

通过活化的ICMP重定向攻击进行路径 外网络流量操纵

冯学伟，清华大学计算机科学与技术系&BNRist；李琦，清华大学网络科学与网络空间研究所&BNRist，中关村实验室；孙坤，乔治梅森大学信息科学与技术系&CSIS；钱志云，加州大学河滨分校；赵刚，清华大学计算机科学与技术系&BNRist；匡晓辉，北京邮电大学；傅传璞，清华大学计算机科学与技术系&BNRist；徐珂，清华大学计算机科学与技术系&BNRist，中关村实验室

<https://www.usenix.org/conference/usenixsecurity22/presentation/feng>

第31届USENIX安全研讨会论文集的
开放访问由USENIX赞助。

通过活化的ICMP重定向攻击进行路径外网络流量操纵

冯学伟¹, 李琦^{2,5}, 孙坤³, 钱志云⁴, 赵刚¹, 匡晓辉⁶ 付传普¹, 徐珂^{1,5*}

¹清华大学计算机科学与技术系&BNRist ²清华大学网络科学与网络空间研究所
&BNRist ³乔治梅森大学信息科学与技术系&CSIS ⁴UC 河畔 中关村实验室
⁶北京邮电大学

确定了一个更好的路由，路由器将发出一个ICMP重定向消息给

*通讯作者: xuke@tsinghua.edu.cn。

摘要

ICMP重定向是一种机制，它允许终端主机动态地更新其对特定目的地的路由决定。以前的研究表明，ICMP重定向可能被攻击者利用来操纵受害者traffic的路由。然而，人们普遍认为，ICMP重定向攻击不是一个现实世界的威胁，因为它们只能在特定的网络拓扑结构（如LAN）下发生。在本文中，我们对ICMP的合法性检查机制进行了系统的研究，发现了检查机制和无状态协议之间的根本差距，导致了广泛的漏洞。特别是，我们发现路径外攻击者可以利用一套无状态协议（如UDP、ICMP、GRE、IPIP和SIT）来轻松制作逃避的ICMP错误信息，从而使ICMP重定向攻击在现实世界中恢复活力，特别是在广域网中造成巨大的破坏。首先，我们表明，路径外攻击者可以通过欺骗互联网上的各种公共服务器，用一个伪造的ICMP重定向消息将其流量误导到黑洞中，从而进行隐蔽的DoS攻击。例如，我们揭示了互联网上有超过43K的流行网站容易受到这种DoS攻击。此外，我们发现互联网上54.47万个开放的DNS解析器和186个Tor节点也是脆弱的。其次，我们表明，通过利用针对NAT网络的ICMP重定向攻击，同一NAT网络中的路径外攻击者可以进行中间人（MITM）攻击，拦截受害者的流量。最后，我们制定了反措施来阻止这些攻击。

1 简介

ICMP重定向机制的设计是为了最大限度地减少特定流量在前往目的地途中必须穿越的路由跳数，从而优化转发路径，减少每个路由器必须处理的流量[18, 67]。一旦

告知发端人替代路线。在收到消息并成功验证其合法性后，发端者将更新其路由表，将消息中的网关互联网地址字段设置为其到目的地的新下一跳。几乎所有的主要操作系统都支持ICMP重定向机制。

原则上，ICMP重定向消息应该只由路由器发送，用于报告数据包处理错误[2, 12, 67]。然而，由于目前互联网缺乏对数据包转发路径的验证[42, 87, 88]，任何主机都可以模仿路由器来伪造ICMP错误信息[26]。因此，攻击者可以通过发送伪造的ICMP重定向消息给受害者发起者，将流量从发起者重定向到特定的主机。为了解决这个问题，ICMP规范[6, 12, 31, 67]对发端者收到的ICMP错误信息实施合法性检查机制，即ICMP错误信息应嵌入引发错误信息的原始数据包的至少28个八位字节（即IP头的20个八位字节加上至少前8个八位字节）。

因此，如何逃避ICMP重定向攻击的合法性检查是一个关键问题。在以前的广播网络中，主机由集线器连接，攻击者可以窃听来自发端者的数据，然后将数据嵌入到精心制作的ICMP重定向消息中，以逃避发端者的检查，从而误导发端者的流量[8, 9, 48, 56, 63, 86]。现在，随着交换式网络的广泛部署，主机被交换机或路由器连接起来，路径外攻击者不能再窃听其他主机的网络流量，从而轻易伪造一个可接受的ICMP重定向。因此，以前的ICMP重定向攻击[8, 9, 48, 56, 63, 86]在现代网络拓扑结构中总是失败。

历史上，一些技术博客和讲座已经对路径外攻击者进行恶意ICMP重定向的方法进行了讨论[5, 22, 37, 41, 83]。例如，在内核版本2.6.20之前的Linux系统不检查嵌入UDP数据的ICMP错误信息，因此有可能伪造一个嵌入UDP数据的可接受的ICMP重定向信息，以进行路径外ICMP重定向攻击。然而，现代操作系统会检查嵌入的UDP数据是否存在。

UDP套接字，因此大多数先前的方法将失败[5,22,37,83]。在Kulas的演讲中[41]，ICMP回音信息被利用来伪造重定向信息并逃避发起者的检查机制。然而，建议的ICMP重定向攻击只能在本地网络上成功。此外，在现实世界中，发端者可能出于性能和安全的考虑而禁用ICMP回波[79]，从而挫败了攻击。一般来说，人们普遍认为ICMP重定向攻击不是一个现实世界的威胁，因为它们只可能发生在有限的网络拓扑结构中[8, 9]。

在本文中，我们证明了ICMP重定向攻击可以不受网络拓扑结构的限制，在现实世界中造成严重破坏[8, 9]。特别是，我们发现它实际上在广域网络中广泛适用。我们发现，由于ICMP的合法性检查机制与一系列状态较差的协议（如ICMP、UDP、GRE[25]、IPIP[64]和SIT[61]）之间存在差距，受害者发起人本质上无法检查嵌入这种协议数据的ICMP错误信息的合法性。因此，受害者可能会错误地接受来自路径外攻击者发出的伪造的ICMP重定向消息，从而导致他们的流量被错误地重定向。这个漏洞影响到广泛的主要操作系统，包括Linux 2.6.20及以上版本，FreeBSD 8.2及以上版本，Android 4.3及以上版本，以及Mac OS 10.11及以上版本。¹

在现代交换网络中，路径外攻击者无法窃听其他主机的流量来制作ICMP重定向消息。然而，我们发现，ICMP的合法性检查机制的模糊性可以被路径外攻击者利用来制作一个逃避的ICMP错误消息。由于无状态协议不能记住先前发送的数据，如果攻击者能迫使受害者发起者弹出无状态协议数据，然后伪造嵌入这种协议数据的ICMP错误消息，那么发起者就很难准确检查消息的合法性。现代操作系统可能会执行一些简单的检查，例如，如果UDP数据被嵌入到收到的ICMP错误信息中，Linux系统自内核2.6.20版本以来会检查相应的UDP套接字的存在。然而，路径外攻击者可以欺骗发端者提前建立一个可预测的UDP套接字，然后他们伪造嵌入了这个已知UDP套接字数据的ICMP错误，受害者发端者执行的检查将很容易被逃避。由于UDP的无记忆性，发端者无法进行进一步的检查，最终会接受伪造的信息。ICMP和无状态协议的合法性检查机制之间的这种内在差距使得路径外攻击者可以轻易地伪造逃避性的ICMP错误。在本文中，我们使用一个伪造的ICMP重定向消

息来虚假地更新受害者的路由，然后将其后续流量错误地重定向到

¹ 我们发现，Windows是无懈可击的，因为它没有严格遵守ICMP的规范。Windows默认启用了ICMP重定向机制；然而，它只是放弃了所有收到的ICMP重定向消息，即使这些消息是合法的。

一个指定的主机。

我们证明了我们重新激活的ICMP重定向攻击可以在现实世界中造成严重破坏。首先，一个非路径攻击者可以通过发布一个伪造的ICMP重定向消息，迫使互联网上的一个远程脆弱目标将其流量路由到黑洞（默认情况下主机转发功能被禁用），从而导致一个隐蔽的DoS攻击。我们的实验表明，互联网上有超过43,000个流行的网站是脆弱的。此外，我们证明我们的DoS攻击甚至可以在切断发起者和目的地之间的通信时，关闭DNS和Tor等后端服务的整个操作，从而导致更广泛的影响。我们发现，互联网上54,470个开放的DNS解析器和186个Tor节点容易受到我们的攻击。其次，当攻击者和受害者重新在同一网络中时，我们表明路径外攻击者可以演变成中间人（MITM），然后进行各种劫持攻击，例如，在NAT（网络地址转换）[81]网络中劫持DNS请求。

最后，我们制定了不同的反击措施来对付这些攻击，并系统地衡量其有效性。首先，我们建议改变网络设置以阻止互联网上的欺骗性ICMP重定向消息，这可以防止在ISP部署过滤机制的情况下发生的再移动DoS攻击。其次，我们评估了采用协议变化的可能性，以改善ICMP消息的合法性检查机制，例如，在UDP中嵌入秘密以验证通信。最后，我们建议严格区分无状态协议和有状态协议，在无状态协议上禁用ICMP重定向机制。这一对策可以有效地击败上述DoS攻击和MITM攻击。此外，该对策可以很容易地部署，因为它只需要在担心ICMP重定向攻击的特定主机上进行修改。我们实现了一个原型，并在我们的真实世界网络中评估了这个对策。实验结果表明，它可以有效地防止攻击，而对网络性能的副作用很小。

