网络与信息安全学报 Chinese Journal of Network and Information Security

中国计算机学会会刊 CCF推荐中文科技期刊 中国网络空间安全协会会刊 Scopus收录期刊 中国科技核心期刊

网络与信息安全学报, 2019, 5(1): 66-77 doi: 10.11959/j.issn.2096-109x.2019008

学术论文

匿名网络Tor与I2P的比较研究

杨云 (mailto:yyang@yzu.edu.cn), 李凌燕, 魏庆征

扬州大学信息工程学院，江苏 扬州 225127

Comparative study of anonymous network Tor and I2P

YANG Yun (mailto:yyang@yzu.edu.cn), LI Lingyan, WEI Qingzheng

College of Information Engineering,Yangzhou University,Yangzhou 225127,China

摘要

Tor（the onion router）是部署最多的匿名通信系统，提供在线匿名和隐私保护，而隐形互联网I2P （invisible Internet project）允许应用程序通过使用大蒜路由，以匿名和安全方式相互发送消息。匿名网络Tor和I2P目前已受到学术界、工业界的高度重视，也受到用户的欢迎。网络Tor和I2P之间的设计理念区别关键在于：I2P试图将现有的互联网服务转移到I2P网络，并在框架内提供服务实现，而Tor则允许匿名访问分别实施和操作外部互联网服务。对匿名网络Tor、I2P分别从使用术语、项目开发、匿名服务、关键技术、威胁类型等多个方面进行比较，揭示两种匿名网络的内在联系与本质区别。

关键词： 匿名网络；Tor；I2P；洋葱路由；大蒜路由

Abstract

Tor is the most deployed anonymous communication system,providing online anonymity and privacy protection,while the invisible Internet project allows applications to send messages to each other anonymously and securely by using garlic routing.The anonymous network Tor and I2P have been highly valued by the academic community and the industry,and are also welcomed by users.The key difference between the design concept between the Tor network and the I2P is that I2P attempts to transfer the existing Internet service to the I2P network,and service implementation is provided within the framework,while Thor allows anonymous access to implement and operate external Internet services separately.The anonymous networks Tor and I2P in terms of terminology,project development,anonymous services,key technologies,threat types,etc.were compared,revealing the inherent and essential differences between the two anonymous networks.

Keywords: anonymous network ; Tor ; I2P ; onion routing ; garlic routing

本文引用格式

杨云, 李凌燕, 魏庆征. 匿名网络Tor与I2P的比较研究. *网络与信息安全学报*[J], 2019, 5(1): 66-77 doi:10.11959/j.issn.2096-109x.2019008

YANG Yun. Comparative study of anonymous network Tor and I2P. *Chinese Journal of Network and Information Security*[J], 2019, 5(1): 66-77
doi:10.11959/j.issn.2096-109x.2019008

1 引言

Tor 是一个基于电路的低延迟覆盖网络，提供匿名和隐藏服务，它是当今时代部署最多、应用广泛的匿名通信系统[1,2]。它的用户数十万，如军事、情报机构、记者等以及超过75个国家的6 011个继电器提供在线匿名和隐私保护。

I2P 是一个基于分组的高延迟匿名重叠网络。它在通信方之间构建虚拟网络，保护通信不被其他人（如互联网服务提供商）进行调查和检查[3,4]。I2P的用户通常是记者、活动家、举报人以及普通用户。没有网络可以“完全匿名”，I2P旨在使攻击越来越难以登录。随着网络规模扩大，其匿名性将变得更强，I2P用户可以控制匿名和延迟之间的权衡。

I2P是在借鉴了Tor的许多开发理念、网络技术的基础上开发的，网络Tor和I2P之间的理念区别关键在于：I2P试图将现有的互联网服务转移到I2P网络，并在框架内提供服务实现，而Tor则允许匿名访问分别实施和操作外部互联网服务。网络Tor和I2P之间的关键技术差异在于：消息流置换了细胞、单向隧道置换了双向电路、分组交换变换为电路交换、基于性能的对等体选择代替了基于带宽的对等体选择、分布式架构代替了集中式框架等。

