Address Translator，NAT）技术得到了广泛的应用和发展，从一定程度上缓解了 IPV4 地址短缺的问题[2]。

NAT 是一种将数据报中的 IP 地址转换为另一种 IP 地址的技术。当内网主机需要访问外网时，NAT 主要实现内部网络和外部网络之间的 IP 转换，这种通过使用少量的公网 IP 地址代表较多的私网 IP 地址的方式，极大程度提高 IP 地址的利用率[3]。同时，结合防火墙技术，把一些重要的服务器隐藏起来，使内网与外网隔离，从而避免来自外部网络的攻击，保障内部网络的安全[4]。

P2P（Peer to Peer）技术是互联网即时通讯领域中的新技术，它改变了传统 C/S 通讯模式的交互体系，采用全新的理念提出对等实体的概念，利用彼此相连的计算机互相提供服务和资源，缓解了中心服务器的负载压力，提高了系统整体的处理和反应能力[5]。实现 P2P 网络节点之间顺畅、高质量通信的关键是进行 NAT 穿透，由于数据传输依赖于建立在 NAT 上的映射表项，如果没有相应的表项，外网主机无法直接访问内网主机，并且网络结构复杂和 NAT 类型多样，造成 NAT 穿透存在穿透率低甚至无法穿透的缺点，大量科研工作者提出一些解决方案并将其应用到各类即时通讯系统中。

本文针对不同场景提出了相应的基于 STUN 的穿透策略，这些策略无需对现有设备进行更改并且实现简单。相较于传统的穿透策略，解决了抗干扰能力弱和对成型 NAT 穿透成功率较低等问题，能够很好的应用于对网络安全要求较高而使用对称型 NAT 的场景下。

2 相关工作

NAT 设备的出现造成 P2P 通信变得非常困难。节点之间进行双向通信，必须穿透 NAT。NAT 穿透技术主要分为两类，一类是依赖于 NAT 设备，这类技术主要的方案有应用层网关技术（Application Level Gateway, ALG）、通用即插即用（Universal Plug and Play, uPnP）、隧道技术等。

ALG 将一些应用层协议报文中的地址进行转换处理，从而保证某些应用层协议也能透明完成 NAT 转换，缺点是只适用于应用群体内部之间；UPnP 主要以 Internet 标准和技术为基础，用于实现网络中各种设备彼此自动连接和协同工作，并简化相关网络实现。但是，一旦开启 UPnP，路由防火墙将完全失效，主机容易受到网络窥探和感染病毒等问题影响[6]；隧道技术是将隧道服务器放置于公网中，处于私网的隧道客户端通过隧道协议与隧道服务器建立一条隧道，从而实现 NAT 穿透，但隧道技术需要额外的硬件设备，成本较高。

另一类是基于一些穿透协议且不依赖额外的硬件设备。这类技术主要的有 STUN（Simple Traversal of UDP Through Network Address Translator）、TURN（Traversal Using Relay NAT）、ICE（Interactive Connectivity Establishment）等，大量科研工作者基于这些协议提出了改进方案，但这些方案都存在一些问题。

Srirama 等人[7]提出基于 UDP 打洞的穿透策略，节点借助于一个位于公网带有 Rendezvous 服务器在 NAT 设备上建立临时的地址绑定，公网服务器命令对端节点与在 NAT 上的绑定地址通信。该策略能够较好的解决非对称型 NAT 穿透，实现过程简单，适用场景广泛，但需要解决对称型 NAT 穿透和 NAT 地址绑定失效等问题；Wang 等人[8]提出 PS-STUN 算法，通过节点改变源端口与对端进行通信。该策略能够基本实现递增型 NAT 穿透，但无法穿透随机型 NAT，并且在实际应用中源端口一般是固定不变的；Wei 等人[9]提出通过限制 TTL 大小的方式控制 NAT 设备端口分配的策略，但是，TTL 的限制需要获取系统 root 权限，在实际应用中获取较为困难，适用性较低；D'Angelo 等人

[10]提出基于 websocket 协议实现节点之间双向通信。但是，该穿透策略需要高性能硬件设备，实际使用环境中资金成本较大，实用性较低；郑浩[11]提出组合两台单网卡服务器提供 STUN 服务，简化 NAT 检测流程，缩短检测时间。该策略能够一定程度缩小 NAT 穿透时间，但 NAT 类型检测阶段只需要一张网卡，并且探测流程可以进一步优化从而缩短时间；冯金哲等人[12]提出了一种穿透对称型 NAT 的新策略，解决了部分对称型 NAT 穿透难题。但该策略没有考虑网络拥塞情况下进行遍历扫描对整个网络通信造成的影响，容易导致网络丢包严重，甚至网络崩溃。

