基于 SDN 节点淆乱机制的接收方不可追踪的混合匿名通道

赵蕙，王良民
（江苏大学计算机科学与通信工程学院，江苏 镇江 212013）

摘 要：针对以 Tor 为代表的匿名通信系统在时延和下载时间方面的用户体验不够理想的问题，利用新一代软件定义网络带来的优势，面向接收方不可追踪，设计了新的匿名解决方案。提出使用 SDN 域内淆乱的方法，构建基于 Tor 和 SDN 的混合匿名通道，提供发送方和接收方匿名，拓展了 Tor 匿名通道的纵深，有效降低了攻击者对匿名路径的追踪率。实验结果表明，相比 Tor，所提方案在增加 15%时延的代价下，可提供相当于 2 条 Tor 电路的抗追踪能力。

关键词：匿名通信；软件定义网络；混合通道；淆乱节点
中图分类号：TP393
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2019155

Hybrid anonymous channel for recipient untraceability via SDN-based node obfuscation scheme

ZHAO Hui, WANG Liangmin
School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang 212013, China

Abstract: Leveraging the advantages of software defined networking (SDN), a new anonymous communication solution was de-signed for recipient untraceability. An obfuscation scheme in SDN domain was proposed to build a hybrid anonymous channel to solve the problem of large and highly variable delays and download time when using existing anonymous com-munication system such as Tor. The hybrid anonymous channel concatenated two sender anonymous channels in Tor and SDN to provide both sender and receiver anonymity. Adversaries can trace smaller portions of the path in hybrid channel. Experimental results show that the hybrid channel is as anonymous as two connected Tor circuits, with only a small larger latency (15%) compared with Tor.

Key words: anonymous communication, SDN, hybrid channel, obfuscated node

1 引言

开放的互联网中隐藏着大量的网络活动、用户身份、区域位置等敏感信息。斯诺登事件、Facebook 用户数据信息泄露事件等，让互联网用户意识到在使用网络的过程中，需要保护自己的隐私信息[1]，这种隐私保护可以通过保护信息的内容实现，也可以通过保护信息发布或接收者的身份实现。匿名通信技术通过隐藏通信实体的身份信息，使网络的攻击者不知道谁发送了数据和接收了数据，无法关联发送方和接收方之间的数据传输，吸引了广大研究者和网络用户的兴趣。广泛使用的匿名系统有 Tor[2]、Anonymizer[3]、I2P[4]、JAP[5]、Freenet[6]等。这些匿名系统中，Tor 的影响最大，诺威治大学的一份暗网交易分析报告显示，每年有超过 1 亿美元的网络交易是利用 Tor 等工具在暗网完成的。

然而，这些匿名技术在保护了匿名者隐私的同时，也隐藏了违法者的交易[7]。因此，一些针对匿名系统的监控方法也得到了广泛的研究，如被动和主动流量分析[8]、基于机器学习进行网站指纹分析[9]、

收稿日期：2019–03–04；修回日期：2019–06–06
基金项目：国家自然科学基金资助项目（No.U1736216, No.61702233）
Foundation Item: The National Natural Science Foundation of China (No.U1736216, No.61702233)

攻击 Tor 节点上运行的其他服务[10]等。这些监控技术大大降低了匿名性，虽然增加中继节点、延长匿名转发路由的措施可以降低匿名通道被发现的可能性，但是，由于通过中继节点进行层层加密的间接消息传输会导致较长的端到端路径，明显加剧匿名网络的访问速度，带来较大的时延和下载时间，如 Tor 匿名网络中，每增加一个中继节点，网络服务的时延会增加到原来的 1～2 倍，这对原本就服务体验不佳的匿名系统会带来灾难性的影响。

本文主要集中在匿名通道的出口节点，借力当前新兴的 SDN[11]的特性，将出口节点隐藏在一个 SDN 域内，虽然有限地增加了匿名通道长度，但可大大降低通道被捕获的概率。

本文工作主要体现在以下几点。

1) 在匿名通道出口节点所在区域，利用 SDN 在域内构建淆乱，降低匿名通道出口的发现概率和匿名路径的可追踪率。

2) SDN 域内淆乱路径和原有匿名通道结合的混合通道，同时提供发送方和接收方匿名，SDN 域内接收方的匿名性不依赖于（或者说独立于）发送方做出的选择。混合通道的匿名性随 SDN 域所选的参与淆乱结构的节点规模的增长而增强，而网络代价上远远低于在原有通道上增加一倍中继节点带来的时延。

2 相关工作

与本文相关的研究工作包括现有匿名系统的通道构建方法、SDN 域的基本知识，以及在 SDN 域内构建匿名通道的方法。

2.1 匿名的常见方法

匿名领域的开创性工作最初源于 1981 年 Chaum[12]提出的 Mix-net 方法，该方法是大部分匿名协议的基础。匿名通信系统可以根据时延性能、网络类型、路由方案、密码学机制等不同属性进行分类[13-14]。当前传统互联网中典型的匿名系统可以称为 Overlay 覆盖层匿名系统。这类系统建立在 TCP 传输层的基础之上，选择采用混淆、多层加密、多次转发的方法，达到间接隐藏分组头信息，并抵制流量分析的目的，其中比较有影响的典型系统有 Tor[2]、Anonymizer[3]、I2P[4]、JAP[5]、Freenet[6]等。较新的研究，如 Riffle[15]、Aqua[16]、Herd[17]等面向匿名文件分享和 IP 语音的应用，被认为是现有匿名系统的应用补充，并能更好地对抗流量分析。

随着未来互联网架构的研究发展，出现了 Network-layer 网络层匿名通信系统[18]，主要借助新的互联网架构中分段路由等关键技术，使路由器等网络基础设施参与建立匿名通信通道，并协助转发匿名流量。与覆盖层匿名系统间接隐藏分组头的匿名通信方法不同，这种匿名技术在网络层直接隐藏分组头，在理论上被认为有更快的传输速度和更高的可扩展性。目前，比较有代表性的有 Dovetail[19]、HORNET[20]、PHI[21]、TARANET[22]等。相比 Overlay 结构下的匿名系统 Tor 和 I2P 约 100 Mbit/s 的吞吐量，网络层匿名系统 HORNET 等可达到约 100 Gbit/s 的吞吐量[18]。但是不足之处在于，在安全性方面，轻量级加密技术使该类系统匿名性稍弱。此外，目前网络路由结构还不能全面支持网络层匿名系统，该系统走向具体应用还有相当长的时间。因此，目前实用的系统中主要还是使用 Tor 等传输速度较慢的 Overlay 结构的匿名技术构建的通道，覆盖网络匿名通信协议和网络层匿名通信协议在可拓展性、时延、吞吐量、安全和匿名性以及部署规模等方面的对比如表 1 所示。

2.2 针对 Tor 匿名的攻击方法

Tor 是目前使用最广泛的低时延匿名系统[23]，也是最具有代表性的第二代洋葱路由匿名系统，其使用洋葱路由方法对消息进行多层加密和多次转发，使消息看起来好像来自它的最后一个中继，而不是用户。其结构包含洋葱代理、洋葱节点和目录服务器，这些功能都集成在 Tor 的软件包中，用户可以下载公开源码的软件包，通过修改软件的配置文件实现 Tor 的具体功能。

从匿名性方面考虑，如果 Tor 用户随机选择路径长度来抵抗攻击者对路径中节点位置的学习，同时选择更多 Tor 节点参加消息中继，可以获得更高的系统匿名性。但是，中继节点的数量与系统的传

表 1 覆盖网络匿名通信协议和网络层匿名通信协议

典型工具	协议层位置	可拓展性	时延性	吞吐量	安全性	匿名性	部署规模
Mix-net	应用层	低	高	<100 kbit/s	强	抵制流量分析	区域部署
Tor/I2P	应用层	中	中	100 Mbit/s	中	按位不可关联	全球规模化部署
LAP/Dovetail	网络层	高	低	100 Gbit/s	弱	隐藏转发路径	尚未规模化部署