贡献。我们的主要贡献有以下几点：

- 我们发现了ICMP和无状态协议的合法性检查机制之间的一个基本差距，我们揭示了差距可能导致广泛的主要操作系统的漏洞，包括Linux 2.6.20及以后，FreeBSD 8.2及以后，Android 4.3及以后，Mac OS 10.11及以后。
- 我们证明ICMP重定向攻击可以在互联网上形成，

从而在现实世界中造成严重破坏。我们发现互联网上有超过43,000个流行网站、54,470个开放的DNS解析器和186个Tor中继节点容易受到我们的攻击。

- 我们分析了其根本原因，并提出了一个增强的ICMP合法性检查机制来防止攻击。一个原型验证了我们的策略的有效性。

道德方面的考虑。在本文中，我们进行了两种类型的真实世界实验，以验证所确定的攻击的可行性和影响，即发现互联网上易受DoS攻击的公共服务器（见第5节）和劫持我们校园网络中易受攻击的DNS转发器的请求（见第6节）。在进行实验时，我们把伦理道德作为首要任务。

在发现互联网上易受攻击的公共服务器的实验中，我们使用我们自己的测试平台的机器作为公共服务器的目的地。通过发布精心制作的ICMP重定向，我们只改变了服务器数据包对我们自己机器的路由，因此我们的实验不会影响正常用户对服务器的访问。此外，一个ICMP重定向消息对服务器产生的负载可以忽略不计。实验结束后，我们通过发布一个补救性的ICMP重定向消息（即指定服务器的默认网关为到我们机器的下一跳）来恢复服务器的路由变化。我们还确认了治疗性ICMP重定向消息的有效性。

在我们的校园网进行劫持DNS的实验之前，我们向网络管理员解释了我们攻击的细节和潜在的风险。我们获得了他们的批准，只为研究目的进行实验。在管理员的帮助下，我们在午夜进行实验。管理员确定在我们进行实验之前没有用户访问目标网络，防止我们的实验对正常用户产生潜在的隐私风险。此外，为了尽量减少对转发者的DNS缓存的影响，我们只拦截转发者对一个特定网站（即我们实验中的目标网站 "www.yahoo.com"）的DNS查询。一旦实验结束，网络管理员将DNS转发器重置为正常状态。

2 背景介绍

2.1 网络流量的ICMP重定向

自1981年以来，作为RFC 792的标准[67]，ICMP重定向机制被路由器用来通知发端者从发端者到目的地的更优化路径。它减少了到达目的地所必须经过的跳数。图1显示了ICMP重定向的基本程序。当发端人的网关收到一个IP数据包时，该网关将检查其路由表以确定下一个网关的地址。如果下一个网关和由数据包的源IP地址确定的发端者在同一个网络上，则一个ICMP重定向消息将从网关发送给发端者。生成的ICMP重定向消息建议发端者将其目的地网络的traffic直接发送到下一个网关

，而不是当前的网关，因为直接通过下一个网关转发是通往目的地的较短路径。

一旦发端人收到ICMP重定向消息

并且该报文通过其检查，发端者将下一个网关设置为其到目的地的路线的下一跳。在ICMP规范[67]中，ICMP重定向消息的Type字段被指定为5，Code字段可以指定为0、1、2和3，分别表示为网络重定向数据包、为主机重定向数据包、为服务类型和网络重定向数据包、为服务类型和主机重定向数据包。下一个网关是在ICMP重定向消息的网关互联网地址字段中指定的。

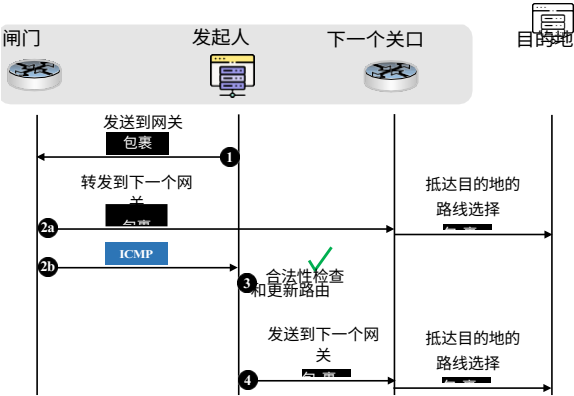
ICMP重定向机制对于减少路由跳数和实现路由器之间的负载平衡非常有用。如果重定向机制被禁用，发端者将不知道到目的地的最优化路由。因此，ICMP重定向机制在广泛的主要操作系统的IP实现中是默认启用的，例如，Linux 2.6.20及以后，FreeBSD 8.2及以后。配备这些操作系统的发起人默认接受ICMP重定向消息，一旦消息通过检查机制，就将其流量重定向到指定的网关互联网地址（即，下一个网关）。

图1：通过ICMP 重定向优化路由路径。

2.2 对ICMP错误的合法性检查

ICMP重定向机制也可能被攻击者利用来操纵网络流量。攻击者可以向发起者发送一个伪造的ICMP重定向消息，这表明所有未来的目的地流量必须被重定向到一个特定的系统，作为目的地的较短路径。

为了防止ICMP重定向的滥用，当收到ICMP重定向消息时，发起人会进行两次检查[6, 12, 67]。首先，发端者检查该消息是否由其默认网关发送，即ICMP重定向消息的源IP地址应被指定为默认网关的IP地址。第二，ICMP错误信息应该携带触发错误信息的原始数据包的至少28个字节（即IP头的20个字节加上至少前8个字节）。这28个八位字节的数据将被发端者用来将信息与相关的数据相匹配。



最终导致了接下来描述的现实世界的ICMP重定向攻击。

² 初始序列号是随机产生的，随后的序列号在其基础上单调递增。

响应的过程，并检查消息的合法性。此外，根据较新的标准RFC 1812 [6]，ICMP错误消息应携带触发数据包的大部分内容，但不超过576个八位字节。

2. 3对检查的现有规避

不幸的是，即使实现了对ICMP重定向的合法性检查，攻击者仍然可能逃避检查，进行ICMP重定向攻击。由于互联网上的IP地址欺骗的脆弱性，第一个检查很容易被规避。非路径攻击者可以冒充受害者发起者的网关，发出欺骗性的ICMP重定向消息。根据先前的研究[44, 49]，互联网上约有四分之一的自治系统（AS）没有过滤离开其网络的带有欺骗性源IP地址的数据包。在本文中，我们发现互联网上有超过5100个AS没有执行有效的入口过滤[7, 28]。因此，这些AS中的网关带有欺骗性源IP地址的ICMP重定向消息可以通过整个路由路径并被转发到受害者的发端（详见后面的第4节）。

对ICMP重定向消息中嵌入的有效载荷的第二次检查对于路径外的攻击者来说更难逃避，即使发起者只执行RFC792中定义的较弱的检查机制（即检查原始数据包的前28个八位字节）。如图2所示，当发端者使用TCP作为高级协议与他人进行通信时，攻击者必须猜测识别TCP连接的四元组和发端者发送窗口中的序列号来制作一个规避的ICMP重定向消息。特别是，路径外的攻击者很难猜到这些值，因为源端口和序列号是随机产生的。²在现代操作系统中[32]。

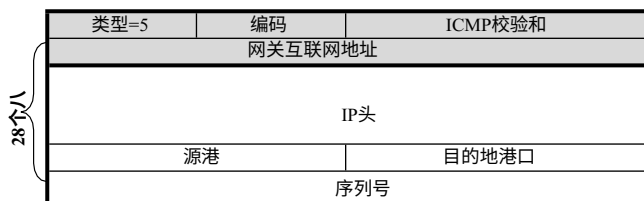


图2：嵌入TCP的ICMP重定向 消息。

在本文中，我们表明，无论检查的是28个八位数还是576个八位数，都可以顺便通过第二次检查。这是由于ICMP的合法性检查机制和无状态协议之间的差距，这

3 检查ICMP错误的漏洞

3.1 ICMP合法性检查中的漏洞

与TCP不同，无状态协议不能记住先前发送的数据。因此，如果路径外的攻击者伪造了嵌入这种协议数据的ICMP错误信息，发端者就很难准确地检查嵌入数据的合法性。因此，受害者可能会接受这些伪造的信息。一旦伪造的ICMP重定向消息被接受，受害者将根据消息中指定的新网关虚假地更新其路由。因此，由IP承担的全部流量将受到影响并被交叉攻击。在实践中，当受害者找到一个更好的下一跳时，重定向所有后续的流量是合理的，因为流量路由发生在IP层，与上层协议无关。然而，不同协议之间相互作用的复杂性给目前的网络原则带来了许多挑战[26]。

目前的ICMP实现可能对收到的嵌入无状态协议数据的ICMP错误消息进行一些检查。例如，当收到嵌入UDP数据报的消息时，Linux内核2.6.20及以后的版本会检查它和目的地之间是否存在UDP套接字。这种检查可以防止以前的ICMP重定向攻击[22, 37, 83]。然而，我们发现，由于ICMP的合法性检查机制存在固有的缺陷，这种检查很容易被规避。