3 相关技术

3.1 NAT 原理

网络地址转换（Network Address Translation，NAT）是将 IP 数据报文头中的 IP 地址转换为另一个 IP 地址的过程，主要用于实现内部网络访问外部网络的功能。转换具体过程如图 1 所示：当内网（A 类：10.0.0.0-10.255.255.255；B 类：172.16.0.0-172.31.255.255；C 类：192.168.0.0-192.168.255.255）主机需要与外部网络中的主机进行通信时，内网主机发送数据报到达 NAT，NAT 设备用自身的公网 IP 地址和分配的端口替换数据报中的源 IP 和源端口，在自身的映射表中记录下本次通信；当外部网络目标主机数据返回时，NAT 设备查询映射表，根据映射表中的表项信息，将数据报转发给内网中的对应主机。根据转换过程可知，可以将 NAT 设备的公网 IP 地址充分复用，以此缓解 IPv4 地址紧缺问题[13]，同时，能够将内网中一些重要的服务器 IP 地址隐藏起来，使内网和外网隔离，保障内网服务器安全[14]。

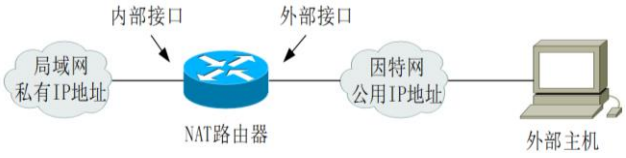

图 1 NAT 转换示意图

3.2 NAT 类型

不同的 NAT 设备有着不同的地址映射规则和数据过滤策略。NAT 设备类型一般可以划分为以下四类，即：完全锥型 NAT（Full Cone NAT）、限制锥型 NAT（Restricted Cone NAT）、端口限制锥型 NAT（Port Restricted Cone NAT）、对称型 NAT（Symmetric NAT）[15]。

(1) 完全锥型 NAT（Full Cane NAT）

当内网主机 A 向公网主机 Y 发送请求时，主机 A 的 IP 地址和端口信息都会被映射成同一个公网 IP 地址和端口。任何公网主机向映射的公网 IP 地址和端口发送报文，都可以实现和内网主机 A 建立通信。通信流程如图 2 所示。

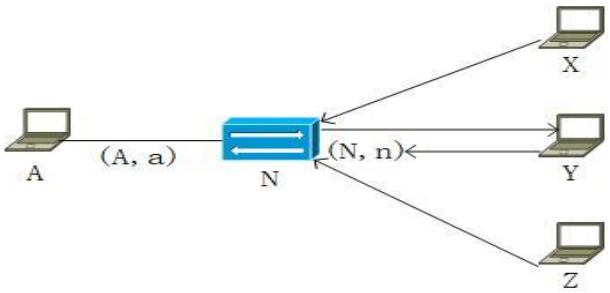

图 2 完全锥型 NAT 示意图

(2) 限制锥型 NAT（Restricted Cone NAT）

当内网主机 A 向公网主机 Y 发送请求时，主机 A 的 IP 地址和端口信息都会被映射成同一个公网 IP 地址和端口。与完全锥型不同的是，当且仅当内网主机 A 之前进行过数据通信的外网主机 Y（可以使用任何端口）才能与主机 A 进行通信，外网其他主机不能与主机 A 进行通信。与完全锥型 NAT 相比，限制锥型 NAT 多了 IP 地址限制。通信流程如图 3 所示。

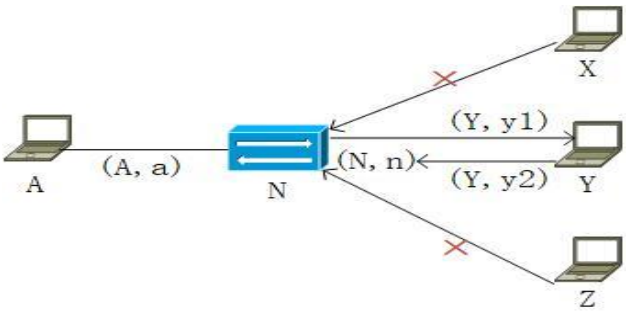

图 3 限制锥型 NAT 示意图

(3) 端口限制锥型 NAT（Port Restricted Cone NAT）

当内网主机 A 向公网主机 Y 发送请求时，主机 A 的 IP 地址和端口信息都会被映射成同一个公网 IP 地址和端口。与限制锥型不同的是，当且仅当内网主机 A 之前进行过数据通信的外网主机 Y（只能使用先前建立通信的端口）才能与主机 A 进行通信，外网其他主

机和主机 Y 的其他端口都不能与主机 A 进行通信。与限制锥型 NAT 相比，端口限制锥型 NAT 多了端口限制。通信流程如图 4 所示。

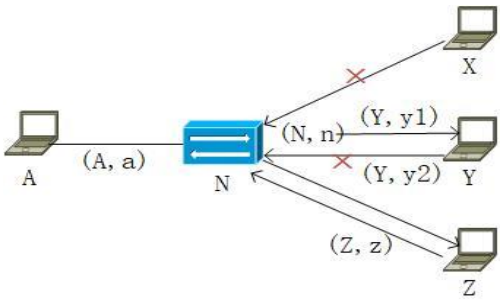

图 4 端口限制锥型 NAT 示意图

(4) 对称型 NAT（Symmetric NAT）

所有从同一个内网 IP 地址和端口发送到外网的一个特定的目的 IP 地址和端口的情况，都会被映射成同一个公网 IP 地址和端口。如果同一台主机使用相同的源 IP 地址和端口发送数据报，但发送的目的地址不同，NAT 将会使用不同的映射。通信流程如图 5 所示。