输速度成反比，考虑到提供交互服务的实时体验，当前默认的方法中，Tor 总是选择 3 个与自己和目的地无关的洋葱路由节点来构建一条匿名传输路径，并在概率上倾向于选择具有高带宽能力的节点以平衡负载、降低时延，并且不对流量做批处理、填充或整形[24]，这些以传输性能为出发点的设计都降低了 Tor 匿名性。

针对 Tor 匿名性的攻击，最具代表性、危害最大的是流量分析[25]。攻击者可以通过控制入口/出口节点对及统计相关性方法关联通信的实体、识别 Tor 用户身份，如图 1 所示。文献[26]利用 Cisco 的 NetFlow 监测工具检测服务器端和客户端信息的相关性，对实验室和现实网络中 Tor 用户的正确识别率分别达到 100%和 81.6%。文献[27]显示控制 9% 的 Tor 节点就可以关联 46.46%～60.58%的匿名路径，并且 Tor 网络出口节点到接收方的明文连接会使接收方完全暴露在网络中，尽管可以通过隐藏服务提高接收方匿名，但基于网站指纹研究的攻击者可以识别出与隐藏服务有关的电路和其在隐藏服务中的角色的情况下，发起网站指纹攻击，破解用户所访问的隐藏服务[28]。政府级别的强制监管可以在管辖权范围内与企业合作，要求 ISP（Internet service provider）在传输过程中复制用户的流量动态并通过安全通道将其转发；可以将监控设备架设在主干网等特权位置，保证更快的应对速度，再利用数据分析工具筛选流量，识别 Tor 用户。

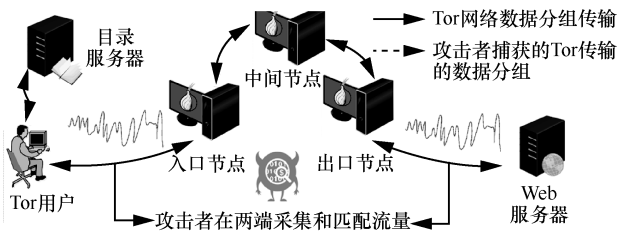


图 1　Tor 流量分析示意

这些针对 Tor 的流量分析，大大降低了 Tor 的匿名性。虽然可以通过增加中间节点数目（目前典型的 Tor 网络是 3 个中继节点）增强匿名性，但是这种方法一方面显著降低了匿名服务的效率，另一方面如果出口节点被攻击者控制，则增加节点来抵抗流量分析并没有显著的效果。因此，本文尝试通过 SDN 域内淆乱的方法，隐藏出口节点，提高匿名通道的匿名性。

2.3　SDN 匿名

SDN 是一种新兴网络架构，它采用中央集中控制机制，将控制逻辑从路由器和交换机中分离出来，以软件方式由 SDN 控制器集中规划，SDN 控制器可以俯瞰整个网络，可以对网络内的交换机快速编程，具有高效的控制管理和可编程特性。

不同文献的研究关注点在随机改变 IP 地址和端口[29]、需要修改主机[30, 31]、伸缩性部署[32]、特定应用和协议限制[33]、数据分组应用加密[34] 、多路径路由选择[35]等方面各有差别。其中比较典型的方法是利用 SDN 控制器对网络拓扑进行的全局视角和集中式可编程管理，由控制器分配域内地址空间，计算传输路由，向交换机安装流规则，通过 SDN 交换机节点重写或移除数据分组原始分组头，改变消息中真实的 IP 地址、MAC 地址、端口等信息，从而达到隐藏通信双方身份的目的。

为提高匿名通道的传输效率，一些研究者提出在 SDN 域内建立匿名通道的方法。文献[29]面向数据中心网络高带宽低时延的应用需要，提出 C/S 结构的 mimic 匿名通道，通道中的消息流经若干台由控制器指定的交换机节点，这些交换机节点相当于轻量级的匿名中继，它们不能进行加解密等计算密集型操作，只可以根据控制器下发的流表执行分组头信息的修改，从而获得匿名，控制器是 mimic 通道内所有路由的计算和管理者。文献[29]考虑了路由冲突避免机制、流量分析抵制机制，以及部署时如何与入侵检测、防火墙等系统共存。文献[30]提出可部分部署的网络层匿名系统 iTAP（in-network traffic analysis prevention），通过在 SDN 的边缘交换机节点重写分组头，随机改变 IP 地址，从而隐藏真实身份，使网络内实际地址和通信主机的数量都不能被识别。iTAP 最少需要 2 台 SDN 交换机设备就可以部署，系统可伸缩性强，匿名性随 SDN 设备的数量线性增长。

SDN 内的匿名传输通道与 Tor 相比，有更短的路由建立时间、更短的传输时延、更大的网络吞吐量，并且因为在底层网络传输，匿名路径长度的增加对时延的影响明显小于路径长度增加对 Tor 的影响。但是，控制器节点成为系统唯一脆弱点，存在单点失效问题，即控制器了解整个通道的节点及流量。

3　网络结构和威胁模型

考虑当前典型的混合结构的互联网模型，面向接收方不可追踪的匿名系统的发送方（Alice）和接收方（Bob）可以利用公开的匿名系统建立匿名通信渠道，

但是对其匿名性存在担忧，尤其是接收方很可能被攻击者发现，如 Tor 系统中，出口节点到接收方的明文连接会使接收方完全暴露在网络中，使用 Tor 隐藏服务建立的匿名通道也可能被指纹攻击破解[28]。

在混合网络模型中，Bob 可能位于一个与 Alice 不同的网络域，因此无法直接使用基于 SDN 构建的匿名通道，如 mimic[29]、PHEAR（packet header randomization）[34]等。因此，在模型中，Alice 利用公开的匿名系统，同时为保证处于可信 SDN 自治域内的 Bob 的通信身份不被泄露，设置淆乱节点 Bobo 作为接收方 Bob 的影子节点，代理往来 Bob 的消息，Bobo 同时连接 2 段不同的匿名通道，形成混合匿名通道。具体结构如图 2 所示。

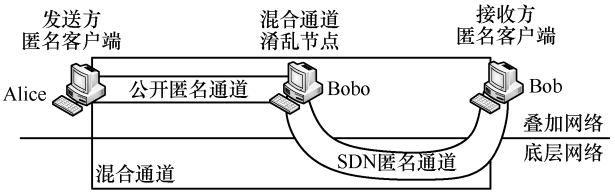


图 2 混合匿名通道示意

图 2 所示网络存在 3 类不同属性的域：1) 发送方所在的域；2) 接收方所在的域；3) 不同于发送方和接收方的第三方的多个网络域。网络的威胁模型主要来自第三方域。根据 Delve-yao 安全模型假设，在本文的威胁模型中，除发送方和接收方所在域外，都被匿名系统的分析者完全掌握，经过第三方域的流量、明文传输的信息内容都为分析者所知晓。同样，根据 Delve-yao 安全模型假设，攻击者不能破坏密码原语，一切的安全性和匿名性源于发送者和接收者对于所持有密钥的机密性。

本文使用的符号及其定义如表 2 所示。

表 2 本文使用的符号及其定义

符号	定义
Alice	消息发送方节点
Bob	消息接收方节点
Bobo	接收方节点选择的淆乱节点
SC	SDN 控制器
TDS	目标目录服务器
PK_X	节点 X 的公钥
SK_X	节点 X 的私钥
K_{XY}	节点 X 和 Y 共享的对称密钥
g^{XY}	Diffie-Hellman 握手
$\{M\}$	混合通道中使用对称加密传输的消息

4 基于 Tor 的跨域混合通道结构

Internet 由多个复杂异构管理域构成，本节提出的混合匿名通道构建方法，主要考虑跨域匿名通信，通过对出口节点的淆乱，进而提高整个通道的匿名性。基于一般性匿名系统中通道构建的基本规范，本节从淆乱节点选择、端到端通信建立、淆乱路径计算和淆乱节点更新这 4 个方面构建跨网络域的混合通道。