在实践中，现代操作系统为轻量级服务（如NTP、SNMP、DHCP、DNS和TFTP）默认开放了几个公开的UDP端口。³因此，攻击者可以首先探测受害者的这种开放的UDP端口，然后欺骗受害者在探测的开放端口上为远程目的地生成一个可预测的UDP套接字。之后，攻击者伪造一个ICMP重定向消息给受害者，其中嵌入了已知的UDP套接字和一些任意的填充数据。由于UDP的无状态性，填充数据不能被准确检查。因此，伪造的ICMP重定向消息将逃避安全检查并被错误地接受，即成功地对受害者进行非路径ICMP重定向攻击。除了UDP，我们发现ICMP、GRE[25]、IPIP[64]和SIT[61]的无状态协议也可以被路径外攻击者利用来逃避ICMP的合法性检查机制。在我们的攻击中，我们以UDP为例来阐述和利用这个漏洞。请注意，使用无状态协议来触发ICMP合法性检查机制的漏洞的方法是通用的。路外攻击者可以利用无状态协议来伪造所有类型的ICMP错误信息（不仅仅是ICMP重定向信息）来逃避检查。

³ 一个开放的端口足以进行我们的攻击。例如，在Linux内核版本的Ubuntu 20.04中，超过6个UDP端口是默认开放的。

5.4.我们发现互联网上有超过43K个网络服务器、54K个开放的DNS解析器和186个Tor中继节点至少开放了一个UDP端口（见§5）。

3.2 易受影响的实施

所发现的差距影响了广泛的实现，即Linux 2.6.20（2007年2月发布）及以后，FreeBSD 8.2（2011年2月发布）及以后，Android 4.3（2012年6月发布）及以后，Mac OS 10.11（2015年9月发布）及以后。在Linux系统、FreeBSD系统、内核版本6.0之前的Android系统和内核版本10.11.6之前的Mac OS中，ICMP重定向机制被默认启用。在安卓系统中，一旦内核中启用了ICMP重定向机制，普通用户很难手动禁用该机制，因为禁用的操作需要root权限[1]，而世界上只有大约7.6%的安卓系统用户对他们的设备进行了root[3]。对于内核版本10.11.6之后的Mac OSs，一旦ICMP重定向机制通过sysctl的参数被启用，Mac OSs也会变得脆弱。

我们还审查了Linux系统和FreeBSD系统的源代码，以确认它们对我们的攻击确实是脆弱的。例如，图3显示了自Linux内核2.6.20版本以来处理嵌入UDP数据报的ICMP错误信息的代码。⁴可以看出，Linux会首先检查套接字的存在（在第106行）。由于UDP的无状态和无记忆性，Linux不能对嵌入的UDP数据进行进一步的检查（不像TCP会进一步检查以确认携带的序列号是否在其发送窗口内）。因此，只要到远程目的地的套接字存在，Linux就会为目的地重定向出站流量（在第113行）。然而，正如我们之前在第3.1节所描述的，攻击者可以很容易地制作一个UDP套接字来逃避这种检查，从而欺骗受害者顺从地重定向其流量。

```
100 空白 udp4_lib_err ()
101 {
102     .....
103     const int type = icmp_hdr(skb)->type;
104     const int code = icmp_hdr(skb)->code;
105     struct sock *sk;
106     sk = udp4_lib_lookup();
107     if(!sk) {
108         ICMP_INC_STATS(net, ICMP_MIB_INERRORS)
109         return; /* 没有套接字的错误 */
110     }
111     switch (type) {
112         case ICMP_REDIRECT:
113             ipv4_sk_redirect();
114     }
115     .....
116 }
```

图3：处理嵌入UDP的ICMP错误。

3.3 炮制回避的ICMP重定向

图4说明了嵌入已知UDP数据报的伪造的ICMP重定向消息的结构，它可以

⁴ Linux自内核4.20.17版本以来引入了一些小的变化，但基本逻辑没有改变。

被用来规避ICMP规范中的检查机制。在IP头中，协议文件被指定为ICMP，源IP地址和目的IP地址分别被指定为网关的IP地址和受害者发起人的IP地址。然后在ICMP头中，类型字段被指定为5，表示这是一个ICMP重定向消息。代码字段的值不是唯一的，攻击者可以选择四个值中的任何一个（即0、1、2或3）来重定向受害者发端者的网络流量，用于下一个嵌入UDP数据报中指定的目的地。网关互联网地址字段指定了发端人在前往目的地途中的新网关。

无论RFC792和RFC1812中定义的检查是否被实施，我们伪造的ICMP重定向信息都能发挥作用，因为检查机制在设计上对无状态协议（即我们演示的UDP）是无效的。此外，我们发现RFC 1812（即尽可能多地检查触发数据包，但不超过576个字节）在我们在§3.2中列出的易受攻击的操作系统中没有严格实施。因此，在实践中，攻击者只需要制作图4中UDP数据报的前28个八位字节的数据，以逃避检查机制，然后成功执行我们的攻击。

我们的远程DoS攻击的一个必要条件是，由路径外攻击者制作的恶意ICMP重定向消息可以转发给远程受害者。在本节中，我们将进行

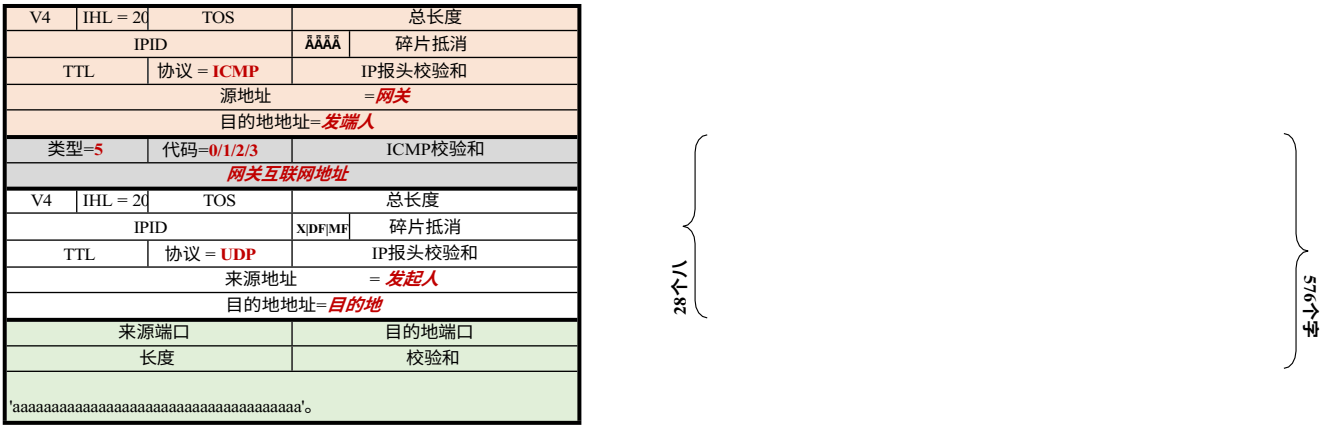


图4：伪造的ICMP，嵌入UDP的重定向。

通过制作这样一个回避的ICMP重定向消息，攻击者可以操纵受害者的流量来构建非路径攻击，即（i）当攻击者不与服务器居住在同一网络中时，对互联网上的脆弱服务器进行隐蔽的远程DoS攻击，或者（ii）如果攻击者是一个与受害者居住在同一网络中的正常用户，则劫持受害者的流量来构建MITM攻击。

4 伪造互联网上的ICMP重定向

表1: 在互联网上转发ICMP重定向信息。

AS交叉 寄件人	接收器	亚洲					美国			欧洲	
		北京 159.226.*.202	东京 124.156.*.135	孟买 119.28.*.146	新加坡 150.109.*.233	香港 43.129.*.233	加利福尼亚州 170.106.*.100	多伦多 49.51.*.40	弗吉尼亚州 170.106.*.40	法兰克福 162.62.*.44	莫斯科 162.62.*.197
美国	加州 47.88.*.24 弗吉尼亚州 47.90.*.227	AS7497									
		AS174	AS2914	AS6453	AS7473	AS6453	AS8003	AS3356	AS2914	AS1299	AS6762
		AS2914			AS4766	AS9304		AS2914	AS3356	AS2914	AS2914
		AS7497	AS2516	AS174	AS6453	AS3491				AS31133	
欧洲	伦敦 8.208.*.114	AS174	AS3356	AS9498	AS7473	AS6453	AS3356	AS3356	AS3356	AS2914	AS3356
		AS3356	AS45102	AS45102	AS1299	AS3491	AS45102	AS45102	AS45102	AS1299	AS6939
		AS45102			AS45102	AS3356				AS209141	AS45102
		AS7497	AS2914	AS7473	AS7473	AS7474	AS6453	AS6453	AS7474	AS1299	AS6939
澳大利亚	悉尼 47.74.*.68	AS174	AS7474	AS7474	AS7474	AS7474	AS7474	AS7474	AS6461	AS7474	AS45102
		AS3491	AS7473	AS9498	AS7474	AS45102	AS7473	AS45102	AS45102	AS45102	AS15412
		AS45102	AS45102	AS45102	AS45102	AS9304	AS45102	AS7473	AS7473	AS7473	AS209141
		AS7473									
亚洲	雅加达 147.139.*.126	AS7497									
		AS3491	AS2914	AS7473	AS3491	AS10217	AS6453	AS6453	AS3356	AS1299	AS2914
	青岛 118.190.*.74	AS10217	AS10217	AS9498	AS135391	AS10217	AS2914	AS2914	AS10217	AS10217	AS10217
		AS2914		AS135391						AS2914	AS3356
	迪拜 47.91.*.206	AS7497	AS4837	AS4837	AS7473	AS37963	AS4134	AS6453	AS7018	AS4837	AS4837
		AS37963	AS45102	AS37963	AS58541	AS58541	AS45102	AS4837	AS4837	AS1299	AS12389
	北京 183.173.*.12	AS3491	AS2914	AS45102	AS45102	AS4134	AS58541	AS45102	AS37963	AS37963	AS45102
		AS6762	AS45102	AS9498	AS8003	AS9304	AS3356	AS3356	AS45102	AS45102	AS31133
亚洲	吉隆坡 47.250.*.16	AS45102	AS15802	AS9498	AS15802	AS15802					
		AS15802									
	北京 183.173.*.12	AS7497	AS2914	AS4637	AS4134	AS4134	AS4134	AS6453	AS4134	AS4134	AS4134
		AS7497	AS4134	AS9498	AS4809	AS4809	AS4134	AS4637	AS3356	AS3356	AS31133