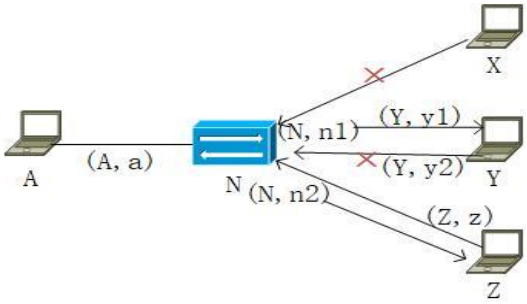

图 5 对称型 NAT 示意图

对称型 NAT 的映射关系是由源 IP、源端口、目的 IP、目的端口这四元组确定的，只要其中任意一项发生变化，映射关系都会改变。对称型 NAT 的映射分配规则分为以下三种：

①固定增量型，即在上一次分配的端口号上增加或减少一个固定值。

②小范围随机型，即在上一次分配的端口号附近小范围内随机分配一个未使用的端口号。

③完全随机型，即在 1024 至 65535 中间随机生成一个未使用的端口号。

3.3 网络状态检测算法

对称型 NAT 穿透，采用策略是进行端口预测，端口预测需要发送大量数据包到网络中进行 NAT 穿透，可能造成网络拥塞，甚至网络崩溃。因此，引入网络网络状态检测算法，动态决定端口预测时机。

通过 UDP 数据报单程时延波动预测网络拥塞程度，规定 UDP 数据报的接收时间间隔和发送时间间隔的差值达到一定程度就可以认为网络发生了拥塞。根据时间间隔差值的偏离程度可以将 UDP 拥塞级别划分为空闲、良好和拥塞三种情况。若第 n 个数据报发送时的时间戳为 sT_n，第 n 个数据报接收时的时间戳为 rT_n，第 n+1 个数据报发送时的时间戳为 sT_{n+1}，第 n+1 个数据报接受时的时间戳为 rT_{n+1}，假设 L 为拥塞级别，其计算方法如公式(1)所示。

$$L = \left|\frac{(rT_{n+1}-rT_n)-(sT_{n+1}-sT_n)}{sT_{n+1}-sT_n}\right| \times 100\% \quad (1)$$

上式中，L 的值越大，表明网络中数据报的延迟越高，网络拥塞程度越严重。其拥塞级别的划分如表 1 所示。其中，Vi 为网络低负载状态的上限值，VC 为网络轻度拥塞的上限值。

表 1 拥塞级别划分

拥塞级别	1	2	3
网络状态	空闲	良好	拥塞
L 的范围	$0<L\leq V_i$	$V_i<L<V_C$	$L\geq V_C$

4 NAT 穿透

4.1 NAT 类型检测方法改进

传统基于 STUN 的 NAT 类型检测算法将 NAT 分为完全锥型 NAT、对称型 NAT、限制锥型 NAT 和端口限制锥型 NAT 这四类，并针对这四类进行类型检测。但随着对称型 NAT 设备在网络中越来越普及，穿透成功率越来越低。同时，穿透流程也较为复杂，需要 2 个公网 IP、2 台服务器和 4 个 RTT。

针对传统检测算法存在的不足，本文提出一种新的检测策略。将锥型 NAT 不再细分，将对称型 NAT 细分为固定增量型、小范围内随机型和完全随机型三类。对穿透流程也进行精简，只需要 1 个公网 IP、1 台公网服务器和 3 个 RTT。借助一个位于公网的服务器，该服务器监听两个 socket，分别是（dIP，dPort1）和（dIP，dPort2）。检测流程如下图 6 所示，具体过程如下。

步骤一：普通节点使用源地址为（sIP，sPort）向目的地址（dIP，dPort1）发送 NAT 检测数据报，其中

含有源 IP 和端口等信息（下同）。服务器收到该 NAT 检测数据报后，比较映射地址（natIP，natPort1）与源地址（sIP，sPort），若两者相同，则为无 NAT 结构，停止检测算法；否则进行步骤二。

步骤二：普通节点使用源地址为（sIP，sPort）向目的地址（dIP，dPort2）发送 NAT 检测数据报。服务器收到该 NAT 检测数据报，其映射地址为（natIP，natPort2），比较步骤一的 natPort1 和本步骤的 natPort2，若两者相同，则为锥型 NAT，停止检测算法；否则进行步骤三。