2 Tor与I2P的使用术语

在技术方面，I2P在许多方面类似于Tor，但它的开发人员经常使用稍微不同的术语表示几乎相同的功能。表1提供了Tor和I2P之间使用的不同术语之间的映射[5]。

表1　Tor与I2P比较：使用术语

Tor	I2P
Cell，细胞	Message，消息
Client，客户	Router、Clients，路由器或客户端
Circuit，电路	Tunnel，隧道

Tor	I2P
Directory，目录	NetDB，网络数据库
directory server，目录服务器	floodfill router，floodfill路由器
Entry guard，入境卫兵	Fast peer，快速对等体
Ingress node，入口节点	Inproxy，入口代理
exit node，退出节点	Outproxy，出口代理
hidden service，隐藏服务	Eepsite or destination，Eepsite或目的地
hidden service descriptor，隐藏服务描述符	lease set，租约集
introduction point，介绍点	inbound gateway，入站网关
onion routing，洋葱路由	garlic routing，大蒜路由
Node、Server，节点、服务器	Router，路由器
Onion agent，洋葱代理	I2P Tunnel客户端
Onion service，洋葱服务	隐藏服务，Eepsite或目的地
Rendezvous Point，会合点	Inbound Gateway+Outbound Endpoint，入站/出站网关
Router descriptor，路由器描述符	Routerinfo，路由器信息

3 Tor与I2P的项目开发

表2,表3,表4是基于Tor和I2P的特征构建的，分别从认知度、性能、开发技术3个方面，比较了匿名网络Tor和I2P。

表2　Tor和I2P比较：认知度

特征	Tor	I2P小
用户群	非常大	
学术界关注度	较多、可见	较少见到
黑客群体关注度	较多、可见	较少见到
可扩展性	较好	一般
开发者	较多	较少
支付或资助	较多	较少
软件/语言	C	Java

新窗口打开 (2096-109x-5-1-00066/T2.html) | 下载CSV (2096-109x-5-1-00066/T2.csv.zip)

表3　Tor和I2P比较：性能

特征	Tor	I2P
来自DoS攻击的脆弱性	更脆弱	不那么脆弱
出口节点的数目	大量的出口节点	较少的出口节点
文档记录	良好的文档记录	较差的文档记录
网站	较好	很好
不同语言的文档记录	可获得	不可获得
内存使用情况	更高效	无效的
带宽偷听情况	很低	很高
集中式/分布式控制	集中式	分布式
对Sybil是脆弱的	是	不是
吞吐量	较高	较低
时延	低	高

新窗口打开 (2096-109x-5-1-00066/T3.html) | 下载CSV (2096-109x-5-1-00066/T3.csv.zip)

表4　Tor和I2P比较：开发技术

特征	域名	节点选择标准	目录服务器/floodfill对等体	分组/电路交换	单向/双向	保护以免检测客户端活动	隧道/电路的期限	TCP/UDP传输	SOCKS/I2P API
Tor	.onion	信任、声明、能力	信任和硬编码	电路交换	双向电路	较少保护	时间长	TCP	SOCKS
I2P	.i2p	不断分析和排名性能	多变且不可信	分组交换	单向隧道	较多保护	时间短	两者都可以	I2P API

新窗口打开 (2096-109x-5-1-00066/T4.html) | 下载CSV (2096-109x-5-1-00066/T4.csv.zip)

1) SOCKS/I2P API：Tor使用Socket Secure （SOCKS）接口，因此SOCKS能够感知应用程序，可以很容易地指向 Tor 软件[6]，这表明采用 SOCKS 的应用程序无须任何更改，可以直接使用。另外，I2P 是一个中间件，提供应用程序可用于通过网络进行通信的 API，这意味着应用程序需要进行复杂的调整。SOCKS 与I2P API极大地改变了构建使用 I2P 或 Tor 网络、通过 Internet 进行匿名通信的应用程序的工作量和能力。SOCKS 接口只能通过 TCP 传输消息，而 I2P可以在 UDP和 TCP之间进行选择，这可使I2P在使用某些应用程序时提供更好的性能。

2) 可用的应用程序：I2P和Tor都具有广泛的应用程序，而大多数I2P应用程序专门用于访问I2P网络内的服务（例外的是Susimail/2IpMail能够从公共Internet发送和接收邮件）。另外，由于Tor使用SOCKS接口，Tor能够与使用SOCKS代理配置的任何应用程序一起使用（如常用的Web浏览器）[7,8]。

3) 消息安全性和匿名性：两个网络都具有各种加密层，从由 OR（onion routers）或I2P 对等体维护的 TLS 连接提供的传输层加密开始，I2P还具有额外的隧道加密功能。通过网络发送的消息是洋葱或加密的大蒜，这意味着从用户到隧道或电路的连接始终是加密的。只要在网络内部进行交互，I2P中的消息也是端到端加密的。但在 Tor 的情况下，无法保证端到端加密，这取决于所使用的传输层协议[9]。