对向远程受害者发送精心制作的ICMP重定向消息的可行性进行测量研究。

4.1 在互联网上转发重定向

根据ICMP规范[12, 67]，ICMP重定向消息应该只由当前第一跳门路向所连接的主机发出，这意味着ICMP重定向消息不应该在网际网络上被转发。因此，如果ICMP重定向信息出现在互联网上，它们应该被过滤机制[7, 28, 39]默默地丢弃，只允许合法流量通过网络。然而，通过对互联网的广泛测量研究，我们发现，精心制作的ICMP重定向消息仍然被允许穿越相当数量的AS，从而在互联网上成功转发。

实验设置。我们在全球4个地点部署了19个有利位置，以测试在互联网上不同AS中转发精心制作的ICMP重定向消息的可行性。我们从其中9个有利位置制作ICMP重定向，然后将制作好的消息发送到其余10个位置（关于我们均匀分布在世界各地的有利位置的更多细节，见表1）。请注意，我们在这个实验中没有进行任何IP欺骗，因为我们的目标是看重定向信息本身是否能在互联网上成功转发。

实验结果。表1显示了我们的实验结果。我们发现，在我们的90次测量中，精心制作的信息总是可以被转发到接收器，而没有任何

在互联网上的限制，即使信息的转发跨越了几个AS，而且信息的指定源IP地址显然是非法的，即信息的源IP地址是根本不可能是接收方的网关的发件人。

4.2 在目标AS中接收欺骗的重定向信息

除了在网上转发ICMP重定向消息，我们的远程DoS攻击还要求受害者发起人所在的目标AS不会丢弃伪造的ICMP重定向消息，该消息的源IP地址是AS内受害者的网关。

在我们对互联网的实证研究中，我们发现大量易受攻击的AS允许被欺骗的ICMP重定向信息（其源IP地址为这些AS内的网关）进入。这些被欺骗的信息将被成功地转发到附属于网关的受害者发起者，从而操纵受害者的网络流量（关于受害者发起者和互联网上相应的脆弱AS的检测细节，见第5.2节）。

我们完全检测到5184个脆弱的目标AS（位于全球185个国家）没有过滤欺骗的ICMP重定向消息。考虑到互联网上大约四分之一的AS还没有实施有效的过滤机制来阻止欺骗的数据包，这并不奇怪[44, 49]。表2列出了30个脆弱AS的详细信息。例如，如第一行所示，一个IP地址为154.54.x.157的网关位于AS 174，它位于美国，属于Cogent公司。

通信。我们用这个网关的欺骗性源IP地址伪造一个ICMP重定向消息，并将该消息发送到连接到这个网关的受害者（我们在Alexa前100万个网站列表中检测到的一个脆弱的网络服务器，更多细节见§5.3）。最后，被欺骗的ICMP重定向消息被成功地转发给受害者。

受到我们的DoS攻击。

表2：允许欺骗性重定向信息的易受攻击的AS。

帐户号：	GatewayAS No.	组织机构	地点
154.54.x.157	AS174	Cogent Comm.	美国
64.86.x.66	AS6453	TATA Comm. (AMERICA)	美国
45.79.x.5	AS63949	Linode, LLC	美国
204.93.x.159	AS23352	服务器中央网络	美国
72.29.x.133	AS7393	CYBERCON, INC.	美国
148.163.x.24	AS53755	输入输出洪流有限责任公司	美国
64.74.x.198	AS63410	私人系统网络	美国
209.58.x.15	AS394380	美国租赁网	美国
188.170.x.58	AS31133	PJSC MegaFon	RU
92.53.x.34	AS49505	OOO网络	RU
109.234.x.250	AS50340	OOO网络	RU
62.67.x.186	AS3356	Level3, LLC	AAA
213.239.x.230	AS24940	Hetzner Online GmbH	AAA
198.27.x.92	AS16276	OVH SAS	共和
89.30.x.146	AS31216	BSOCOM	共和
185.17.x.66	AS42831	英国专用服务器	GB
87.245.x.221	AS9002	RETN有限公司	GB
125.22.x.166	AS9498	BHARTI Airtel	纳入
183.83.x.29	AS18209	阿特里亚聚合	纳入
218.145.x.26	AS4766	韩国电信	KR
58.159.x.178	AS17506	ARTERIA网络	蒋介
159.226.x.203	AS7497	计算机网络	氯化
195.142.x.162	AS34984	TELCOM iletisim	AAA
80.67.x.207	AS42708	GleSYS AB	AAA
83.137.x.204	AS47692	Nessus GmbH	淘宝
103.245.x.150	AS17660	DrukNet ISP	英国
103.252.x.129	AS45638	协同批发	AU
118.98.x.254	AS18051	普斯泰科姆	身份
113.21.x.217	AS38082	真正的互联网	钰
45.138.x.1	AS207640	专家解决方案	创业

5 隐蔽的远程DoS攻击

在这一节中，我们提出了一种隐蔽的DoS攻击，它可以远程启动，利用弱的ICMP合法性检查机制，切断一对IP地址之间的通信。它不仅可以针对个人用户，例如，阻止一个人访问一个网站，还可以针对服务器之间的通信，例如，关闭DNS解析器与特定的权威名称服务器联系以解析某些域名。当Tor节点之间的通信被切断时，甚至有可能关闭整个服务的运作，如Tor。我们首先介绍了威胁模型和我们攻击的设计。然后，我们进行实证研究，以确定互联网上脆弱的公共服务器。我们发现43,081个流行的网站，54,470个开放的DNS解析器和186个居住在5,184个AS和185个国家的Tor中继节点都容易

5.1 威胁模型

图5说明了我们的路径外DoS的威胁模型。该模型由四个主机组成：1) 一个受害者发起者（在不同的攻击方案中，受害者发起者可能是一个网络服务器，一个开放的DNS解析器或一个Tor中继节点），2) 一个与受害者发起者连接到同一网关的邻近主机，3) 一个受害者目的地（相应地，在不同的攻击方案中，受害者目的地可能是一个网络客户端，一个权威的名称服务器或一个下一跳的Tor重铺节点），4) 一个非路径攻击者。路外攻击者的目的是假装成网关，并伪造一个ICMP重定向消息给发端者，从而将发端者对目的地的网络流量恶意地重定向到邻近的主机。由于主机在默认情况下是转发失效的，它们将作为黑洞，丢弃发端者的流量，这意味着路径外攻击者对受害发端者进行了成功的DoS攻击。为了完成DoS攻击，需要满足以下要求。

受害者的始作俑者

攻击者

图5：DoS攻击的威胁模型。

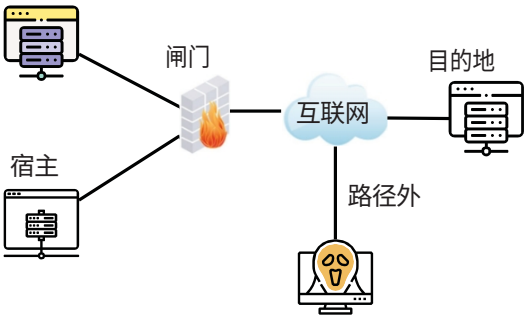
可追踪的网关。网关的IP地址对攻击者来说是已知的，因为攻击者需要冒充网关来制作ICMP重定向消息。一旦发端者的IP地址被确定，其网关的IP地址就可以通过traceroute[46]观察到。

IP欺骗。路外攻击者有能力发送带有网关IP地址的欺骗性数据包。先前的研究表明，互联网上大约四分之一的AS没有过滤离开其网络的带有欺骗源地址的数据包[44, 49]，从防弹托管节点租借这样的机器是很容易的[50]。此外，最近的一项研究[20]发现，互联网上有69.8%的AS不执行入口过滤来阻止欺骗的数据包，这进一步证明了IP欺骗的严重性。

