基于网络地址转换的通信行为隐藏

陶怀舟[1]，黄永峰[1]，杨震[1]

（1. 清华大学 电子工程系，下一代网络及应用实验室，北京 100084）

摘　要:信息隐藏技术以最小的改动向载体中嵌入秘密消息,通信双方通过传输载密载体来隐藏秘密消息内容以及隐蔽通信行为。但在实际应用中，有时双方的正常通信行为就足以引起怀疑。针对这一问题，本文提出利用网络地址转换技术实现对直接通信的隐藏。与匿名通信技术洋葱网络相比,本文的方法不使用特殊的加密协议，隐蔽性更强，延时更低。

关键词：行为隐藏；网络地址转换

Communication behaviour hiding based on network address translation

TAO Huaizhou[1], HUANG Yongfeng[1], YANG Zhen[1]

（1. Lab of Next Generation Network Technology & Applications, Department of Electronic Engineering, Tsinghua University, Beijing 100084, China）

Abstract: The steganographic techniques embed secret messages into the carrier with minimal modifications, then the communication parties transmit the carrier to hide secret message content and covert communication behavior. However, in practical applications, sometimes the normal communication behavior is enough to cause suspicion. In response to this problem, this paper proposes to use network address translation(NAT) technology to hide the direct communication behavior. Compared with The Onion Routing(Tor), a kind of anonymous communication system, the method of this paper is more concealed and has lower latency because it does not use a specific encryption protocol.

Key Words: Behaviour hiding; network address translation

信息隐藏技术可向载体中嵌入秘密消息而不引起易被察觉的变化；通过传输载密载体，使用者可在不引起监听者注意的情况下完成隐蔽通信[1]。互联网与多媒体技术的发展给信息隐藏技术提供了广阔的空间与丰富的载体，大量现代信息隐藏技术将消息嵌入到音频[2]，图像，视频[3, 4]甚至文本[5, 6]当中。

然而随着技术的进步，网络上监听者与攻击者的能力也更加强大。在某些特殊情况下，仅仅是隐蔽通信双方的正常通信行为都足以引起监听者的怀疑。针对这一状况，ZHANG[7]提出了利用社交媒体账户的网络行为进行信息隐藏；发送者通过某个账户在社交媒体上的点赞等行为携带秘密消息，而接收者则记录该账户的行为并将其还原为秘密消息；发送者与接收者之间不存在直接通信，提高了通信链路的隐蔽性。然而这种方法携带信息量较小，且可能被社交媒体中的异常检测技术[8, 9]发现。

收稿日期： 2019-mm-dd

基金项目： 国家自然科学基金资助项目（U1636113，U1536207）

作者简介：陶怀舟（1989－），男，硕士研究生。

通信作者：黄永峰，教授，E-mail：yfhuang@mail.tsinghua.edu.cn

隐藏通信链路的另一种可能方法是匿名通信技术。该技术的目标是隐藏通信单方/双方的真实地址，使监听者无法对通信进行溯源或跟踪，也就无法获得通信双方的真实身份。洋葱网络（The Onion Router, Tor）[10]就是一种应用广泛的基于转发的匿名通信技术。洋葱网络通过代理节点构造虚拟链路，在通信过程中对数据进行层层加密，从而保证每个节点都不知道完整的通信链路，防止攻击者对通信进行溯源。然而，洋葱网络需要使用特殊的加密协议；在隐蔽通信模型中，对数据内容加密足以引起监听者的怀疑。

因此，本文提出了一种基于网络地址转换（Network Address Translation, NAT）[11]的通信行为隐藏方法。该方法同样让通信双方通过代理节点建立间接的通信链路；但在传输过程中使用正常的网络协议，通过地址转换使得监听者无法追踪完整的通信链路。与洋葱网络相比，本文方法具有高隐蔽性，低时延的优点。