步骤三：普通节点使用 N 个 socket 分别向服务器的目的地址（dIP，dPort2）发送检测数据报，服务器接收所有的数据报并处理。取出所有数据报的 natPort 字段，将 natPort 处理成集合，表示为 NATPORT={natPort1，natPort2，natPort3……natPortN}，取

$$\Delta P=\{|natPort2-natPort1|,\ |natPort3-natPort2|\ldots\ldots|natPortN-natPort(N-1)|\}$$

$$=\{\Delta p1,\ \Delta p2,\ \Delta p3\ldots\ldots\Delta p(N-1)\} \quad (2)$$

若$\Delta p1=\Delta p2=\Delta p3=\ldots\ldots=\Delta p(N-1)$，则此类型为固定增量型。取

Ep=(natPort1+natPort2+……+natPortN)/N，其方差表示为：

$$S^2=\sum_{i=1}^{N}(natPorti-Ep)^2/N \quad (3)$$

系统给定一个常量ΔS^2，若 S^2 小于ΔS^2，则此类型为小范围随机型结构，否则为完全随机结构。

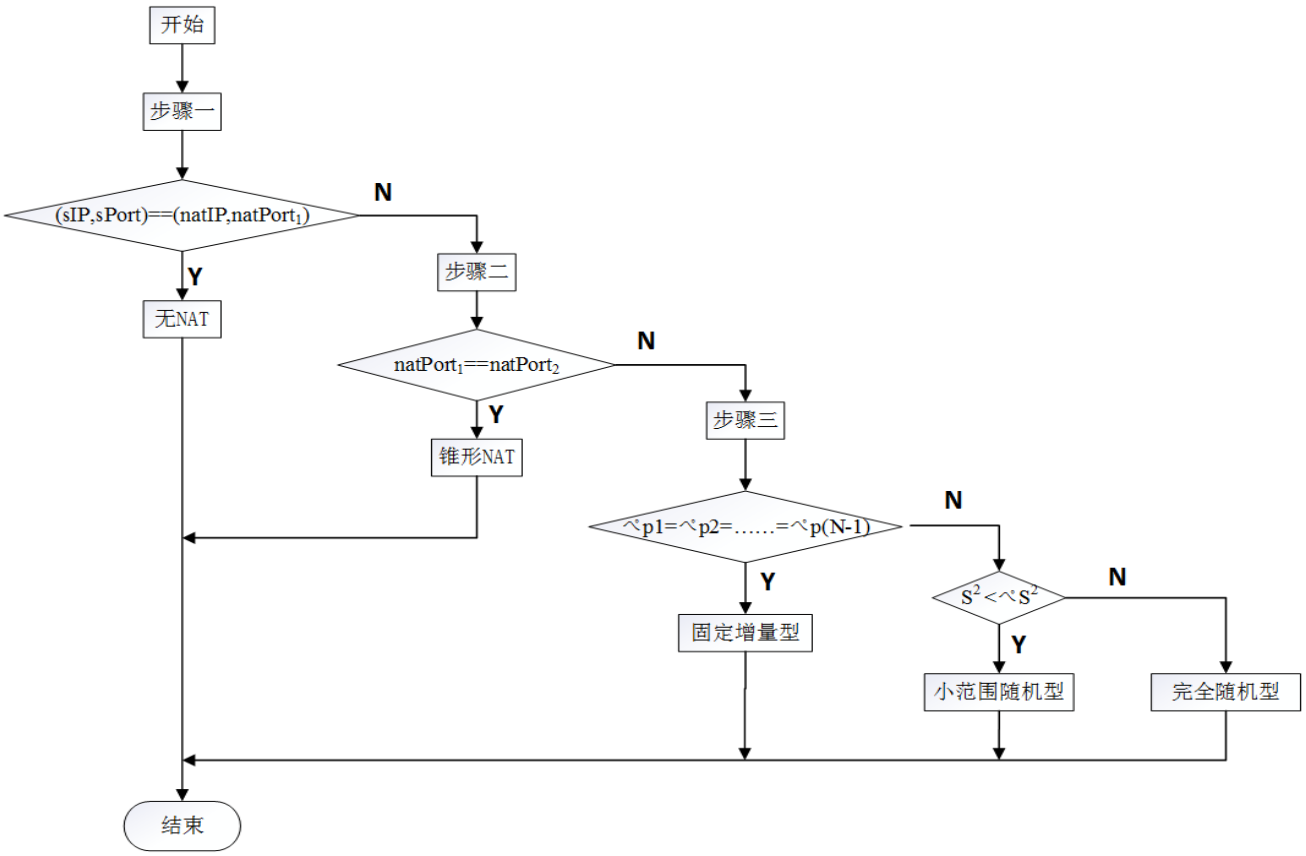

图 6 NAT 类型检测流程

4.2 NAT 穿透改进

4.2.1 锥形 NAT 穿透

锥型 NAT 的映射条件只与源 IP 地址相关，与目标 IP 地址和端口无关，即源 IP 地址相同，映射的目标 IP 地址和端口相同。此类 NAT 穿透较为简单，NAT 穿透过程如下图 7 所示。