脆弱的目标。目的地的出站流量将被误导的受害发起

人必须配备§3.2中列出的易受攻击的操作系统。因此，精心制作的ICMP重定向消息可以逃避发端者的检查，使发端者的路由中毒。

活的邻居主机。在目前的ICMP实现中，发端者将检查主机的可用性，当它



更新其路由以使用该主机作为其下一跳。攻击者可以探测发端者所在的网络，然后通过利用ICMP回波检测发端者的一个活的邻居主机⁵。

5.2 DoS攻击设计

图6展示了我们通过恶意的ICMP重定向进行DoS攻击的步骤。在开始的时候，受害者的发起者和目的地可以正常通信。在我们的攻击中，发起者可能是一个网络服务器，一个开放的DNS解析器，或一个Tor中继节点。相应地，目的地可能是一个网络客户端，一个权威的名称服务器，或一个下一跳的Tor中继节点，分别。路径外攻击者的目的是切断

发端人和目的地之间的通信。该攻击由八个主要步骤组成。

攻击者通过以下方式探测受害发端者的邻近主机
攻击者利用ICMP回波。

通过IP地址欺骗和伪造UDP数据报到受害者发端人的一个监听UDP端口。

受害者发端者被骗建立一个对攻击者来说可预测的UDP套接字，因为套接字的四元组，即源IP地址、目的IP地址、源端口（监听UDP端口）和目的端口（攻击者指定的前一个伪造的UDP数据报的源端口）、

攻击者知道。攻击者假装是通过Traceroute可以观察到的受害者起源地的网关（通过IP地址欺骗），然后伪造一个嵌入已知UDP的ICMP重定向消息。

伪造的ICMP重定向消息。

通过发端人的检查。
发起人更新其路由缓存，并将随后的网络流量（由IP承担的所有类型的网络流量）重定向到邻居家。

顺从地摄取主人。
重定向的流量会被丢弃在转发失效的邻居主机。

这意味着只有一个伪造的ICMP错误信息会导致发端者的DoS。当所有八个步骤都成功时，受害者发端者所在的AS也被认为是脆弱的，即收到§4.2所述的欺骗性ICMP重定向。

通过ICMP回波请求和回复。3) 网络客户端（即目的地），可以访问目标服务器，并接收原始响应。由于道德方面的考虑，所有的客户端都在我们的控制之下。为了全面评估这种攻击在现实世界中的影响，我们在世界各地的不同地点部署了6个controlled客户端（有利位置），即法兰克福、新加坡、加利福尼亚、东京、上海和多伦多。4) 位于俄罗斯的恶意攻击者可以欺骗源IP地址，旨在通过制作ICMP重定向消息来误导焦油服务器的网络流量（发送到我们控制的客户端）进入检测到的邻近主机（即路由黑洞）。如果DoS攻击成功，客户将无法收到来自脆弱服务器的响应。

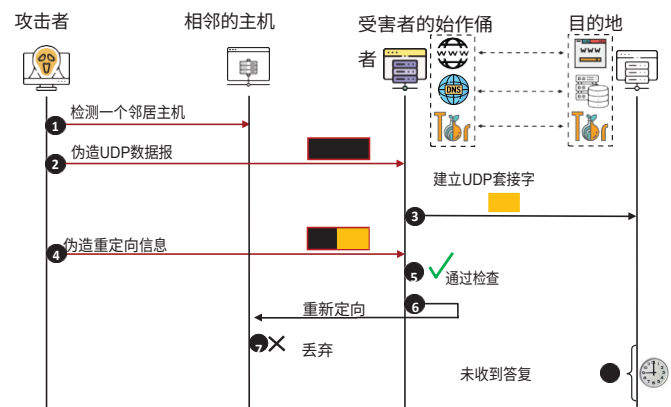


图6：Overview of DoS attacks.

实验结果。图7显示了我们的细节

DoS攻击测量结果。由于不同的网络条件，观察到的易受攻击网站的数量从

不同的视点有很大差异。例如，在弗兰克-此外，我们检测到28,604个脆弱的网站，而在上海、的攻击设计中的受害者发起者，如图6所示），其出站流量可能被伪造的ICMP重定向所操纵。在这个测量研究中，我们使用Alexa前100万网站的服务器作为目标。

2) 目标服务器的邻近主机，它们与服务器居住在同一网络中。这些主机可以被检测到

⁵ 例如，网站 "www.mit.edu" 的一个IP地址是104.76.0.251，我们可以探测到一个IP地址为104.76.0.252的活着的主机是它的邻居，它有相同的TTL和相同的网关（106.187.29.182）从我们的有利位置。

5.3 热门网站的案例研究

实验设置。涉及4种主机。1) 目标网络服务器（即我们

我们只能检测到19,603个脆弱的网站。我们把从六个观测点检测到的易受攻击网站集合在一起（删除在不同观测点检测到的重复网站），然后我们发现位于2872个AS和130个国家的43,081个流行网站对我们的DoS攻击是脆弱的。因此，在Alexa排名前100万的网站中，易受攻击的网站的比例约为4.3%。⁶有趣的是，在统计了我们检测到的最接近的1万个网站中的易受攻击网站的数量后，我们发现，网站的排名越低，它就越有可能被压缩，这也与普通的直觉相一致。

我们阐述了我们的DoS攻击可能失败的原因，如图7所示。平均来说，列表中有17.73%的网站无法从我们的有利位置到达，主要是由于两个原因。首先，我们的客户不能成功地重新

⁶ 2019年，Robert等人[53]测得Alexa前100万名中有1.3%的网站存在TLS padding oracle漏洞[84]。与TLS padding oracle攻击相比，Alexa前100万名中更多的网站容易受到我们的攻击。

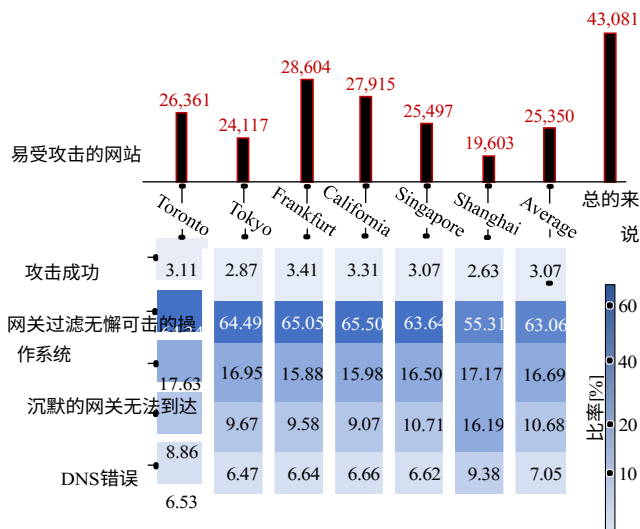


图7：针对流行网站的DoS测量研究。

收到请求网站的DNS回复（在不同的范围内）。阶段，比例在6.47%和9.38%之间变化）。第二，我们的客户无法连接到目标网站（在不同的有利位置，比例在8.86%和16.19%之间）。这两种无法访问的情况主要是由审查制度[71, 82]和ISP过滤规则[66]造成的。在计算我们攻击的成功率时，我们不考虑这些无法访问的网站。沉默的网关造成了16.69%的失败，也就是说，被检测到的网络服务器的网关没有对我们的探测做出反应。这些网关不透露他们的IP地址，因此攻击者不能冒充网关向target服务器发送恶意的ICMP重定向消息。63.06%的失败是由于网关过滤（如入口过滤[28]）或易受攻击的操作系统（如ICMP错误信息节流）。图8展示了我们检测到的脆弱网站的地理分布。

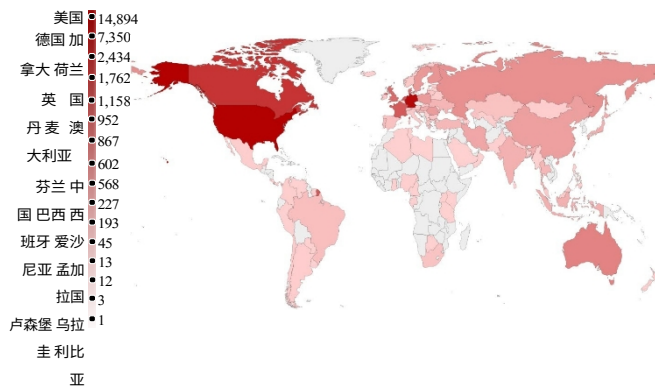


图8：脆弱网站的地理分布。

5.4 额外的攻击场景

ICMP合法性检查中的漏洞，例如，DNS解析器和下游的作者名称服务器之间的通信以及Tor中继节点之间的通信。我们对后端服务器之间的通信的DoS攻击将对现实世界造成更严重的破坏。例如，如果我们能阻止DNS解析器联系其下游权威名称服务器来解析某些域名，那么所有连接到易受攻击的DNS解析器的用户将被阻止访问这些域名。

在我们针对DNS和Tor的DoS攻击测量研究中，公共DNS解析器和Tor中继节点取代了§5.3中的网络服务器（即图-ure 6中的受害者发起者，其出站流量可能被误导到黑洞）。相应地，我们的受控下游授权者命名服务器和Tor中继节点取代了受害者网络客户端（即图6中的目的地）。

表3：DoS攻击测量结果的比较。

目标	数量	无法进入的	无坚不摧的操作系统	数量
		网关	或过滤	Vuls.
DNS解析器	1,951,381	39.69%	15.74%	54,470
				(4.63%)
Tor中继节点	6,518	18.52%	26.22%	186
				(3.50%)
网站	亚历克莎上衣100万	17.73%	16.69%	25,350
				(3.07%)

