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。

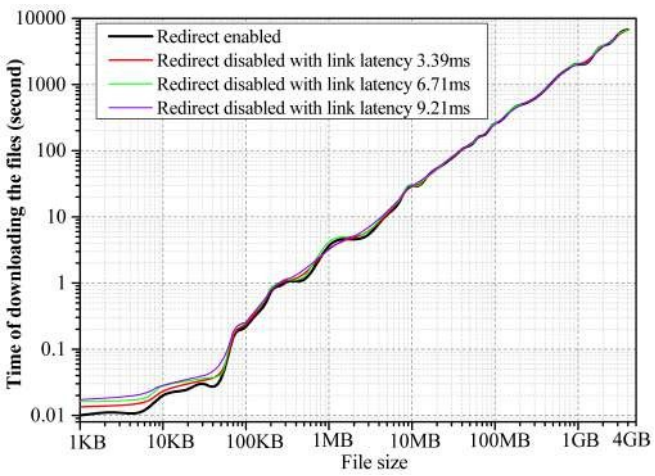
协议变更。另一个可能的对策是修改协议，以改善ICMP的合法性检查机制。例如，UDP可以重新设计一个扩展（即头），在会话开始时嵌入一个额外的秘密--类似于TCP的MD5选项。在这样的设计中，非路径攻击者将不知道这个秘密，因此无法制作一个合法的ICMP消息，在UDP头中嵌入正确的值。然而，这种变化是实质性的，因为它需要对UDP和任何其他可能被攻击者利用的状态较差的协议进行根本的改变。因此、

在现实世界中部署这一对策是一个重大挑战。

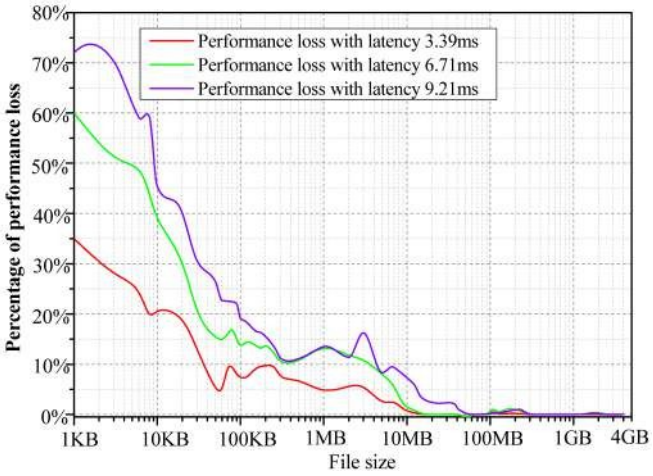
主机改变。鉴于前述对策的局限性，我们提出了另一种防御措施，可以单独部署在受害主机上以阻止攻击。具体来说，我们建议关注ICMP重定向攻击的单个主机禁用无状态协议的ICMP重定向机制。根据ICMP规范[6,67]，在发起者禁用ICMP重定向机制将导致使用次优路由路径到目的地，由于穿越额外的节点（即原始网关）而产生额外的链路延迟；然而，它不影响网络的连接性。因此，产生的额外链路延迟（即增加的RTT）是该对策的唯一副作用。请注意，这种副作用并不适用于TCP，因为我们仍然允许ICMP重定向消息嵌入TCP数据包。我们在现实世界中建立了反措施的原型，并在不同的网络场景中对其进行了评估，特别是对两个广泛使用的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

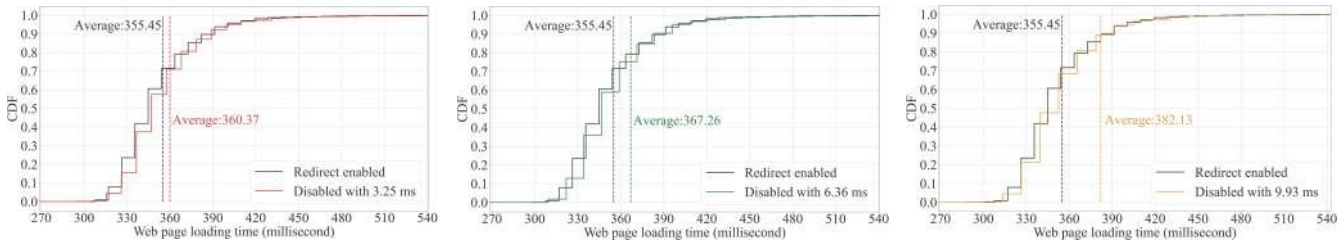
综上所述，我们提出了三种不同的对策（即网络改变、协议改变和主机改变）。

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



(a) 启用重定向与禁用3.25ms。 (b) 启用重定向 与禁用6.36ms。 (c) 启用重定向与禁用9.93ms。

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错误消息可以被利用来终止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*在新的混合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碎片也经常被利用来操纵网络流量，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。