4.1 淆乱节点选择

淆乱节点（obfuscated node）是具有计算能力的主机节点。Bob 从所在的 SDN 域内选择淆乱节点作为自己的影子节点，记为 Bobo，参与通道的构建。淆乱节点 Bobo 需要同时满足以下 3 个方面的属性。

1) 随机性。Bobo 的选择是随机性产生，不能和 Bob 具有明显关联。

2) 多路径关联。Bobo 可以通过多条路径到达 Bob，不能仅有一条或者太少的容易被跟踪的路径。

3) 高效率路由。Bobo 和 Bob 之间的数据传输可以满足匿名访问的数据传输需求。

需要获得接收方匿名服务的 Bob 向 SC 请求匿名服务注册后，得到 SC 分配的虚拟地址。Bob 在淆乱节点集合中随机选出 λ 个节点（$\lambda \geq 1$）作为自己的淆乱节点 Bobo，向 SC 请求建立与 Bobo 之间的匿名通道。SC 存储消息的源和目的地址，根据 Bob 请求中速度优先还是匿名优先等服务质量（QoS, quality of service）信息，利用对域内网络拓扑的掌握，计算匿名传递消息的路由通道，完成真实地址和虚拟地址之间的映射。这是一条由 SDN 交换机组成的底层网络匿名路径，入口交换机地址、转发交换机地址都是由 SDN 控制器计算分配的域内虚拟地址。在这条生成的匿名路径中，只有入口交换机知道发送方的真实地址，只有出口交换机知道接收方的真实地址，SDN 控制器将沿着匿名路径，给交换机安装重写分组头和转发规则的流表，交换机将收到的数据分组和流表匹配，执行分组头重写和向前转发。因此，路径中的每一台交换机只会收到将数据分组转发到下一跳的必要指令，像洋葱路由一样，每台交换机只知道通信链路中的上一跳和下一跳，获得入口交换机和出口交换机的不可关联性。Bob 通过这条匿名路径建立向 Bobo 的连接，请求 Bobo

作为自己的淆乱节点，得到 Bobo 的响应后。Bob 向 SC 请求建立与 TDS 之间的匿名通道，通过该通道将自己的公钥和 Bobo 的连接信息发布到 TDS，这样，任何一个发送方要给 Bob 发送信息时，查询 TDS 得到的是 Bobo 的地址信息，从而达到了以淆乱节点保护真实接收方的目的。图 3 描述了协议的执行过程。

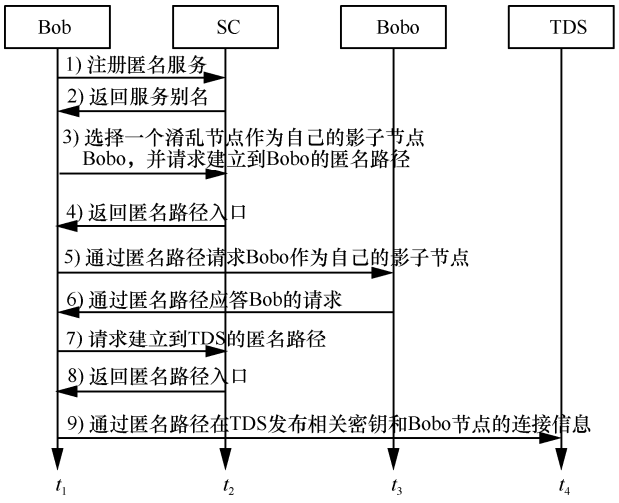


图 3　混合通道协议选择和建立淆乱节点

协议中第 3)步和第 4)步由算法 1 给出描述。

算法 1　淆乱节点的选择和匿名路径生成

输入　混合通道淆乱节点集合 $S_{\text{Bobo}}\{\}$，参数 λ 表示被选出的淆乱节点个数，消息的源和目的地址

输出　淆乱节点 $\text{Bobo}_1,\text{Bobo}_2,\cdots,\text{Bobo}_\lambda$，SDN 匿名通道路由和虚拟地址。

/*以下步骤由 Bob 完成*/

1) 初始化定时器 Φ(time)

2)在 $S_{\text{Bobo}}\{\}$集合中随机选择 λ 个淆乱节点

3) if 定时器 Φ(time)溢出 then

4)　更新 $\text{Bobo}_1,\text{Bobo}_2,\cdots,\text{Bobo}_\lambda$

/*以下步骤由 SDN 控制器 SC 完成*/

5) for 所有来自用户接口的请求 R do

6)　if R 是申请匿名路径的请求 then

7)　　if 该请求来自认证用户 then

8)　　{ 存储源/目的地 IP 地址

9)　　映射真实和虚拟 IP 地址

10)　　计算路由路径

11)　　return 虚拟 IP 地址}

12)　　else if R 是申请匿名服务注册的请求 then

13)　　{ 为该请求分配和存储服务别名

14)　　return 服务别名 }

15)　else return 错误信息

4.2　混合通道端到端通信建立

需要与 Bob 通信的发送方客户端 Alice，使用公开匿名协议，建立一条到达 TDS 的匿名电路。以 Tor 为例，Alice 从 Tor 的洋葱目录中下载共识文件，获取洋葱路由信息，创建一个到达 TDS 的洋葱。根据带外获得的 Bob 的服务别名，Alice 向 TDS 查询并获得 Bob 节点公钥和其淆乱节点 Bobo 的地址。

通过 Bobo 中继 Alice 和 Bob 之间的信息，需要建立 Alice 和 Bob 之间的会话密钥，该会话密钥的建立采用 Diffie-Hellman 握手机制，具体算法如算法 2 所示，描述淆乱节点对接 Alice 和 Bob 之间会话密钥建立机制。

算法 2　Bob 与 Alice 协商会话密钥

输入　Bob 和 Alice 的私钥 SK_B 和 SK_A

输出　K_{AB} 和 $H(K_{\text{AB}})$

/*以下步骤由发送方客户端 Alice 完成*/

1) Alice 通过 Bobo 节点中继，向 Bob 发送访问请求和握手信息 g^{SK_A}，消息由 PK_B 加密

2)当 Alice 从 Bobo 获得来自 Bob 的响应后

3) 生成对称密钥 K_{AB} 并检查 $H(K_{\text{AB}})$

/*以下步骤由接收方客户端 Bob 完成*/

4) 当 Bob 从 Bobo 获得 Alice 的 g^{SK_A} 后

5)　Bob 生成 K_{AB}，通过 Bobo 中继，向 Alice 发送 g^{SK_B} 和 $H(K_{\text{AB}})$

Alice 获得 Bob 的连接信息后，通过公开匿名协议向 Bobo 建立一条匿名电路，以 Tor 为例，Alice 创建一个到达 Bobo 的洋葱，用这个洋葱打包自己对 Bob 的访问请求以及 DH 握手的前半部分 g^{SK_A}，Bobo 收到 Alice 的消息后，通过 Bob 利用算法 1 向自己建立的匿名路径，把消息发送给 Bob，Bob 收到消息后如果接收 Alice 的访问请求，则生成会话密钥 K_{AB}，并将会话密钥的散列 $H(K_{\text{AB}})$以及 DH 握手的另一半 g^{SK_B}，通过 Bobo 发送给 Alice。Alice 接收后，生成会话密钥和该密钥的散列，与来自 Bobo 消息中的密钥散列值比较确认，完成混合通道端到端通信建立。上述过程的具体描述如图 4 所示。其中，Bobo 连接 2 条匿名通道形成混合通道，Alice 与 Bob 之间的加密消息$\{M\}_{K_{\text{AB}}}$通过淆乱节点 Bobo 中继转发。Alice 与 Bobo 之间的连接、Bob 和 Bobo 之间的连接都是匿名的，Bobo 既不知道消息发送方 Alice 的真实地址，也不知道消息接收方 Bob 的真实地址。