表3显示了我们在不同网络场景下的DoS攻击测量结果的比较。与热门网站的平均测量结果相比，我们发现互联网上有54,470个开放的DNS解析器（占从Censys[23]获得的1,951,381个目标的4.63%）和186个Tor重铺节点（占从Dan[21]获得的6,518个目标的3.50%）容易受到我们的DoS攻击，这意味着这些公共服务器的网络流量可以被重新操纵。

动的。请注意，在计算易受攻击的比例时，我们不考虑我们在加州部署的权威名称服务器和Tor中继节点的无法访问的目标。不受我们的DoS攻击影响的原因也在表3中列出。

6 网络流量劫持攻击

6.1 威胁模型

图9说明了我们对于网络流量的威胁模型

除了针对个别用户（即阻止一个人访问一个网站），路径外的攻击者甚至可以通过利用以下方式切断后端服务器与服务器之间的通信。

通过恶意的ICMP重定向进行劫持攻击。与DoS攻击的威胁模型不同，在这个模型中，攻击者和网络流量将被恶意操纵的受害者发起者居住在同一个网络中。攻击者和发起者所连接的网关可能是不同的，例如，将客户捆绑在一个公共IP地址后面的NAT设备、企业或家庭网络的路由器、生成和部署流量的SDN控制器。

规则[13]。请注意，尽管攻击者和受害者发端者居住在同一个网络中，但由于发端者和攻击者是通过交换网络（而不是广播链路网络）连接到网关的，所以路径外攻击者无法窃听发端者的流量。攻击者的目的是将发端者的目的地流量重定向到自己身上，并作为发端者的新网关，从而劫持发端者的流量，演变成MITM。

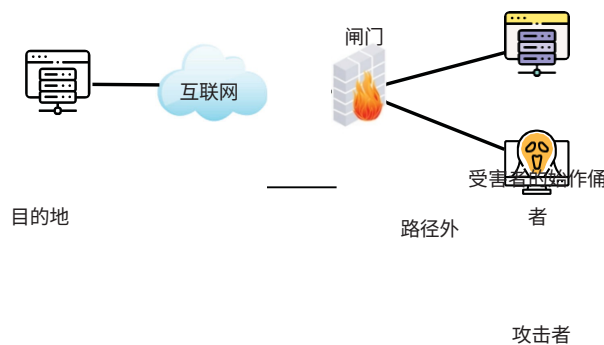


图9：劫持攻击的威胁模型。

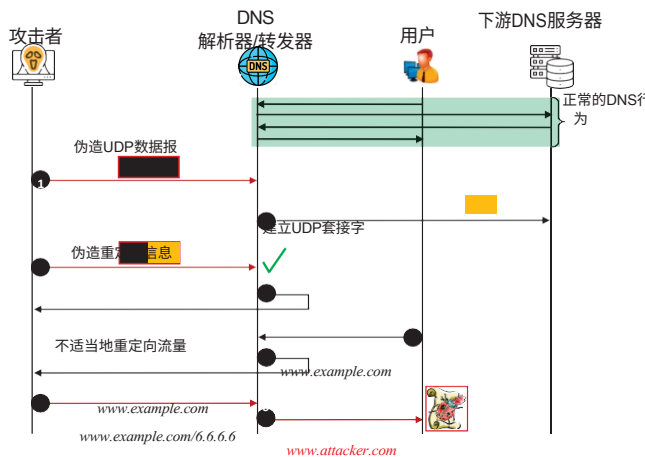
与DoS攻击相比，当攻击者和受害者发起者居住在一个网络中时，IP欺骗是可能的。⁷因为阻止欺骗数据包的安全功能通常部署在网关（较高的侵略层），以过滤流过的网络流量 [28]，ICMP内部欺骗的重定向不通过网关，因此不受阻挡。此外，由于攻击者是受害者发端者的一个活的邻居主机，它在满足最后一个要求并成为新的网关上没有困难（见 §5.1）。

6.2 DNS请求劫持的案例研究

我们的攻击可以在各种情况下进行，以保证网络的安全。我们在一个真实的摄像机网络中进行了一个案例研究，表明我们的攻击可以对NAT网络造成严重的破坏。由于IP地址空间的耗尽，NAT被提议作为一个标准，以允许互联网的扩展继续下去，而不转移到IPv6 [81]。现在，NAT无处不在，特别是在校园网、企业网和住宅网的边缘[47]。在NAT网络中，本地DNS解析器[36, 54]或DNS守护者[36, 72]相当普遍[40, 72, 73]，因为它们可以在本地访问，以减少网络延迟，避免直接暴露于互联网攻击者[35]。在这个问题上，我们表明，路径外攻击者可以劫持来自本地DNS转发器的查询，然后毒害NAT网络的本地DNS缓存。因此，路径外攻击者可以隐蔽地操纵同一网络下所有用户的DNS请求。我们在真实的校园

在一个单一的公共IP地址后面。2) 一个部署在NAT网络中的脆弱的DNS for- warder，它配备了Linux内核5.5版本和BIND 9.16.8。DNS for- warder接收来自NAT网络中用户的DNS请求，然后转发这些查询。3) 一个远程的下游DNS服务器，接收来自转发器的查询，并将答案返回给转发器。在我们的测试中，我们将谷歌的流行DNS服务8.8.8.8设置为下游DNS服务器。4) NAT网络中的受害用户，他们访问本地DNS转发器，获得他们查询的域名的IP地址。5) 位于同一NAT网络中的非路径攻击者-

工作。攻击者没有能力窃听他人的流量，它的目的是通过恶意的ICMP重定向，将DNS转发器的流量重定向到自己身上。因此，攻击者，可以劫持DNS请求，然后毒害整个NAT网络的DNS缓存。



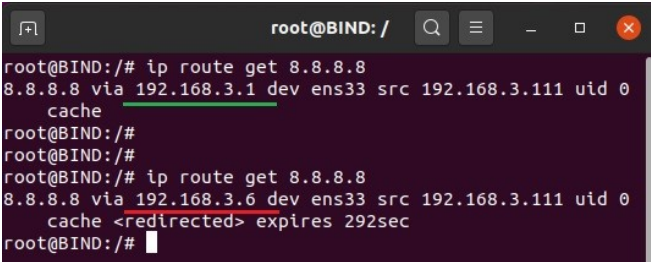
网络中实现了这种攻击，并在道德上显示了其严重性。
实验设置。在这次攻击中涉及5种类型的设备。1) 一个捆绑了120个客户端的HUAWEI NAT网关

⁷ 我们测试了10个真实世界的交换网络，即4个校园以太网LAN，4个企业以太网LAN和2个政府以太网LAN。在所有情况下，我们都能顺利地传递被欺骗的ICMP重定向信息。

图10：NAT网络中的非路径DNS 请求劫持。

实验工作流程。图10展示了如何通过恶意的ICMP重定向在NAT网络中进行非路径DNS请求劫持的工作流程。在正常情况下，DNS的行为是非常直接的。用户向转发器（或解析器）发送DNS查询。转发器和远程服务器完成域名到IP地址的映射，然后将查询结果反馈给用户并缓存在转发器中。在我们的攻击中，攻击者首先冒充服务器向转发器的监听端口5353发送UDP数据报，因为我们观察到多播DNS服务在目标转发器中始终可用。转发器将被欺骗建立一个可预测的UDP套接字，允许攻击者伪造可接受的ICMP重定向消息，并指定攻击机器为转发器的新网关。在转发者对下游DNS服务器的流量被成功重定向后，用户对转发者的DNS查询如果没有被缓存，就会被错误地转发到攻击者那里。然后，路径外的攻击者会丢弃原始的DNS查询，冒充DNS服务器向转发者发送伪造的答案。最后、

转发器用一个假的IP地址回复用户，这个地址也将被缓存在转发器中。因此，由于缓存poisoning，NAT网络中的所有用户都将受到隐蔽的影响。



```
root@BIND: /  
root@BIND:/# ip route get 8.8.8.8  
8.8.8.8 via 192.168.3.1 dev ens33 src 192.168.3.111 uid 0  
cache  
root@BIND:/#  
root@BIND:/#  
root@BIND:/# ip route get 8.8.8.8  
8.8.8.8 via 192.168.3.6 dev ens33 src 192.168.3.111 uid 0  
cache <redirected> expires 292sec  
root@BIND:/#
```

图11：中毒的 DNS解析器的路由缓存。

实验结果。图11显示了易受攻击的本地DNS转发器（其IP地址为192.168.3.111）的中毒路由缓存的结果。该DNS转发器到服务器8.8.8.8的原始网关是192.168.3.1。然而，一旦攻击者执行了我们的劫持攻击，DNS转发器到8.8.8.8的下一跳就会被改写成攻击主线，即192.168.3.6。因此，攻击者可以拦截转发者的查询，然后冒充下游服务器，用假的答案回复转发者。

本地DNS缓存被毒害后，NAT网络中的所有用户都会受到影响，也就是说，路径外攻击者可以任意操纵用户的网络请求。图12显示，由于用户从中毒的DNS转发器收到了假的域名IP地址，用户（出于道德考虑，我们控制下的客户主机）对 "www.yahoo.com "网站的请求被劫持到一个假的网站。由于攻击流量小（实际上只有一个ICMP重定向数据包），劫持攻击是隐蔽的，这意味着成本也可以忽略不计。