步骤一：使用 NAT 类型检测算法检测客户端 A、B 的 NAT 类型，两者均为锥型 NAT，此时服务器已经

保存了客户端 A、B 的内网 IP 地址、映射 IP 地址和端口等信息。

步骤二：当客户端之间需要通信时，客户端 A 请求服务器希望获取客户端 B 的 IP 地址和端口（包括源 IP、源端口、映射 IP 和映射端口等，下同）。同时，客户端 B 也向服务器请求客户端 A 的 IP 地址和端口。

步骤三：客户端 A、B 收到服务器的响应报文，提取出对方的 IP 地址和端口信息。客户端 B 向客户端 A 的映射 IP 地址和端口发送数据报，该数据报通过 NAT B时，NAT 设备会在映射表项中记录下该请求的信息，该项记录可以使 NAT B 接收之后来自于客户端 A 的数据报，让其通过该 NAT 设备进入内部网络。该数据报到达 NAT A 时，由于该设备的映射表项上面没有客户端 A 到客户端 B 的记录，故丢弃该数据报；类似于客户端 B 向客户端 A 发送消息，当客户端 A 向客户端 B 发送数据报，数据报经过 NAT A 时也会在该设备的映射表项上记录该通信，该数据报到达 NAT B 时，由于该设备映射表项上有通信记录，数据报能够通过 NAT B 进入内部网络到达 B。至此，NAT A 和 NAT B 的映射表上都保存了客户端 A 和客户端 B 的通信记录，客户端 A 和客户端 B 之间可以利用该通道进行 P2P 通信。

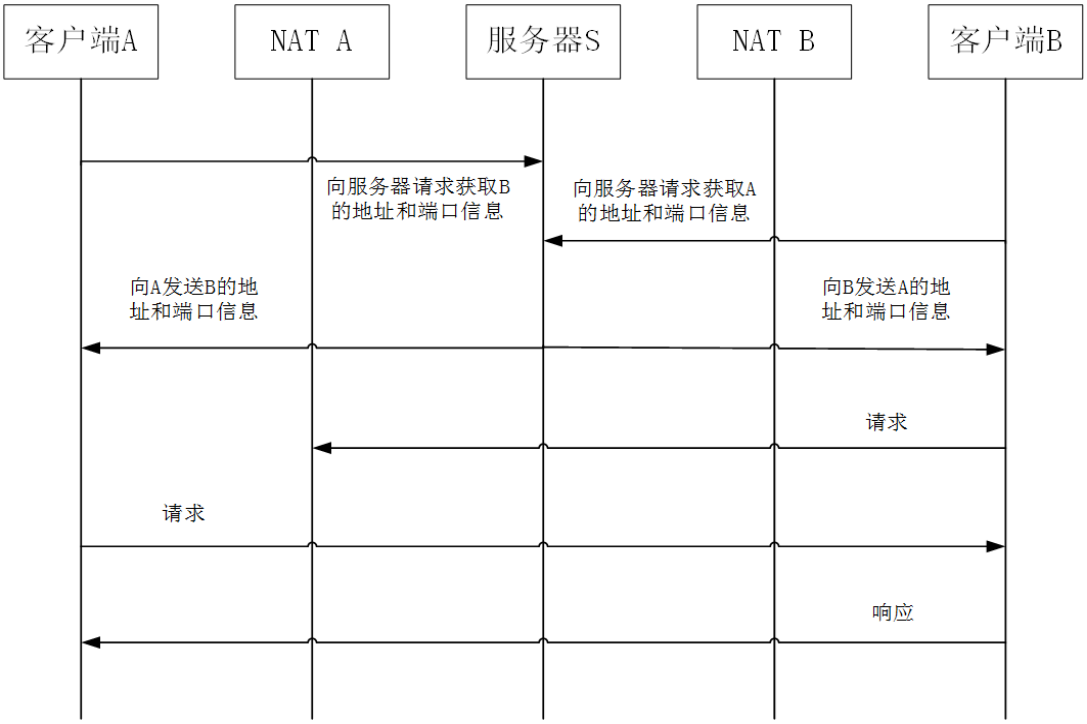

图 7 通信双方均为锥型 NAT

4.2.2 对称型 NAT 穿透

对称型 NAT 的映射规则由源 IP 地址、源端口、目的 IP 地址、目的端口这四个参数决定。当其中任意一项发生变化，其映射端口都会发生变化。根据这一特征，本文列出了锥型-固定增量型和小范围/完全随机型-小范围随机型两种穿透场景，针对锥型-固定增量型这一场景，本文将考虑干扰对穿透成功率的影响，提出了一种新的穿透策略，在较强干扰情况下依然具有较高成功率；针对小范围/完全随机型-小范围随机型这一场景，需要发送大量数据报进行端口预测，本文将网络拥塞情况对穿透成功率的影响，引入网络状态检测算法，选择合适的穿透时机，提高穿透成功率和降低穿透时延。

(1) 锥型-固定增量型

客户端 A 一侧的 NAT 分配策略为锥型，客户端 B 一侧为固定增量型，NAT 穿透过程如下图 8 所示：

步骤一：客户端 B 使用源端口 $sPort_B$ 向 STUN 服务器的 $Port_1$ 端口发送请求，得到 NAT 映射端口为 $natPort_{B1}$。