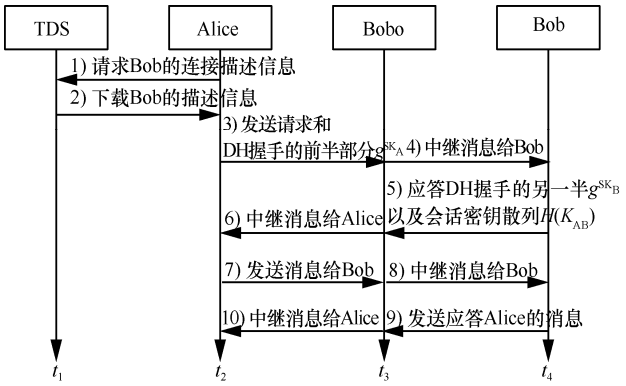


图 4　混合通道端到端通信建立

4.3　淆乱路径计算

混合通道的 SDN 域内采用的淆乱机制包括淆乱路径的计算，由 SDN 控制器计算生成多条用于传输消息的 SDN 交换机节点的有序序列，如算法 3 所示。相比最短路径等固定路径的方法，利用这种机制可以防止攻击者捕获 Bob 与 Bobo 之间的整个通信流。

算法 3　淆乱多路径生成

输入　消息的源和目的地址，参数 η 用于指定期望的最小跳数，参数 k 用于指定生成路径数

输出　路径集合 path{$path_1$,$path_2$, …,$path_k$}，其中每一条路径 $path_i$={V_s,V_1,V_2,…,V_η,V_d}

/*以下流程由 SDN 控制器 SC 完成*/

1) for 每条消息中的一对 V_s 和 V_d do
2)　调用 Yen' algorithm 获得 p 条最短路径
3)　升序排列 p 条路径
4)　for 每一条路径 do
5)　if 路径长度<期望的最小路径数 η
6)　丢弃该路径
7)　else if 路径未满 k 条
8)　该路径添加至路径集合 path{}
9) return path{}

算法 1 中第 11)行为 SDN 控制器对域内路由计算，是在使用链路层发现协议 LLDP 获得域内网络拓扑和经典最短路径算法（Yen's algorithm）的基础上，使用随机化阈值，结合考虑网络中测得的带宽等网络运行状态，计算出前 p 条最优路径。计算出的这 p 条路由作为一组规则安装到路径中的交换机上，使用一张有序表保存，每个规则表示一条路由，最优的路由排在表的顶端，当前时刻只有一条规则是活跃的。用超时标记来表示现存这组规则的生存期，当位于列表顶部的路由超时过期时，交换机将使用列表中的下一条路由，直到这组路由全部超时。若一条路由超时，交换机发送一条消息通知控制器；若所有条目都超时，控制器将推送新的规则组。新组中的路由的超时时间和路由在表中的顺序可能不同，以此增强混淆。当可用路由变化不大时，则不需要由控制器不断地重发规则，一组路由安装后，可使用随机逻辑或定时时间随机变化的计时器，轮询可用路由规则，保证域内网络的动态性。

4.4　淆乱节点更新

混合通道的出口淆乱机制依赖于淆乱节点的存在，有必要根据接收方 Bob 的需要，随机选择 λ ($\lambda \geqslant 1$) 个淆乱节点，并在使用一段时间后更换淆乱节点，从而实现和维护淆乱机制的稳健性，也可以更大程度地对 SDN 控制器隐藏其直接的联系，从而降低控制器单点失效可能带来的影响。淆乱节点的更新可以通过重新启动算法 1～算法 3 实现，也可以在算法 1 的基础上，由 Bob 直接选择，通过秘密通道告诉 Alice，从而实现对 SDN 控制器的匿名性。

5　跨域混合匿名通道的安全分析

经过算法 1～算法 3，Alice 和 Bob 之间构建了一条秘密通道 CH，其加密的密钥由算法 2 的会话密钥建立方法获得。假设构建完成的混合通道是一个封闭的系统，包含 2 个部分，如图 5 所示。一部分是 Alice 到 Bobo 的传统意义上的，由一组 Tor 洋葱节点组成的匿名通道 CH_{sub_1}，另一部分是从 Bob 到 Bobo 的 SDN 域内交换机网络构成的多路径匿名通道 CH_{sub_2}，该多路径是在算法 3 的支持下获得的。

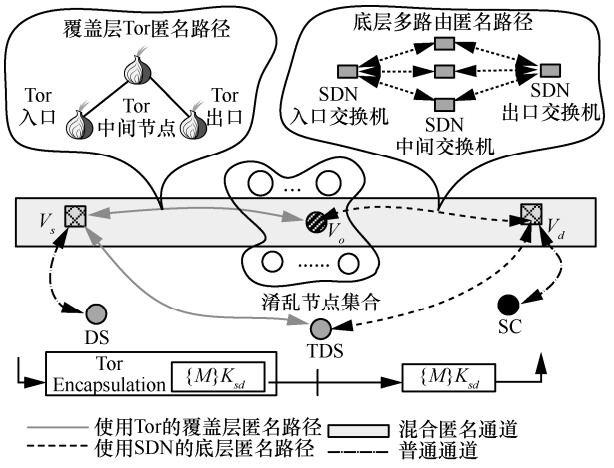


图 5　混合通道结构图

通道 CH_{sub_1} 在传输层建模，包括消息发送方 v_s

和一个规模为 n 的洋葱节点集合，将 $\mathrm{CH}_{\mathrm{sub}_1}$ 通道中一条消息的匿名路径记为 $R=\{R_1,\cdots,R_i,\cdots,R_r\}$，$R_i$ 表示路径中的第 i 跳洋葱路由，r 表示当前消息的匿名路径长度。

通道 $\mathrm{CH}_{\mathrm{sub}_2}$ 在网络层建模，包含淆乱节点 v_o、消息接收方 v_d 和规模为 m 的 SDN 交换机集合，将 $\mathrm{CH}_{\mathrm{sub}_2}$ 通道中一条消息的匿名路径记为 $S=\{S_1,\cdots,S_i,\cdots,S_l\}$，$S_i$ 表示路径中的第 i 跳 SDN 交换机，l 表示路径的长度。

淆乱节点 v_o 连接 2 条匿名通道 $\mathrm{CH}_{\mathrm{sub}_1}$ 和 $\mathrm{CH}_{\mathrm{sub}_2}$。

设 $B=B_{\mathrm{sub}_1}\cup B_{\mathrm{sub}_2}$ 是攻击者能够掌握的混合通道的最大节点数，其中，B_{sub_1} 是攻击者在 $\mathrm{CH}_{\mathrm{sub}_1}$ 中控制的节点数，B_{sub_2} 是攻击者在 $\mathrm{CH}_{\mathrm{sub}_2}$ 中控制的节点数，c 表示所建立匿名路径中选中攻击者控制的节点个数，$C=\{C_1,\cdots,C_i,\cdots,C_c\}$，$C_i$ 表示路径中由攻击者控制的第 i 个节点。

本节从被攻陷概率和可追踪率 2 个方面，分析混合匿名通道的安全性。

5.1　混合通道被攻陷概率分析

混合通道的安全目标是在利用 Tor 实现发送方匿名的基础上，采用 SDN 内部淆乱方法，使对手无法区分可能的通信事件。Alice 可能正在通过混合通道与 Bob 通信，Alice 可能已连接混合通道但未与其他用户交换消息，Alice 可能正与 Bobo 交换信息。对于上述情况，攻击者无法区分。混合通道提供的不可区分性，使攻击者对混合通道进行的观察只能在一定的边界内（例如 ε）改善对通道内怀疑事件的确定性，对任何事件仅获得大致相等的概率。