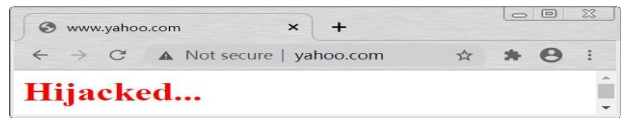


图12：DNS请求被劫持的快照。

7 讨论

负责任的披露。我们向Linux、FreeBSD和AOSP（安卓开源项目）社区报告了该漏洞 和我们的PoC。安卓已经确认了这个漏洞，目前正在与我们讨论对策。我们与

Linux和FreeBSD进行了几轮讨论，但还没有被告知任何决定。此外，我们在互联网上联系了16家受影响的供应商，以披露该漏洞，但还没有收到回复。

7.1 与现有攻击的比较

ICMP重定向攻击以前被认为只是局域网中ARP poisoning的现有操纵攻击的一种替代方法[77, 89]。然而，我们证明本文所开发的攻击是完全不同的。首先，通过利用ICMP合法性检查的漏洞，我们可以远程制作一个可接受的ICMP重定向消息来重写受害者的特定目的地的路由，而不是ARP表。因此，我们的攻击可以在互联网上进行，不受网络拓扑结构的限制。其次，我们的攻击更加隐蔽，因为攻击者只需要向易受攻击的目标发送一个伪造的ICMP重定向信息，而不是广播伪造的数据包（即ARP中毒攻击中的ARP回复数据包，可能导致IDS日志被可疑的流量记录填满）。此外，MAC-IP绑定[59,69]和未经请求的ARP回复丢弃[45,51,78]的对策已经被提出，以防止ARP中毒攻击。相比之下，我们的攻击很难通过这些对抗措施来预防，因为该行为在第二层是正常的。

7.2 来自路由缓存的影响

攻击规模与路由缓存大小有关。一旦攻击者成功地误导了受害者发端者对某一特定目的地的网络流量，受害者将在其路由缓存中用一个新的路由条目替换该目的地的路由条目。因此，多少个目的地的流量可以同时被操纵（即攻击规模）是由受害者发端者的路由缓存大小决定的。在实践中，我们观察到，路由缓存在现代操作系统上是动态分配的，其大小在不同的实现中是不同的。例如，在我们针对装有Linux内核版本3.9.10和5.4.0的脆弱服务器的实验中，我们可以通过向服务器并行发送伪造的ICMP重定向消息（指定不同客户的流量需要被重定向），迫使服务器失去连接，最多可达10240个客户。相比之下，对于装有FreeBSD内核12.2版本的易受攻击的服务器，我们可以迫使服务器同时失去多达55000个客户的连接。在不同的网络场景下，路由缓存大小对我们的DoS攻击的影响是不同的。例如，在我们针对网站和开放的DNS解析器的攻击中，受害者的路由缓存大小对于前者意味着有多少前端网络用户可能同时丢失，而对于后者意味着有多少后端域名可能同时丢失。

由于路由条目的时间限制，攻击失效。在我们的实验

中，我们发现在内核版本为3.9.10及以上的Linux系统中，中毒的路由（即路由缓存中的虚假路由条目是由一个精心制作的ICMP重定向消息导致的）将被缓存300秒。在300秒的时间限制之后，原始路由

指定默认网关为受害者的下一跳的条目将被自动恢复。因此，如果受害者配备的是3.9.10及以上版本的Linux内核，我们的攻击可能在300秒内失效。在实践中，为了永久地毒害目标的路由，攻击者可以在每300秒内持续发送一个伪造的ICMP重定向消息，以防止自动恢复原始路由。

7. 3 IPv6网络中的 攻击

在IPv6网络中，类型=137和代码=0的ICMPv6消息被当前第一跳路由器用来通知发端主机，在通往特定目的地的路径上有一个更好的第一跳路由器，或者通知发端主机，目的地实际上是一个邻居[60]。我们发现，ICMPv6的合法性检查机制和无状态协议之间的差距仍然存在。正如ICMPv6规范[19,60]所述，ICMPv6重定向消息应尽可能多地嵌入触发数据包，而不使重定向消息超过IPv6的最小MTU（即1280字节）。然而，启用IPv6的受害者也不能对嵌入无状态协议数据的ICMPv6消息进行精确的验证，除了一些简单的检查（例如，UDP套接字的存在），可以很容易地逃避。因此，我们的攻击可以很容易地扩展到IPv6网络，以操纵受害者发起人的网络流量。

8 反措施

网络改变。在网络层面，ISP可以对网络进行改变以阻止ICMP重定向。首先，应该应用入口过滤[28]来阻止互联网上一般的欺骗性数据包，包括欺骗性ICMP消息。此外，一个有效的ICMP重定向消息必须欺骗受害者的网关IP地址。这意味着网络更容易识别和阻止欺骗性的传入ICMP重定向消息，因为来自网络外部的数据包不应该有一个内部节点的源IP。我们确实注意到，这种防御不一定适用于局域网攻击者。第二，ICMP重定向消息应该是由本地网关发出的，因此在设计上不应该出现在互联网上[67]。然而，这一政策也无助于对付局域网攻击者。

协议变更。另一个可能的对策是修改协议，以改善ICMP的合法性检查机制。例如，UDP可以重新设计一个扩展（即头），在会话开始时嵌入一个额外的秘密--类似于

TCP的MD5选项。在这样的设计中，非路径攻击者将不知道这个秘密，因此无法制作一个合法的ICMP消息，在UDP头中嵌入正确的值。然而，这种变化是实质性的，因为它需要对UDP和任何其他可能被攻击者利用的状态较差的协议进行根本的改变。因此、

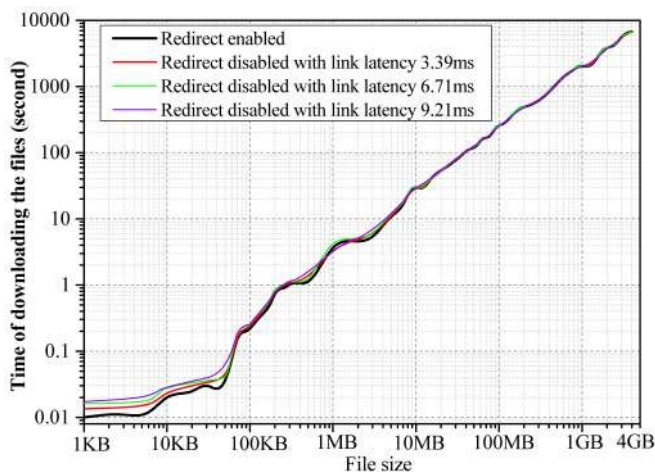
在现实世界中部署这一对策是一个重大挑战。

主机改变。鉴于前述对策的局限性，我们提出了另一种防御措施，可以单独部署在受害主机上以阻止攻击。具体来说，我们建议关注ICMP重定向攻击的单个主机禁用无状态协议的ICMP重定向机制。根据ICMP规范[6,67]，在发起者禁用ICMP重定向机制将导致使用次优路由路径到目的地，由于穿越额外的节点（即原始网关）而产生额外的链路延迟；然而，它不影响网络的连接性。因此，产生的额外链路延迟（即增加的RTT）是该对策的唯一副作用。请注意，这种副作用并不适用于TCP，因为我们仍然允许ICMP重定向消息嵌入TCP数据包。我们在现实世界中建立了反措施的原型，并在不同的网络场景中对其进行了评估，特别是对两个广泛使用的基于UDP的应用程序，即TFTP和QUIC，产生了性能损失。

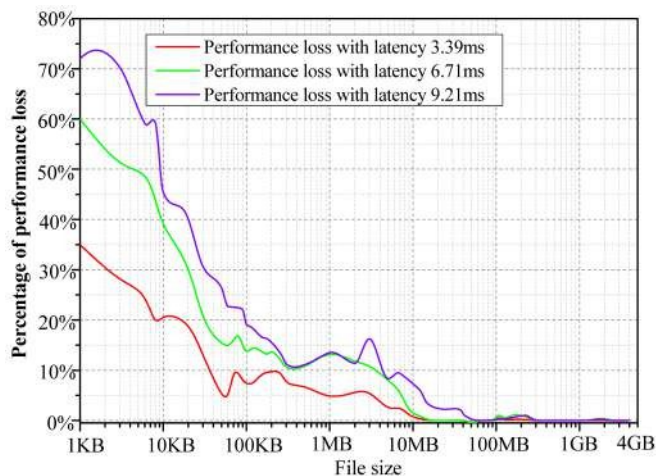
首先，我们在通过TFTP下载文件的情况下评估我们的反措施。我们建立了一个真实的测试平台，在AS4538（带宽10Gbps）内有一个脆弱的UDP服务器，在AS7494（下行带宽10Mbps）内有一个客户端。该服务器有两个网关。两个网关中的一个比另一个有额外的链接，我们用三种不同的链接延迟来衡量我们的对策的影响，即分别为3.39毫秒、6.71毫秒和9.21毫秒。最初，我们将服务器设置为使用次优的网关。当服务器的UDP流量启用ICMP重定向机制时，服务器会动态地更新其路由，以使用最佳网关。相反，当ICMP重定向被我们的对策禁用时，服务器总是使用它的默认和次优网关。