本文第一章介绍了洋葱网络的基本原理与局限，第二章描述了基于源地址转换的通信行为隐藏，第三章建立了基于地址转换的通信行为隐藏网络，第四章为结论。

1 洋葱网络

洋葱网络在 1990 年代中期由美国海军研究实验室以及美国国防高等研究计划署开发，目的在于保护美国的网络情报系统以及为美国的情报人员提供安全隐蔽的通信手段。

Tor 的基本原理是通过多层加密与链路传输，在网络通信过程中隐藏源地址与目的地址的直接通信。由于其使用特殊的多层加密协议，因此进行 Tor 通信需要一个规模可观的洋葱网络；目前这一网络是由世界各地的志愿者与使用者组成的。为发送一个 Tor 数据包，源端会首先访问“目录节点“，获取可用的节点列表。再从列表中选取一些节点，例如 Router A/B/C，并将它们排列成一条链路。规划链路完成后，源端以倒序对发送信息进行层层加密；首先将信息内容与目标地址使用 Router C 的密钥进行加密；再加入 Router C 的信息，并用 Router B 的密钥进行加密；最后加入 Router B 的信息，用 Router A 的密钥加密。由于数据包的多层嵌套结构类似于洋葱，因此该项技术得名洋葱路由。

在报文发送过程中，源端首先将数据包发送给 Router A。Router A 仅能对第一层进行解密得到 Router B 的信息，之后再将剩余部分发送给 Router B；Router B 重复解密操作将数据包发送给 Router C，Router C 最后将消息内容发送给目的端。在整个通信过程中，无论监听者在哪一位置截获洋葱数据包，都无法获取通信真正的源地址与目的地址；同时，参与通信的节点也无法知道源地址与目的地址；每个节点都只能获得数据包上一跳与下一跳的信息，无法探测出整个链路。

由于 Tor 需要使用特殊的多层加密协议，因此它具有明显的局限性。首先，使用 Tor 进行匿名通信的延迟很高；使用者通常要忍受高达十几秒的延迟，同时也很难进行实时的语音或视频通信。其次，由于 Tor 协议与正常网络通信协议完全不同，使用 Tor 协议本身就暴露了源端希望进行匿名通信的意图。因此，通信行为隐藏应该在使用常见的协议的条件下改变通信链路，将隐蔽通信行为隐藏于大量正常网络流量之中。

2 基于源地址转换的通信行为隐藏

网络地址转换是一种当数据包通过路由器或网关时，修改 IP 头部的源地址或目的地址的计算机网络技术。通过使用 NAT 技术，可以使一个私有网络中的多台主机只通过一个公有 IP 地址访问因特网。NAT 技术正是在 1990 年代中期，在 IPv4 地址即将耗尽，而接入因特网的设备数量飞速增长的背景下，在全世界范围得到了广泛的应用。图 1 所示为源地址转换（Source Network Address Translation, SNAT）的基本原理，内网客户端通过网关向服务器建立连接，网关对连接状态进行跟踪，并将发出的报文源地址修改为网关的公有 IP 地址。服务器对网关进行回应，由网关将接收的数据包进行转换传回内网客户端。在这个过程中，服务器只能与网关通信，而子网内部其他设备的地址和端口对服务器来说是不可见的；如果在公网上存在监听者，监听者也只能探测到网关与服务器的通信，而无法得知内网设备的存在，更无法对其进行定位，攻击与渗透。

因此，SNAT 技术除了可以节省 IP 地址，同时也在网络中有效地隐藏了内网设备，提高了接入因特网设备的安全性。由于这一特性，使用 SNAT 技术进行通信行为隐藏是可能的。