假设匿名网络中的节点是被选取的概率相等的随机样本。在有攻击者掌握节点的情况下，用户可能会选中攻击者节点参与匿名路径建立，对一条匿名路径来说，在规模为 N 的网络中，攻击者控制了网络中的 B 个节点，在这种情况下选择 r 个节点构成一条传输路径时，恰好选中 c 个攻击者控制的节点的概率如式(1)所示。以 n=100，B=10，r=3 为例计算，$p(3,1)$=0.247 7，$p(3,2)$= 0.025 0。

$$p(r,c)=\frac{\prod_{i=0}^{c-1}(B-i)\binom{N-B}{r-c}}{\binom{N}{R}c!} \tag{1}$$

更具体地，根据 Tor 的路由选择，洋葱路由被分为 4 类[36]：入口节点、出口节点、既可做入口节点也可做出口节点、既不能做入口节点也不能做出口节点。用 G 表示被控制的入口节点个数，用 E 表示被控制的出口节点个数，如果 Tor 用户建立电路时，入口节点和出口节点恰好都选中攻击者控制的节点，那么攻击者可以分析两端数据的统计信息，则称这条 Tor 通道被攻陷。出现这种情况的概率如式(2)所示。以 N=100，G=5，E=5，r=3 为例计算，$P(3,5,5)$=0.013 9。

$$p(r,G,E)=\frac{GE\binom{N-G-E}{r-2}}{\binom{N}{r}} \tag{2}$$

根据 Tor 的路由选择算法[24]，Tor 对节点的选择分为选取入口节点和选取非入口节点 2 个部分。入口节点的选择会倾向于带宽最高以及运行时间最长的节点，考虑到 Tor 网络中的所有节点在某种程度上都应该得到使用，非入口节点则未必是带宽和运行时长最优的节点，所以真实 Tor 网络中节点被选取的概率并不相同，以仅考虑带宽权重为例，Tor 网络中所有节点的带宽标记为$\{b_1,\cdots,b_i,\cdots,b_N\}$，具有带宽 b_i 的 Tor 节点权重如式(3)所示。

$$w_i=\frac{b_i}{\sum_{i=1}^{N}b_i} \tag{3}$$

如果以 Tor 通道被攻陷的概率 p 为参照基准，理论上使用 2 条 Tor 电路叠加的匿名通道被攻陷概率为 p^2。对于混合通道，淆乱节点连接了 2 条匿名通道，使出口节点隐藏 SDN 域内，假设 SDN 匿名通道内有 m 个节点，那么匿名通道将获得 $\frac{1}{m}$ 的不可区分性，从而使整个匿名混合通道的被攻陷概率降低为 $\frac{p^2}{m}$，3 种匿名通道被攻陷的概率如图 6 所示。

针对匿名 $\mathrm{CH}_{\mathrm{sub}_1}$ 通道路径 $R=\{R_1,\cdots,R_i,\cdots,R_r\}$ 中的节点被攻击者控制的不同情境，对比单条 Tor 电路和混合通道的匿名属性，如表 3 所示。1) 当 $R_1\in C$，即匿名系统的入口节点由攻击者控制的情况下，无论哪种情况都无法保护发送方匿名。2) 当 $R_r\in C$，即匿名系统的出口节点由攻击者控制的情况下，Tor 无法保护接收方匿名。此外，除非消息经 Tor 带外加密，否则消息的内容也会泄露给攻击者。混合通道因为真正的接收方隐藏在淆乱节点背后，所以获得接收方匿名。3) 当 $R_1\in C$ 并且 $R_r\in C$，Tor 通道被彻底攻陷，混合通道获得接收方匿名。

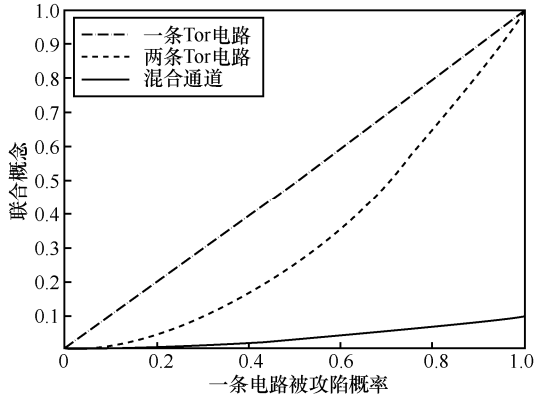


图 6 电路被攻陷概率

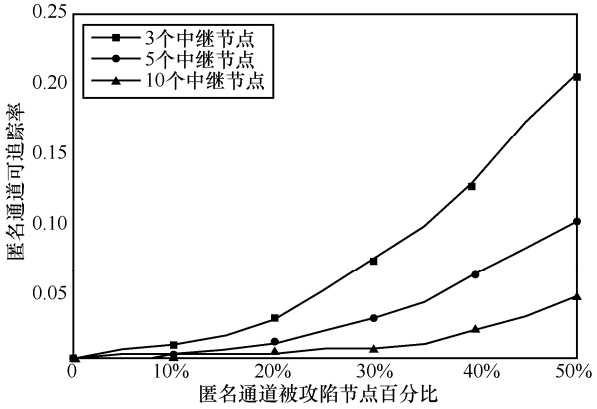


图 7 不同被攻陷节点百分比下可追踪率

表 3 不同攻击情境下 Tor 和混合通道匿名属性比较

匿名属性	$R_1 \in C$		$R_r \in C$		$R_1 \in C$ 且 $R_r \in C$	
	Tor	混合通道	Tor	混合通道	Tor	混合通道
发送方身份保护	×	×	✓	✓	×	×
发送方内容保护	✓	✓	✓	✓	×	✓
接收方身份保护	✓	✓	×	✓	×	✓
接收方内容保护	✓	✓	×	✓	×	✓
通信关联性保护	✓	✓	✓	✓	×	✓

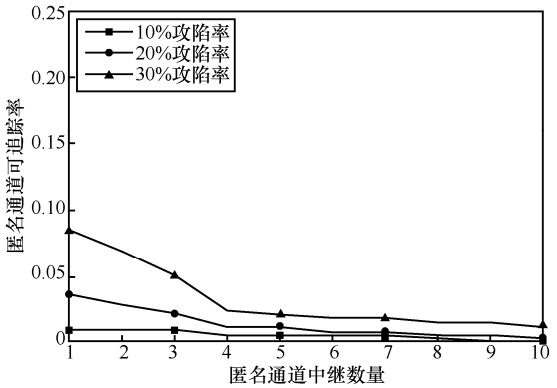


图 8 不同中继节点数量下可追踪率

5.2 混合通道可追踪率分析

文献[37]提出用式(4)刻画系统的可追踪率，文献[38]利用几何分布刻画了其中的($C_{\text{seg},i}$)，并对式(4)进行了计算，计算结果主要受系统的中继节点数量和攻击者攻陷节点百分比的影响。本文所提混合通道出口淆乱的方法将使系统可追踪率降低。

$$P_{\text{trace}} = \frac{1}{\eta^2}\sum_{i=1}^{C_{\text{seg}}}(C_{\text{seg},i})^2 \tag{4}$$

图 7 显示了当系统中被攻陷节点百分比从 0 增加到 50%，路径中节点数分别为 3、5、10 时的可追踪率变化。由图 7 可知，随着被攻陷节点的百分比增加，可追踪率升高；在相同百分比情况下，路径中节点数量越多，可追踪率越低，这是因为随着节点数量的增加，式(4)分母 η^2 的增大相对较快。图 8 显示了当系统中中继节点数量从 1 增加到 10，被攻陷节点百分比分别为 10%、20%、30%时的可追踪率变化。由图 8 可知，路径中节点数越多，可追踪率越低，相同节点数的条件下，被攻陷节点百分比越低，可追踪率越低。

式(4)中 η 表示进行通信的 2 个节点（v_s 和 v_d）之间的跳数，例如当 v_s 和 v_d 建立的路径为 $v_s \to v_2 \to v_3 \to v_4 \to v_d$ 时，则 η =4。当一个节点被攻陷，则这个节点与下一跳的路径段将会被攻击者追踪，即如果 x 个连续节点被攻陷，那么可能有 x 跳的路由段被追踪。C_{seg} 表示被攻陷的路径段的数量，$C_{\text{seg},i}$ 表示在被攻陷的第 i 段路径中包含的跳数。例如在路径 $v_s \to v_2 \to v_3 \to v_4 \to v_d$ 中，如果 v_s、v_2、v_4 这 3 个节点被攻陷，那么攻击者将可以追踪到路径段 $v_s \to v_2 \to v_3$，以及路径段 $v_4 \to v_d$，此时，C_{seg}=2，$C_{\text{seg},1}$=2，$C_{\text{seg},2}$=1，$P_{\text{trace}}=\frac{1}{4^2}\times(2^2+1^2)=\frac{5}{16}$，在所有节点都被攻陷的情况下，$C_{\text{seg}}$=1，$C_{\text{seg},1}$=4，$P_{\text{trace}}=\frac{1}{4^2}\times 4^2=1$。