步骤二：客户端 B 使用源端口 $sPort_B$ 向客户端 A 的映射端口 $natPort_A$ 发送请求，其中 $natPort_A$ 是客户端 A 在 NAT 类型检测时得到的外部映射端口，由服务器发送给客户端 B。客户端 B 监听 $sPort_B$ 端口，等待客

户端 A 的请求信息。

步骤三：客户端 B 使用源端口 $sPort_B$ 向 STUN 服务器的 $Port_2$ 端口发送请求，得到 NAT 映射端口为 $natPort_{B2}$。客户端将 $natPort_{B1}$、$natPort_{B2}$ 和增量 Δp 等信息发送给 NAT 穿透服务器，NAT 穿透服务器收到消息后转发给客户端 A，客户端 A 收到消息后准备进行穿透。

步骤四：客户端 A 使用源端口 $sPort_A$ 向客户端 B 的预测端口区间 $natPort_P$ 发送多个请求信息，其中 $natPort_P$ 满足如下关系式，$natPort_P = natPort_{B1} + n*\Delta p$，n 为正整数，其中 $natPort_{B1} < natPort_P < natPort_{B2}$。

步骤五：客户端 B 在 $sPort_B$ 端口监听到了客户端 A 的请求信息时，表明 NAT 穿透成功，后续即可进行 P2P 通信。

本穿透策略中，即使客户端 B 的其他进程向外请求产生大量干扰端口，预测端口也位于 $natPort_{B1}$ 和 $natPort_{B2}$ 之间，只需要在这个区间内进行有限次猜测即可成功。

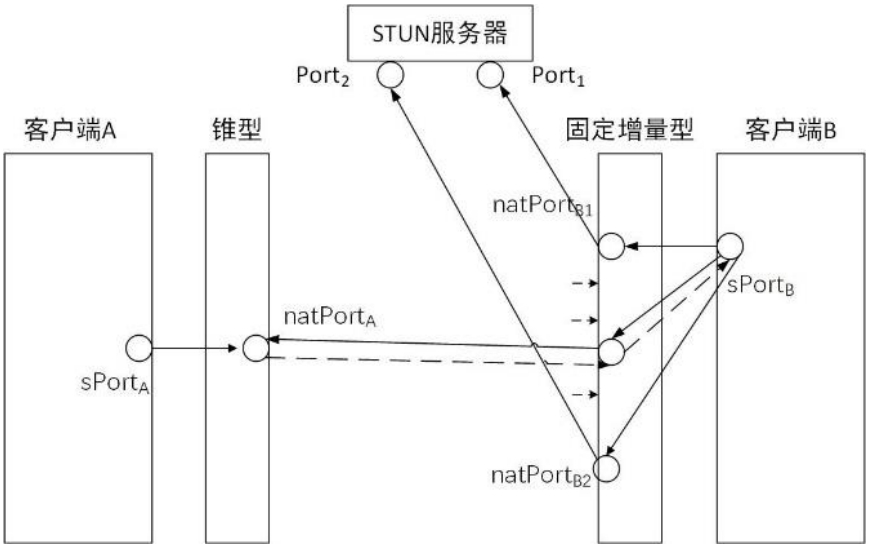

图 8 新型端口预测穿透方法

(2) 小范围/完全随机型-小范围随机型

两侧客户端的 NAT 分配策略是小范围或完全随机的，可以采用端口预测的方式增加 NAT 穿透的成功率，但端口预测需要付出一定的代价，尤其是在通信频繁、网络较差的信道中，大量无效请求造成穿透时间增加。本文引入网络状态检测算法，根据网络状况，动态决定是否进行端口预测。客户端 A 的一侧的 NAT 分配策略为小范围/完全随机型，客户端 B 一侧为小范围随机型，NAT 穿透过程如下图 9 所示：

步骤一：根据网络状态检测算法，向网络中发送 UDP 数据报，根据 UDP 数据报的接收时间间隔和发送时间间隔的差值计算网络拥塞级别 L，若 $L \geq V_C$（V_C 为网络轻度拥塞的上限值），说明网络拥塞严重，通信质量较差，此时进行端口预测并不能提高成功率，直接选用中转通信完成基本通信需求。否则，进行步骤二。

步骤二：客户端 A 使用源端口 $sPort_A$ 向 STUN 服务器的 $Port_1$ 端口发送请求，得到 NAT 映射端口为 $natPort_A$。将 $natPort_A$ 等信息发送给 NAT 穿透服务器，NAT 穿透服务器收到消息后转发给客户端 B，客户端 B 收到消息后准备进行穿透。

步骤三：①若客户端 A 为小范围随机型。客户端 B 使用源端口 $sPort_B$ 向客户端 A 的映射端口 $natPort_A$ 附近端口发送 n 个请求信息；②若客户端 A 为完全随机型。由于分配规则不能预测，具有很大的随机性，故可以采取完全随机猜测、伪随机猜测和端口分区猜测等方式以源端口为 $sPort_B$ 向客户端 A 发送 n 个请求尝试进行端口预测。