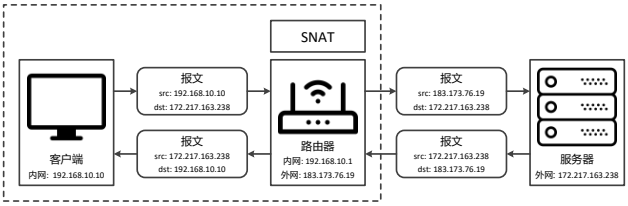


图 1 SNAT 基本原理示意图

仍以图 1 为例，如果客户端希望与服务器进行隐蔽通信，它可以网关作为代理，从而隐藏通信行为本身。对载体进行嵌入后，客户端将包含载密载体的报文发送给网关，网关修改报文源地址并将其发送给服务器；服务器返回的载密报文也通过网关进行地址转换，最终完成通信过程。在通信过程中，由于 SNAT 对公网隐藏了内网设备，公网的监听者只能探测到网关与服务器的通信行为，而无法探测客户端到服务器的整条通信链路；从而实现了通信行为的隐藏。

基于 SNAT 的通信行为隐藏可以很方便地进行扩展。如图 2 所示，Alice 和 Bob 可通过两层的 SNAT 代理进行通信行为隐藏，每一层的代理都对报文的源地址进行转换。对于公网上的监听者 Wendy 1，他只能探测到代理 2 与 Bob 的通信行为，而无法探测到 Alice 的存在；对于处于中间网络的监听者 Wendy 2，他只能探测到代理 1 与 Bob 的通信行为，同样无法探测到 Alice 的存在。也可以在此基础上，加入更多的代理进行多层的 SNAT 通信行为隐藏。

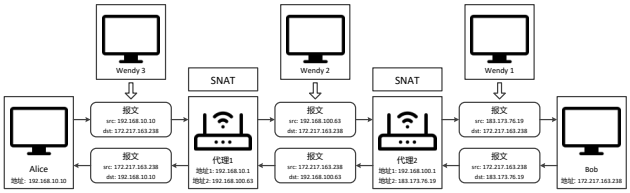


图 2 多层 SNAT 通信行为隐藏示意图

同样由图 2 可以看出，基于 SNAT 的通信行为隐蔽仍然存在缺陷。例如，如果在 Alice 所处的内网中存在监听者 Wendy 3，他就可以截获源地址为 Alice 且目的地址为 Bob 的通信报文，从而探测到 Alice 与 Bob 的通信行为。同样，如果 Wendy 2 监听到了代理 1 与 Bob 的通信行为，由于 Alice 与代理 1 处于同一子网，Wendy 2 也能确定该子网中存在设备正在与 Bob 进行通信。例如在实际应用中，某情报人员在酒店中与目标进行隐蔽通信，而监听者监控了酒店的网关；那么监听者很快就能确定该情报人员位于酒店内部。

3 基于地址转换的通信行为隐藏网络

SNAT 通信行为隐藏的缺陷，其主要原因在于 Bob 的地址在整个通信链路中都是暴露的。因此，为了达到通信行为隐藏的目标，有必要在通信链路中对 Alice 与 Bob 的地址都进行隐藏。目的地址转换（Destination Network Address Translation, DNAT）技术通过修改报文的目的地址，可以使外网的设备通过网关，向内网服务器发起连接请求并进行通信。DNAT 的基本原理如图 3 所示，外网上的客户端向网关发送报文，网关将报文的目的地址转换为服务器的内网地址，从而通过网关建立了外网客户端向内网服务器发起的连接。对于外网客户端来说，他只与网关进行通信，无法探测到内网服务器的存在；因此 DNAT 技术有效地对内网提供服务的设备进行了隐藏。DNAT 技术常常被用于提升服务器的安全性，以及实现负载均衡等功能。