可追踪率的结果除了与中继节点数量和被攻陷的节点数量有关，还有一个关键因素是攻击者获得的路径是否连续。如果攻击者攻陷的节点比较多，但因为被攻陷的节点不连续，也将难以关联掌握的路径段进行持续的路径追踪。如果攻击者攻陷 3 个节点 v_s、v_2、v_4，泄露给攻击者的 2 段路径分别是 $v_s \to v_2 \to v_3$ 和 $v_4 \to v_d$，$P_{\text{trace}}=\frac{5}{16}$。尽管 v_3 前后 2 个路径段都已经被攻陷，但是只要 v_3 节点安全，攻击者就无法判断获得的这 2 个路径段是否属于

同一条路径。如果攻击者攻陷节点 v_2、v_3、v_4，同样是 3 个节点，泄露给攻击者的路径为 $v_2 \to v_3 \to v_4 \to v_d$，$P_{\text{trace}}=\dfrac{9}{16}$。

根据混合通道的定义，消息在混合通道中传输的路径为 $R_1 \to R_2 \to \cdots \to R_r \to v_o \to S_1 \to S_2 \to \cdots \to S_l$。因此，如果混合匿名通道的淆乱节点 v_o 是安全的，而前后 2 段匿名路径均泄露给攻击者，混合通道的可追踪率 $P_{\text{trace}}=\dfrac{1}{(r+l)^2}(r^2+l^2)$，在 $r=l$ 时有最小值 50%。

6　混合通道效率与仿真

本文从 SDN 域内时延和与 Tor 隐藏服务的比较 2 个方面开展对混合通道的效率评估。

6.1　混合通道效率分析

混合通道构建的过程与 Tor 隐藏服务的实现流程部分相似，不同的是，混合通道连接的是 2 段不同匿名协议下的发送方匿名通道，并用淆乱节点代替隐藏服务中引入节点和汇聚节点的功能，对比文献[36, 39]中对 Tor 隐藏服务流程的描述。图 9 给出混合通道（左侧）与 Tor 隐藏服务（右侧）关键流程比较，其中混合通道在 a_1、c_1、e_1、f_1 阶段花费的时间低于对应的 Tor 隐藏服务在 a_2、c_2、e_2、f_2 阶段花费的时间。

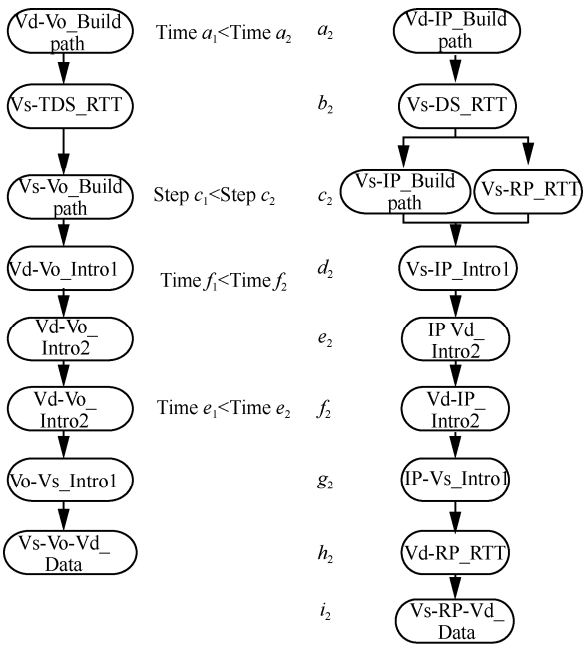


图 9　混合匿名通道和 Tor 隐藏服务流程关键步骤比较

表 4 针对图 9 中的步骤给出解释和说明。

表 4　　图 9 各步骤说明

步骤	说明
a_1	Bob 向控制器申请到 Bobo 的 SDN 匿名通道
a_2	Bob 建立到引入点的 Tor 电路
b_1	Alice 建立到 TDS 的 Tor 电路，查询下载 Bob 淆乱节点连接信息
b_2	Alice 建立到隐藏目录服务器的 Tor 电路，查询下载引入点信息
c_1	Alice 建立到 Bobo 的 Tor 电路
c_2	Alice 建立到 Bobo 的 Tor 电路；同时 Alice 向汇聚节点建立 Tor 电路，请求该节点做自己的汇聚节点并得到应答
d_1	Alice 通过 Tor 电路连接到 Bobo，发送 DH 握手的前半部分和向 Bob 的访问请求，由 Bobo 中继消息给 Bob
d_2	Alice 通过 Tor 电路连接到引入点，发送 DH 握手的前半部分，汇聚点信息和向 Bob 的访问请求，由引入节点中继消息给 Bob
e_1	Bobo 通过 SDN 匿名通道中继 d1 步骤中来自 Alice 的消息给 Bob
e_2	引入点通过 Tor 电路中继 d_2 步骤中来自 Alice 的消息给 Bob
f_1	Bob 把应答和 DH 握手的另一半，通过 SDN 匿名通道发送给 Bobo，由 Bobo 中继消息给 Alice
f_2	Bob 把应答通过 Tor 电路发送给引入点，由引入点中继给 Alice
g_1	Bobo 通过 Tor 电路中继 f_1 步骤中来自 Bob 的消息给 Alice，至此，Alice 和 Bob 完成握手
g_2	引入点通过 Tor 电路向 Alice 中继 Bob 的应答消息，Alice 收到后撤销与引入点之间的 Tor 电路
h_1	Alice 和 Bob 通过 Bobo 进行数据通信
h_2	Bob 向汇聚点建立 Tor 电路，发送 DH 握手的另一半，将汇聚点中继给 Alice，Alice 和 Bob 完成握手
i_2	Alice 和 Bob 通过汇聚点进行数据通信

图 9 和表 4 比较本文提出的混合匿名通道协议和 Tor 隐藏服务协议的流程，分析影响时延和计算开销的关键路径，体现出以下优点。

1) 混合通道协议使用淆乱节点代替隐藏服务中汇聚点的功能，从而减少了 Alice 和 Bob 分别向汇聚点建立匿名路径带来的时延和开销，对应图 9 中的 c_1、c_2 步骤。

2) SDN 域内的匿名路径拥有较短的端到端距离，交换机只做转发动作，在数据传输阶段体现出显著的速度优势，对应图 9 中 a_1、e_1、f_1 步骤。

3) 混合协议增加了一层加密封装操作，开销体现在 Alice（加密）和 Bob（解密）客户端，但 Bob 和 Bobo 之间的匿名路径计算和建立由计算能力强的控制器完成，减小了客户端主机的开销。

6.2　仿真结果

根据对混合通道效率理想的估计，如果以 Tor 电路端到端传输时延 t 为基准，使用 2 条 Tor 电路

叠加的传输时延将线性增长为 2t，混合匿名通道传输时延增长为 t+t'，SDN 域内匿名通道的建立过程主要取决于控制器性能，通信过程主要取决于底层交换机设备转发速度，因此 t'应远小于 t，即 t'<<t 。

第一部分的实验设置，通过采集将一个数据分组从交换机发送到控制器，在控制器上做出决策并将数据分组返回到交换机的时间，获取混合通道在匿名服务和匿名路径请求、淆乱节点选择、淆乱路径计算阶段、Bob 与 Bobo 建立起匿名会话等的控制器计算时延。仿真实验采用集成在 Ubuntu 14.04 环境下的 Mininet version 2.2.1 模拟器，连接 Ryu 控制器组成 SDN 仿真网络，所有虚拟软件 SDN 交换机均由 Open vSwitch 构建，Iperf 作为性能测试工具获取消息的时间相关度量。混合通道的原型包括基于客户端的连接组件和基于 SDN 控制器的匿名应用组件，图 10 描绘了在 Ryu 控制器基础上，使用 Python 脚本为匿名通道设计的应用组件。