步骤四：客户端 B 使用源端口 $sPort_B$ 向 STUN 服务器的 $Port_1$ 端口发送请求，得到 NAT 映射端口为 $natPort_B$。将 $natPort_B$ 等信息发送给 NAT 穿透服务器，NAT 穿透服务器收到消息后转发给客户端 A，客户端 A 收到消息后准备进行穿透。

步骤五：客户端 A 使用源端口 $sPort_A$ 向客户端 B 的映射端口 $natPort_B$ 附近端口发送 n 个请求信息。当客户端 B 的 $sPort_B$ 端口接收到了来自客户端 A 的请求信息时，说明 NAT 穿透成功，后续即可进行 P2P 通信。

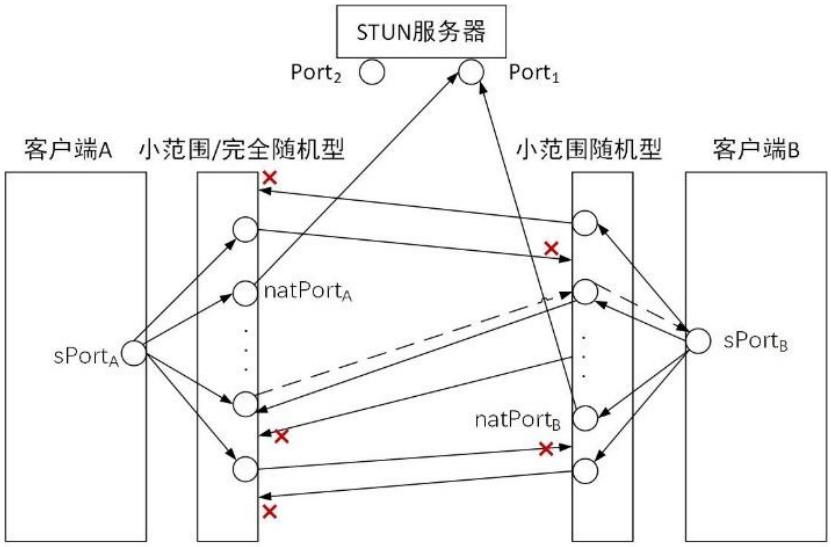

图 9 范围/完全随机型-小范围随机型

步骤三和步骤五中 n 的取值越大，穿透成功率越高。NAT 设备分配的端口范围为[1024,65535]，从概率与统计的角度分析，对一定范围内端口预测时，假设尝试 i 次能够猜中，P1 为客户端在 i 次尝试中一次都不成功的概率，所以在 i 次实验中至少成功一次的概率为 P2=1-P1。令 N=65535-1024，则 P1 的概率公式可以表示为：

$$P1=\frac{N-i}{N}\times\frac{N-i-1}{N-1}\times\frac{N-i-2}{N-2}\times\ldots\times\frac{N-i-(i-1)}{N-(i-1)}=\sum_{j=0}^{i-1}\frac{N-i-j}{N-j} \quad (4)$$

根据上式可以计算出当尝试次数 i≥439 时，至少成功一次的概率为 95%。因此，可以通过增加尝试次数提高穿透率。

5 实验与分析

实验拓扑结构如下图 10 所示。服务器 S 分配的公网 IP 地址为 202.0.0.1，两台 NAT 设备 NAT A 和 NAT B，客户端 A 和客户端 B 的 IP 地址分别为 192.168.1.1 和 192.168.2.1。在服务器 S 上安装 MySql 数据库，建立 dataCollection、natInfo 表，dataCollection 表记录下端口采集数据，natInfo 表记录 nat 映射信息。实验涉及硬件设备参数如下表 2 所示。

图 10 实验网络拓扑图

表 2 实验硬件设备信息表

设备类型	设备名	详细参数
主机	CPU 型号	Intel(R) Core(TM) i5-6200U CPU @ 2.30GHz
	RAM 容量	12GB
	操作系统	Windows 10 家庭中文版
虚拟机	CPU 型号	Intel(R) Core(TM) i5-6200U CPU @ 2.30GHz
	RAM 容量	2GB
	操作系统	Centos 7

在实验中，选择锥型（以端口限制锥型为例）、固定增量型、小范围随机型和完全随机型这四种 NAT 类型进行测试。经过多次实验，统计结果如下表 3 所示：

表 3 实验测试结果

样本名	NAT A	NAT B	穿透成功率
样本 1	端口限制锥型	端口限制锥型	100%
样本 2	端口限制锥型	固定增量型	100%
样本 3	小范围随机型	小范围随机型	100%
样本 4	完全随机型	小范围随机型	91.2%