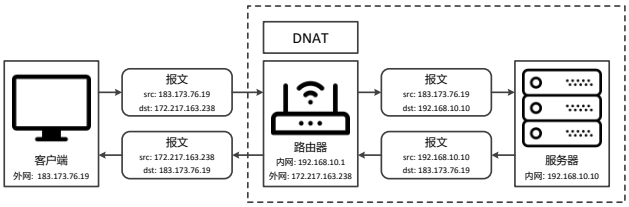


图 3 DNAT 基本原理示意图

结合 SNAT 与 DNAT 技术，即可实现在整条通信链路上的通信行为隐藏。如图 4 所示，Alice 首先发送目的地址为代理的报文；代理对报文的源地址与目的地址都进行了修改，源地址修改为代理，而目的地址修改为 Bob；最后将报文发送给 Bob，即实现了一次报文的传输。对于 Bob 返回的报文，代理通过连接跟踪功能对地址域进行修改，最后发回给 Alice 完成通信过程。

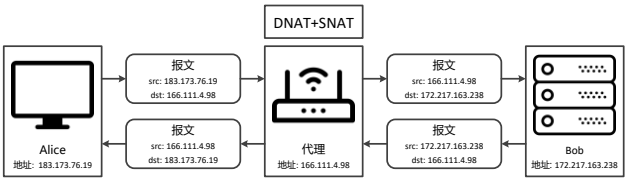
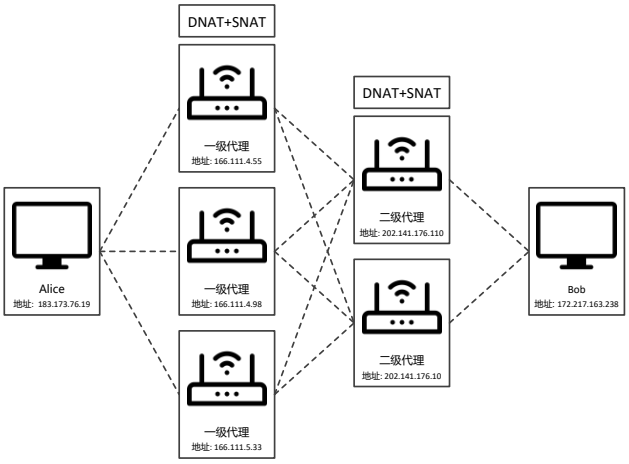


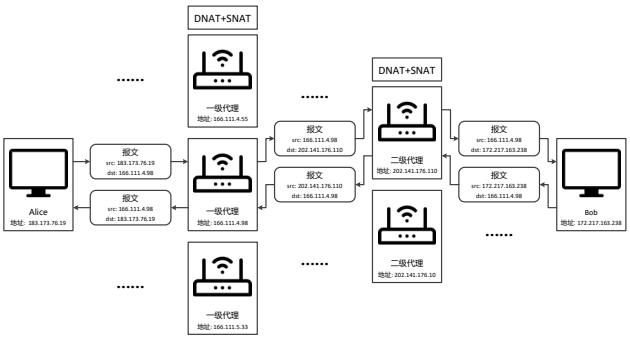
图 4 基于 NAT 的通信行为隐藏

由图 4 可以看出，在整个通信过程中，不存在源地址为 Alice，目的地址为 Bob（或相反）的报文；所有报文都是通过代理转换并传输的。对于 Alice 一侧的网络设备，代理隐藏了 Bob 的地址；而对于 Bob 一侧的网络设备，代理隐藏了 Alice 的地址。因此无论监听者处于通信过程的任何一侧，都无法探测到 Alice 与 Bob 间的通信行为。而且代理可以与 Alice，Bob 不处于同一个子网，使得代理的设置更加灵活，进一步增加监听者探测隐蔽通信行为的难度。

可以进一步扩展该通信行为隐藏系统的结构，如图 5（a）所示。在这个由多个节点组成的网络中，代理节点被分为多层；每层的代理节点之间没有连接，而任一个上一层的代理节点与任一个下一层的代理节点之间都可以建立连接。报文在网络中的传输方式如图 5（b）所示。Alice 在发送报文时，从一级代理中随机选择一个节点，将报文传输给该节点；此时报文的源地址为 Alice，目的地址为一级代理；收到报文的一级代理随机选择一个下一层节点，并对报文进行源/目的地址转换，最后发送报文；此时报文的源地址为一级代理，目的地址为二级代理；在示意图中二级代理就是出口节点，收到报文的出口节点同样对报文进行地址转换，使报文的源地址为二级代理，目的地址为 Bob；最终 Bob 接收该报文，完成一次发送过程。Bob 返回的报文同样也要经过两次网络地址转换，才能被 Alice 接收。