第二部分的实验设置，通过测量 Tor 隐藏服务的时延和本文方案进行比较。一方面，为了采集 Tor 建立三跳电路和建立隐藏服务时各个阶段的时延，实验部署了由 30 个洋葱节点组成的局域网私有 Tor 环境，包含 2 台目录服务器和 2 台隐藏目录服务器，可提供 Tor 服务和 Tor 隐藏服务。Tor 版本 Tor-0.2.9.15，配置一台 HTTP 服务器作为提供文件下载服务的匿名接收方，分配 100 MB/s 带宽以尽量避免服务器容量成为实验下载的瓶颈。另一方面，为了获得互联网隐藏服务时延数据，配置代理网络后，将该 HTTP 服务器发布为隐藏服务，域名以及端口为 vh3g64sdpbmj6uls.onion:9046，客户端分别使用普通域名和隐藏服务域名 2 种访问方式，采集 500 KB 大小文件的下载时间。

混合通道的下载时间使用两部分实验的叠加结果，尽管没有部署真实的 SDN 环境，但是单 SDN 域内的地理位置跨度较小，匿名路由产生的时延主要来自控制器算法开销，仿真结果有参考价值。实验的结果分别如图 11 和图 12 所示。

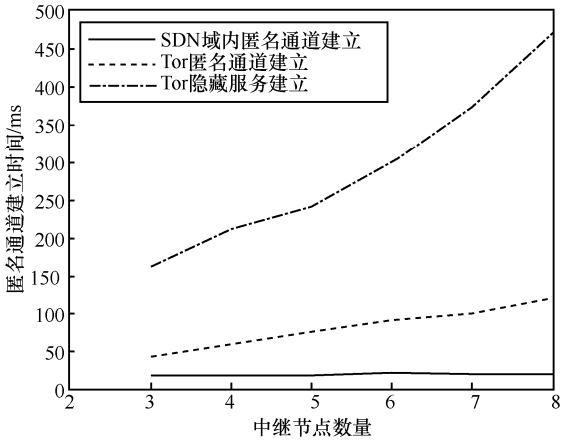


图 11 3 种匿名通道的路由建立时延比较

图 11 描绘了匿名电路建立阶段时延随中继节点个数变化产生的结果，数据来自 mininet 仿真和局域网 Tor。由于混合匿名通道内路径建立由控制器完成，因此在匿名路径建立阶段，时延性优于 Tor 和 Tor 隐藏服务。由于 Tor 的匿名通道建立需要与每一跳洋葱节点协商密钥，因此通道建立时间随着中继数量的增加有明显增加，但在混合通道内增加

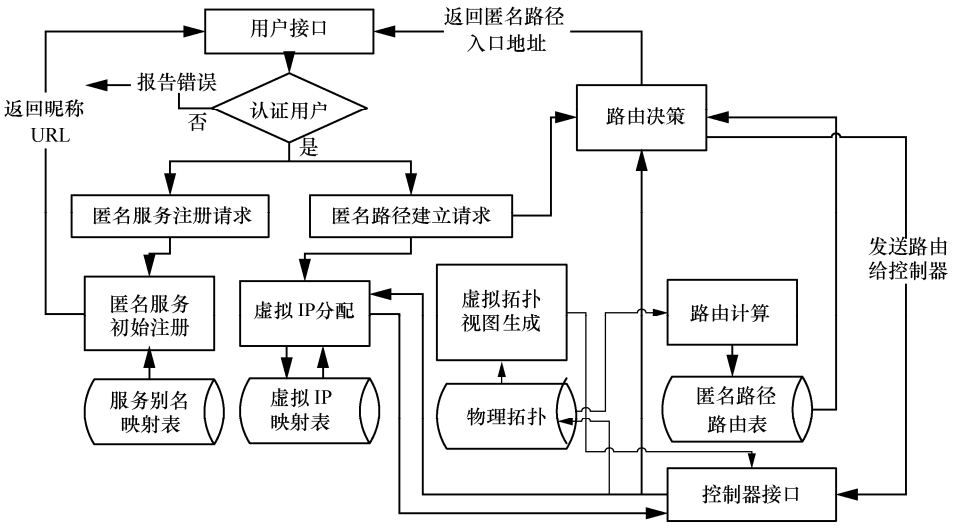


图 10 基于 SDN 控制器的匿名应用流程图

较为缓和，因为尽管发送方连接到淆乱节点的路径建立时间也随之增加，但 SDN 域内匿名通道建立的时延不会受到影响。

由于 SND 匿名通道具有更少的加密操作和更短的传输路径，相比 Tor 隐藏服务，混合通道实现了更低的时延，结合仿真结果，下载时间相较普通 Tor 电路仅增加 15%～20%，如图 12 所示。

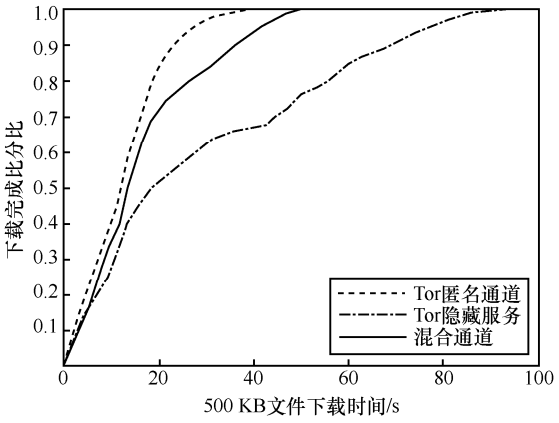


图 12　3 种匿名通道的文件下载时延比较

7　结束语

本文介绍了一种混合匿名通道机制，降低攻击者对匿名网络的追踪率，适用于对接收方匿名要求较高的匿名应用。混合通道匿名机制的有效性在于组合了传统互联网络匿名通道与 SDN 匿名通道，SDN 域内淆乱机制的应用实现了通道出口节点的隐藏。使用部署广、用户多的公开匿名系统作为信息匿名传输的一环，满足了匿名应用对地域广泛性的需要；SDN 自治域内匿名通道传输时延低、带宽高，网络状态的动态淆乱有利于抵制攻击者攻击。与 Tor 相比，混合通道获得了更高的匿名度和更低的可追踪率，增加的时延非常有限。有迹象表明，更多的国家可能寻求建立国家云和 Web 服务提供商，以及独立的互联网线路，这些线路会尽可能少地跨越其他国家或大洲，因此，SDN 自治域内匿名路由和出口淆乱方法有其应用价值。下一步的工作将增加跨 SDN 子网和 SDN 域的设计，随着未来 SDN 域的数量和域间距离的增加，性能优势会更加明显，混合匿名通道可以在更广的范围内，提供低时延、带宽密集应用的匿名传输。

参考文献：

[1] ALSABAH M, GOLDBERG I. Performance and security improvements for Tor: a survey [J]. ACM Computing Surveys, 2016, 49(2): 1-36.

[2] DINGLEDINE R, MATHEWSON N, SYVERSON P. Tor: the second-generation onion router [C]// The 13th USENIX Security Symposium. USENIX, 2004: 1-18.

[3] BOYAN J. The anonymizer: protecting user privacy on the Web [J]. Computer-Mediated Communication, 1997, 4(9): 1-6.

[4] HERRMANN M, GROTHOFF C. Privacy-implications of performance-based peer selection by onion-routers: a real-world case study using I2P[C]//International Symposium on Privacy Enhancing Technologies Symposium. Springer, 2011: 155-174.

[5] BERTHOLD O, FEDERRATH H, KÖPSELL, et al. Web MIXes: a system for anonymous and unobservable Internet access [C]// International Workshop on Designing Privacy Enhancing Technologies: Design Issues in Anonymity and Unobservability. Springer, 2000: 115-129.