在端口限制锥型-固定增量型场景中，本文提出的穿透策略具有较强的抗干扰能力，在高负载情况下依然具有较高的成功率。在 NAT 设备分配端口分别进行频率为 0、0.5、1、2、5、10、20、50 个/秒的干扰，进行实验并计算成功率。实验结果如下图 11 所示。

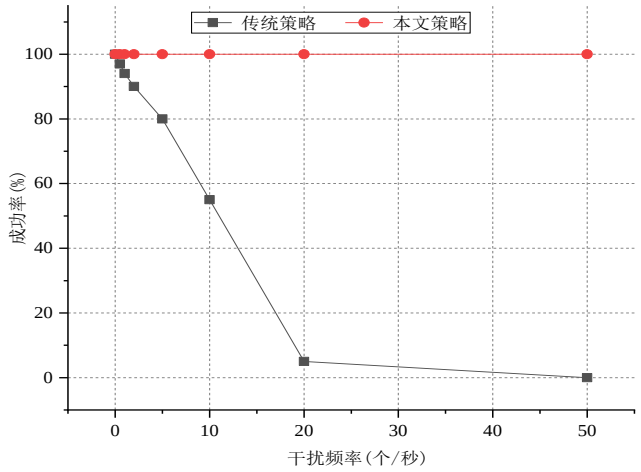

图 11 端口限制锥型-固定增量型成功率对比图

由图 11 图像可知，当干扰频率较低时，两种穿透策略的成功率都比较高。但随着干扰频率的增加，传统穿透策略的成功率急剧下降，当干扰频率达到 20 个/秒时，成功率已经趋近于 0%。

6 总结

本文针对传统 NAT 类型检测方法繁琐且逐渐不适用当前越来越多的对称型 NAT 通信场景，通过将锥形 NAT 不在细分，将对称型 NAT 划分为固定增量型、小范围随机型和完全随机型三类，将原来检测流程由四步减少为三步，缩短了检测时间，并且细化对称型 NAT 有助于后续根据不同类型选择不同的穿透策略；针对穿透过程中穿透率较低等问题，通过优化穿透步骤和引入网络状态检测算法等措施，极大程度的提高了穿透成功率和抗干扰能力。

参考文献

[1] Ordabayeva G K, Othman M, Kirgizbayeva B, et al. A systematic review of transition from IPV4 To IPV6 [C]//Proceedings of the 6th International Conference on Engineering & MIS 2020. 2020: 1-15.

[2] Li X, University C. Analysis on NAT technology and its application [J]. Wireless Internet Technology, 2019.

[3] Livadariu I, Benson K, Elmokashfi A, et al. Inferring carrier-grade NAT deployment in the wild [C]//IEEE INFOCOM 2018-IEEE Conference on Computer Communications. IEEE, 2018: 2249-2257.

[4] Huang F, Yu L, Shen T, et al. The P2P Solution Research and Design Based on NAT Traversing Technology [C] // 2019 IEEE 3rd Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC). IEEE, 2019.

[5] Yue G. Research on C/S Protocol and P2P Protocol in Wireless Communication [C] // Journal of Physics: Conference Series. IOP Publishing, 2020, 1486 (4): 042004.

[6] 冯佳欣, 王建林, 孟丹, 等. 主流 NAT 穿越技术对比研究 [J]. 信息与电脑 (理论版), 2020, 32 (14): 174-176.

[7] Srirama S N, Liyanage M. Tcp hole punching approach to address devices in mobile networks [C]//2014 International Conference on Future Internet of Things and Cloud. IEEE, 2014: 90-97.

[8] Wang Y, Lu Z, Gu J. Research on symmetric NAT traversal in P2P applications [C]//2006 International Multi-Conference on Computing in the Global Information Technology-(ICCGI'06). IEEE, 2006: 59-59.

[9] Wei Y, Yamada D, Yoshida S, et al. A new method for symmetric NAT traversal in UDP and TCP [J]. Network, 2008, 4 (8).

[10] D'Angelo G, Rampone S. A NAT traversal mechanism for cloud video surveillance applications using WebSocket [J]. Multimedia Tools and Applications, 2018, 77 (19): 25861-25888.

[11] 郑浩. 基于 STUN 协议的 NAT 穿越技术的研究与应用 [D]. 武汉理工大学, 2018.

[12] 冯金哲, 殷海兵. 一种 Symmetric NAT 穿透的新方法 [J]. 计算机应用与软件, 2017, 34 (01): 125-128.

[13] Ashraf S, Muhammad D, Aslam Z. Analyzing challenging aspects of IPv6 over IPv4 [J]. J. Ilm. Tek. Elektro Komput. Dan Inform, 2020, 6 (1): 54-67.

[14] Ghafouri R, Ashrafi A, Vahdat B V. Security consideration of migration to IPv6 with NAT (Network Address Translation) methods [C]//2015 23rd Iranian Conference on Electrical Engineering. IEEE, 2015: 746-749.

[15] 黄佳庆, 闵江, 程文青. 一种利用 TURN 穿越对称型 NAT 方案的设计与实现 [J]. 微电子学与计算机, 2009, 26 (04): 255-259.