（a）网络结构示意图



（b）报文传输过程示意图

图 5 基于 NAT 的通信行为隐藏网络

由图可见，在一次通信过程中，Alice 的地址只出现在 Alice 与一级代理之间传输的报文中，而 Bob 的地址只出现在 Bob 与二级代理之间传输的报文中；无论监听者位于网络中的哪个位置，都无法同时探测到 Alice 与 Bob 的地址，也就无法发现 Alice 与 Bob 间存在通信链路，从而达到通信行为隐藏的目的。同时，每次通信 Alice 与 Bob 可以选择网络中不同的节点组成新的通信链路，进一步提高通信行为的隐蔽性。

基于 NAT 的通信行为隐藏网络与洋葱网络的比较如表 1 所示。

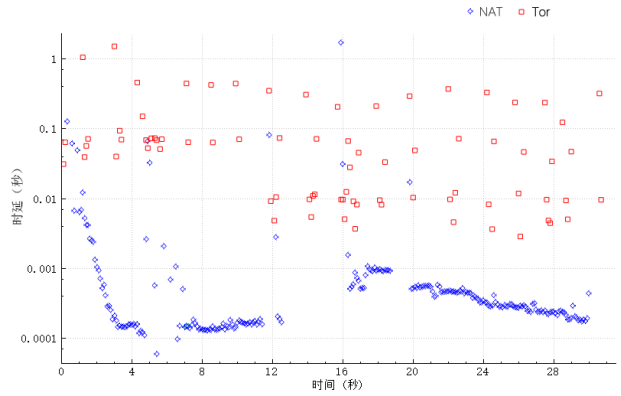
表 1 本文方法与洋葱网络的比较

	基于 NAT 的 通信行为隐藏	洋葱网络
内容安全	信息隐藏	加密
使用特殊协议	否	是
时延	低	一般
吞吐率	高	一般
代理节点	由隐蔽通信使用者 控制的可靠代理	由志愿者提供的 不可靠代理
网络灵活性	一般	好

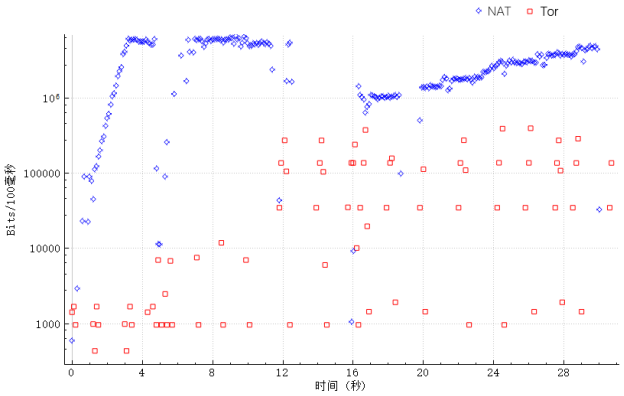
本文方法与洋葱网络相比，在内容安全上采用了不同的技术，这是由二者不同的目的决定的。洋葱网络的目的是保持用户的匿名性，防止监听者对用户进行溯源；而通信行为隐藏的目的在于使监听者无法发现用户正在进行隐蔽通信，也无法发现用户与目标之间的通信链路。同样由于这个原因，相对于洋葱网络，基于 NAT 的通信行为隐藏不能使用特殊的自定义协议，否则就等于暴露了用户正在进行隐蔽通信的事实。由于洋葱网络在通信过程中需要经历多层加密/解密，因此洋葱网络的时延更高，吞吐率则更低。