[6] CLARKE I, SANDBERG O, WILEY B. Freenet: a distributed anonymous information storage and retrieval system[C]// International Workshop on Designing Privacy Enhancing Technologies: Design Issues in Anonymity and Unobservability. Springer, 2000: 44-66.

[7] LING Z, LUO J, WU K. TorWard: discovery, blocking, and traceback of malicious traffic over tor [J]. IEEE Transactions on Information Forensics and Security, 2015, 10(12): 2515-2530.

[8] RAYMOND J F. Traffic analysis: protocols, attacks, design issues, and open problems [M]// Designing Privacy Enhancing Technologies. Berlin Heidelberg: Springer, 2001:10-29.

[9] WANG T, GOLDBERG I. On realistically attacking tor with website fingerprinting [J]. Proceedings on Privacy Enhancing Technologies, 2016(4): 21-36.

[10] BIRYUKOV A, KHOVRATOVICH D, PUSTOGAROV I. Deanonymisation of clients in Bitcoin P2P network [C]// ACM SIGSAC Conference on Computer and Communications Security. ACM, 2014: 15-29.

[11] 黄韬, 刘江, 张晨, 等. 基于 SDN 的网络试验床综述[J]. 通信学报, 2018, 39(6): 155-168.
HUANG T, LIU J, ZHANG C, er al. Survey on SDN-based network testbeds[J]. Journal on Communications, 2018, 39(6): 155-168.

[12] CHAUM D L. Untraceable electronic mail, return addresses and digital pseudonyms [J]. Communication of the ACM, 1981, 24(2): 84-88.

[13] EDMAN M, YENE R, BÜLEN T. On anonymity in an electronic society: a survey of anonymous communication systems[J]. ACM Computing Surveys, 2009, 42(1):1-35.

[14] KELLY D, RAINES R, BALDWIN R, et al. Exploring extant and emerging issues in anonymous networks: a taxonomy and survey of protocols and metrics [J]. IEEE Communications Surveys & Tutorials, 2012, 14(2): 579-606.

[15] KWON A, LAZAR D, DEVADAS S. Riffle: an efficient communication system with strong anonymity [J]. Proceedings on Privacy Enhancing Technologies, 2016(2):115-134.

[16] LEBLOND S, CHOFFNES D, ZHOU W. Towards efficient traffic analysis resistant anonymity networks[J]. ACM SIGCOMM Computer Communication Review, 2013, 43(4): 303-314.

[17] BLOND S L, CHOFFNES D, CALDWELL W. Herd: a scalable, traffic analysis resistant anonymity network for VoIP systems [C]// The 2015 ACM Conference. ACM, 2015: 639-652.

[18] CHEN C. Infrastructure-based anonymous communication protocols in future internet architectures [D]. Pittsburgh: Carnegie Mellon Uni-

versity, 2018.

[19] SANKEY J, WRIGHT M. Dovetail: stronger anonymity in next generation internet routing [C]// International Symposium on Privacy Enhancing Technologies Symposium. Springer, 2014: 283-303.

[20] CHEN C, ASONI D E, BARRERA D. HORNET: high-speed onion routing at the network layer [C]// The 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, 2015:1441-1454.

[21] CHEN C, PERRIG A. PHI: path-hidden lightweight anonymity protocol at network layer [J]. Proceedings on Privacy Enhancing Technologies, 2017(1):1-18.

[22] CHEN C, DANIELE E, DANEZIS G. TARANET: traffic analysis resistant anonymity at the network layer [C]// IEEE European Symposium on Security and Privacy. IEEE, 2018: 137-152.

[23] 王啸,方滨兴,刘培朋,等. Tor 匿名通信网络节点家族的测量与分析[J]. 通信学报, 2015, 36(2): 80-87.
WANG X, FANG B X, LIU P P, et al. Measuring and analyzing node families in the Tor anonymous communication network[J]. Journal on Communications, 2015, 36(2): 80-87.

[24] BAUER K, MCCOY D, GRUNWALD D, et al. Low-resource routing attacks against tor[C]//Proceedings of the 2007 ACM Workshop on Privacy in Electronic Society. ACM, 2007: 11-20.

[25] 潘吴斌,程光,郭晓军,等. 网络加密流量识别研究综述及展望[J]. 通信学报, 2016, 37(9): 154-167.
PAN W B, CHENG G, GUO X J, et al. Review and perspective on encrypted traffic identification research[J]. Journal on Communications, 2016, 37(9): 154-167.

[26] CHAKRAVARTY S, BARBERA M V, PORTOKALIDIS G. On the effectiveness of traffic analysis against anonymity networks using flow records[C]// International Conference on Passive and Active Network Measurement. Springer, 2014: 247-257.

[27] LING Z, LUO J, YU W, et al. Protocol-level attacks against Tor [J]. Computer Networks, 2013, 57(4): 869-886.

[28] KWON A, ALSABAH M, LAZAR D. Circuit fingerprinting attacks: passive deanonymization of tor hidden services [C]// USENIX Conference on Security Symposium. USENIX Association, 2015: 287-302.

[29] ZHU T, FENG D, WANG F. Efficient anonymous communication in sdn-based data center networks [J]. IEEE/ACM Transactions on Networking, 2017, 25(6): 3767-3780.

[30] MEIER R, GUGELMANN D, VANBEVER L. iTAP: in-network traffic analysis prevention using software-defined networks [C]// The Symposium on SDN Research. ACM, 2017: 102-114.

[31] TATLICIOGLU S, CIVANLAR S, GORKEMLI B. A security services platform for software defined networks[C]//IEEE Conference on Network Function Virtualization and Software Defined Networks. IEEE, 2016: 39-43.

[32] JAFARIAN J H, AL-SHAER E, DUAN Q. OpenFlow random host mutation: transparent moving target defense using software defined networking [C]// ACM SIGCOMM Workshop on Hot Topics in Software Defined Networks. ACM, 2012: 127-132.

[33] MACFARLAND D C, SHUE C A. The SDN shuffle: creating a moving-target defense using host-based software-defined networking [C]// The 2th ACM Workshop on Moving Target Defense. ACM, 2015: 37-41.

[34] SKOWYRA R, BAUER K, DEDHIA V. No PHEAR: networks without identifiers [C]// The 3th ACM Workshop on Moving Target Defense. ACM, 2016: 3-14.

[35] SILVA E G D, KNOB L A D, WICKBOLDT J A. Capitalizing on SDN-based SCADA systems: an anti-eavesdropping case-study [C]// IFIP/IEEE International Symposium on Integrated Network Management. IEEE, 2015: 165-173.

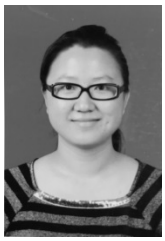
[36] LING Z, LUO J, WU K. Protocol-level hidden server discovery [C]// The 32th IEEE International Conference on Computer Communications. IEEE, 2013: 1043-1051.

[37] KONG J J, HONG X Y. ANODR: anonymous on demand routing with untraceable routes for mobile ad-hoc networks [C]// International Symposium on Mobile Ad Hoc Networking and Computing. ACM, 2003: 291-302.

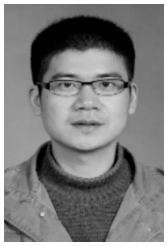
[38] SAKAI K, SUN M T, KU W S. Performance and security analyses of onion-based anonymous routing for delay tolerant networks[J]. IEEE Transactions on Mobile Computing, 2017, 16(12): 3473-3487.

[39] WIRTZ G, SANDMANN W, LOESING K. Performance measurements and statistics of tor hidden services[C]// International Symposium on Applications and the Internet. IEEE, 2008:1-7.

[作者简介]



赵蕙（1979− ），女，江苏镇江人，江苏大学博士生，主要研究方向为网络安全、隐私保护。



王良民（1977− ），男，安徽潜山人，博士，江苏大学教授、博士生导师，主要研究方向为密码学与安全协议、物联网安全、大数据安全。