我们能够确认，受我们对策保护的服务器将忽略嵌入UDP数据报的ICMP重定向消息，从而成功地防御攻击。为了确定使用次优路径所引起的性能下降，我们通过TFTP将视频文件从服务器下载到客户端，并比较启用和不启用我们对策的下载时间。图13 (a) 显示了下载不同大小的文件的时间。可以看出，不同的链接延迟（即3.39毫秒、6.71毫秒和9.21毫秒）由于我们的对策而引起的影响了下载时间，特别是当文件大小小于100KB时，链接延迟越大，下载文件的时间就越长。如图13(b)所示，我们的对策所带来的额外下载时间按百分比计算对小文件来说是很重要的。这是因为链接延迟（即RTT）通常占了下载小文件的大部分时间，因此

我们的对策中增加的链接延迟非常重要。然而，当文件很小（100KB或



(a) 启用或不启用ICMP重定向时下载文件的时间。



(b) 禁用ICMP重定向后的性能损失。

图13：在通过TFTP下载文件的情况下对我们的反措施进行评估。

少），下载文件所需的绝对时间（见图13(a)）是微不足道的，远远小于一秒钟。当文件超过1MB时，我们看到性能损失的百分比迅速减少到17%（或当文件大小超过100MB时<1%）。这是因为大文件对我们的反击所引入的额外链接延迟不敏感，而且所产生的延迟占到了传输文件总时间的一小部分。

其次，我们评估了我们的反措施对基于UDP的QUIC协议的影响。实验设置如下。AS132203内的一个易受攻击的网络客户端运行Chrome浏览器来访问谷歌的网站。客户端和谷歌网站服务器之间的通信是由基于UDP的QUIC协议进行的。客户端的带宽是20Mbps，它有两个网关。起初，我们将客户端设置为使用次优路径的网关，其额外的链接延迟分别为3.25毫秒、6.36毫秒和9.93毫秒。当客户端的UDP流量启用ICMP重定向机制时，它将动态地更新其路由，使用最佳路径中的网关来访问Web服务器。相反，当ICMP重定向被禁用时，客户端总是使用其默认和次优的。

我们在不同情况下（即启用ICMP重定向和禁用ICMP重定向，延迟分别为3.25毫秒、6.36毫秒和9.93毫秒）从客户端向服务器发出1000个请求，然后比较加载网页的时间。图14显示了不同情况下页面加载时间的累积分布函数（CDF）。平均而言，三种设置的性能惩罚（额外的页面加载时间）分别为4.92毫秒（1.38%）、11.81毫秒（3.32%）和26.68（即7.51%）毫秒。

综上所述，我们提出了三种不同的对策（即网络改变

、协议改变和主机改变）。

以减轻已确定的攻击，并显示每个对策的适用场景。
网络运营商可以根据自己的要求选择合适的对策。

9 相关工作

ICMP重定向的滥用。ICMP重定向是RFC792[67]中提出的一项标准，被网关用来通知主机更好的路由。然而，它也被攻击者滥用，重写受害者主机的路由。Bellovin提出滥用ICMP重定向来重写受害者主机的网关，结果是操纵了受害者的网络流量[8,9]。然而，人们认为，重定向信息必须与现有的连接相联系，并且该信息不能被用来对受害者的路由进行未经请求的改变[8]。此外，重定向被认为只适用于有限的拓扑结构[8,9]。最近，ICMP重定向被用来进行侧信道攻击，可以推断出DNS查询中使用的短暂端口号，导致DNS缓存中毒[38]。Zimperium提出了 "DoubleDirect"，它首先重定向受害者的DNS流量并识别受害者正在访问的IP，然后它再次重定向受害者的traf-fic发送至这些IP，从而实现全双工MITM [89]。然而，由于Linux不接受ICMP重定向信息，所以被认为Linux是不可抗力的。我们发现了ICMP合法性机制的漏洞，并证明了Linux系统也有严重的脆弱性。

在Kulas的演讲中，ICMP回波被利用来规避Windows 7和不包括内核版本3.6.x的Linux sys- tems的合法性检查机制，然后在LANs上进行ICMP重定向攻击[41]。实际上，我们测量到 Windows 7（Windows 7 professional with SP1, SP2 and SP3）对嵌入ICMP回波的ICMP重定向信息是无能为力的，因为Windows系统没有严格遵循ICMP规范（Windows启用ICMP重定向

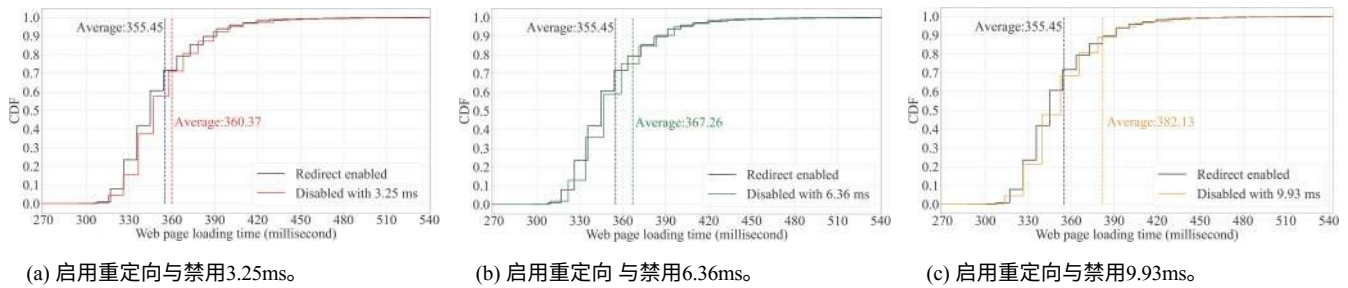


图14：我们的对抗措施对QUIC应用程序的性能影响。

默认情况下，它不会对收到的ICMP重定向消息作出反应，即使这些消息是合法的[80])，我们证明Linux内核版本的

3.6.x (即3.6.0~3.6.11版本) 仍然可以在我们的攻击中被破坏。此外，在现实世界中，ICMP回波可能是由于性能和安全方面的考虑[79]而被阻止，导致了之前攻击的失败。与她的工作不同，我们揭示了ICMP合法性检查的漏洞，并发现一套无状态协议是可以利用来逃避检查的。此外，我们首次将攻击扩展到Inter-net，并在现实世界中发现了大量易受攻击的公共服务器。

实际上，以前关于ICMP重定向攻击的研究可以搜索到不少[48,56,63,85,86]，包括那些重新在技术博客或教科书中租赁的[5,22,37,83]。然而，目前，这些攻击很少能在互联网上成功，因为它们只能在早期的广播链路网络中进行[48,56,63,86]，或者伪造的ICMP重定向信息不能通过现代操作系统的检查[5,22,37,83,85]。例如，UDP套接字的存在将被检查，这将阻止接受先前伪造的ICMP重定向信息[5,22,37,83]。

路外网络流量操纵。 Qian 等人讨论了TTL过期的ICMP错误消息可以被用来终止TCP连接，但是消息中嵌入的序列号必须通过检查机制，这是很不可能的[68]。通过挑战ACK机制中的侧信道[70]，Cao 等人证明了一个纯粹的非路径攻击者可以终止或毒害一个受害者的TCP连接，从而恶意操纵受害者的TCP流量[14,15]。Chen和Qian表明，半双工IEEE 802.11或Wi-Fi技术中存在的定时侧信道也可以被路径外攻击者利用来操纵TCP流量[16]。Man 等人提出，路径外攻击者可以利用ICMP速率限制中的侧信道来操纵UDP流量，从而使DNS缓存中毒[50]。Feng 等人新的混合IPID分配中发现了一个侧信道，也可以被路径外攻击者利用来操纵TCP流量[26,27]

。这些攻击的目标都是针对传输层的网络流量，例如TCP和UDP，而我们提出的攻击将包括

承诺由IP层承担的所有流量。此外，以前的大多数攻击已经被安全界缓解了[14,15,50]。

控制平面的路由劫持（例如，异常的BGP公告[17,62,74]和OSPF路由表中毒[57,58,76]）也允许非路径攻击者操纵网络流量。幸运的是，已经提出了安全机制来防止这些攻击[10,11,43]。IP碎片也经常被用来操纵网络流量，如DNS缓存中毒[33,34]，流量互斥[29,30]，或IDS规避[4,65,75]。已经提出了几个标准来发现路径MTU，从而防止IP碎片的滥用[24,52,55]。

10 总结

在本文中，我们研究了ICMP规范中的漏洞，该漏洞可以被纯粹的非路径攻击者利用来逃避检查机制。在这个出现在各种主要操作系统中的漏洞的推动下，我们证明了ICMP重定向攻击可以在现实世界中恢复活力，造成严重破坏。特别是，我们证明了远程非路径攻击者可以对互联网上的公共服务器进行隐蔽的DoS攻击，而互联网上大量的公共服务器都容易受到我们的攻击。我们还证明，如果路径外攻击者和受害者居住在同一个网络中，攻击者可以通过发布伪造的ICMP重定向消息来构建MITM攻击。我们开发了不同的对策来对付这些攻击。部署在主机上的增强型ICMP重定向机制的原型证实了我们的反措施的有效性，对网络性能的副作用有限。

鸣谢

我们感谢匿名审稿人提出的有见地的意见。特别是，我们感谢我们的导师Alexandra Dmitrienko对我们工作的指导。这项工作得到了中国国家杰出青年科学基金（编号：61825204）、国家自然科学基金（编号：61932016）和中国科学院院士（编号：61932016）的部分支持。