通过实验测试两种方法时延与吞吐率的性能，测试方法为从同一个地址通过两种不同方法传输同一个大小为 100MB 的文件。其中基于 NAT 的通信行为隐藏网络使用图 4 的单跳结构；由于其跳数比 Tor 网络少了两跳，因此在比较时延时，可以用实验结果的 2 倍来估计一个跳数与 Tor 网络相同的基于 NAT 的通信行为隐藏网络的性能。

两种方法时延的对比如图 6（a）所示：基于 NAT 的通信行为隐藏网络其平均时延大部分时间内保持在 0.1ms 至 10ms 之间，将其扩大为 2 倍则时延保持在 0.2ms 至 20ms 之间；而 Tor 网络其平均时延大部分时间内保持在 10ms 至 500ms 之间。两种方法吞吐率的对比如图 6（b）所示：基于 NAT 的通信行为隐藏网络的平均吞吐率约为 23.8Mbps；Tor 网络的平均吞吐率约为 0.194Mbps。



（a）时延



（b）吞吐率

图 6 两种方法的性能比较

本文方法仍处于起步阶段，相比洋葱网络也存在一些缺点。洋葱网络的多层加密算法可以保证网络中一部分节点不可靠时，用户仍然难以被溯源；但在本文中，我们假设代理节点都是由隐蔽通信方所控制的可靠节点。洋葱网络有一套成熟的链路选择与变更方法，使得网络的灵活性大大提升；这一方向是本文未来工作的重点。

4 结 论

行为隐藏是一种重要的信息隐藏技术。本文提出了基于 NAT 的通信行为隐藏，通过网络地址转换技术，利用代理节点，在通信过程中隐藏双方的地址，从而隐藏了通信链路的存在。本文初步构建了隐藏网络的系统结构，提高了方法的隐蔽性与可靠性。未来，我们一方面将继续完善网络与链路构建方法与协议，提升网络灵活性；另一方面将研究防御不可靠节点对网络进行攻击的方法，提高网络可靠性。

参考文献 （References）

[1] FRIDRICH J. Steganography in digital media: principles, algorithms, and applications [M]. Cambridge University Press, 2009.

[2] TANWAR R, BISLA M. Audio steganography [C]// International conference on reliability optimization and information technology, 2014.

[3] HUSSAIN M, WAHAB A W A, DIRIS Y I B, et al. Image steganography in spatial domain: A survey [J]. Signal Processing: Image Communication, 2018, 65: 46-66.

[4] SADEK M M, KHALIFA A S, MOSTAFA M G M. Video steganography: a comprehensive review [J]. Multimedia tools and applications, 2015, 74(17): 7063-7094.

[5] YANG Z L, GUO X Q, CHEN Z M, et al. RNN-stega: linguistic steganography based on recurrent neural networks [J]. IEEE Transactions on Information Forensics and Security, 2019, 14(5): 1280-1295.

[6] SHI S, QI Y, HUANG Y. An approach to text steganography based on search in internet [C]//2016 International Computer Symposium (ICS). IEEE, 2016: 227-232.

[7] ZHANG X. Behavior steganography in social network [M]// Advances in Intelligent Information Hiding and Multimedia Signal Processing. Springer, Cham, 2017: 21-23.

[8] YU R , QIU H , WEN Z , et al. A survey on social media anomaly detection [J]. ACM SIGKDD Explorations Newsletter, 2016, 18(1):1-14.

[9] ANAND K, KUMAR J, ANAND K. Anomaly detection in online social network: a survey [C]// International Conference on Inventive Communication & Computational Technologies. 2017.

[10] DINGLEDINE R, MATHEWSON N, SYVERSON P. Tor: the second-generation onion router [R]. Naval Research Lab Washington DC, 2004.

[11] TSIRTSIS G, SRISURESH P. Network address translation-Protocol translation (NAT-PT) [J]. RFC 2766, 2000.