4) 性能：使用I2P或Tor访问公共互联网时的延迟和带宽作为评价指标，测量发现：I2P 能够在发出简单的HTTP-GET请求时获得更好的结果，但Tor在访问整个网页和下载文件方面提供了明显更好的结果。在 50%的情况下，Tor 能够在不到 16.99 s 时间内检索整个网页，而 50%的I2P请求需要花费103.19 s。在下载速度方面，Tor能够提供51.62 kB/s的平均速度，而I2P的平均速度为12.91 kB/s[10]。

5) 可扩展性：增加参与匿名网络的客户端数量直接影响Tor和I2P，匿名设置量变得更大，网络流量增加并可能导致拥塞等问题。对于Tor可能需要增加用于构建电路的路由器数量，从而增加延迟并减少可用带宽。增加OR的数量会产生另一个问题，即不断增长的目录。在I2P的情况下，假设加入网络的新对等体能够提供足够的容量和带宽，它们也可以是用于构建隧道的对等体。因此，不太可能出现拥塞，但如果足够数量的客户端寻求访问I2P网络之外的服务，则需要提供更多的外部代理。

6) 用法：I2P 提供多种应用程序，专为 I2P网络内的通信而设计，所以它的代理很少。而Tor则设计用于在网络外部的路由流量，与I2P相比具有更多的退出节点。

4 Tor与I2P的匿名服务

Tor与I2P都构建了匿名服务，如表5和表6所示，但I2P现有的应用包括绝大部分典型的因特网应用，如匿名Web浏览、匿名Web hosting、匿名博客、匿名聊天、匿名文件传输、匿名文件共享、匿名E-mail、匿名新闻组和其他一些正在开发的应用。但Tor提供的隐藏服务在外置服务器上，而I2P提供的隐藏服务在内置服务器上。虽然Tor 有隐藏服务而 I2P 有退出节点，但 Tor的规范用法是访问外部服务，而I2P规范用法是访问内部服务[11，12]。

表5　Tor匿名服务的构建

匿名服务	描述
Deep Web Radio	文化，世界音乐电台
TorPages	文件存储，静态HTML/文本主机服务
BitBlender	金融，加密电子货币混合交易站点
All You're Wiki	匿名服务的资讯
TorChat	邮件和即时通信

匿名服务	描述
DeepDotWeb	新闻，举报
Cruel Onion Wiki	匿名维基
Onion Link	搜索引擎，通过自己的Tor2 Web服务提供直接的.onion访问
TorBook	社交媒体和论坛，社交网络

新窗口打开 (2096-109x-5-1-00066/T5.html) | 下载CSV (2096-109x-5-1-00066/T5.csv.zip)

5 Tor与I2P的关键技术

由于Tor与I2P在开发理念上不完全相同，因此两个网络在一些网络关键技术上存在差异[13]，表7列出了Tor与I2P在关键技术上的差异，这直接影响了网络的功能与性能。

表6　I2P匿名服务的构建

匿名服务	描述
Eepsites	由基于Jetty2的I2P对等体提供的HTTP服务器
susidns	从Eepsites到目标标识符的映射地址簿
BOB	将任意应用连接到I2P网络的API
I2PSnark	作为web应用集成的bittorrent客户端
Robert	用BOB的I2Pbittorrent客户端
I2P-bt	基于bittorrent客户端的命令行
Transmission for I2P	bittorrent客户端的端口、向I2P传播
I2Phex	Gnutella客户端Phex的I2P移植版，gnutella客户的端口
iMule	基于aMule的文件共享程序
Susumail	假名E-mail服务，通过I2PTunnel利用普通的E-mail客户端访问

匿名服务	描述
I2P-Bote	分布式电子邮件通信系统
I2P-Messenger	I2P的即时通信系统
Syndiemedia (Syndie)	博客工具

新窗口打开 (2096-109x-5-1-00066/T6.html) | 下载CSV (2096-109x-5-1-00066/T6.csv.zip)

表7　Tor和I2P比较：关键技术

Tor	I2P
三跳电路	用户可随机配置隧道数
双向电路	单向隧道
基于带宽的对等体选择	基于性能的对等体选择
7个完整数据的目录服务器	分布式DHT（NetDB）
链接和分层加密，但不是端到端加密	端到端、链接和分层加密
许多退出节点、隐藏服务较少	一个退出节点，集成了许多隐藏服务
隐藏服务在外置TCP服务器上	许多隐藏服务在内置服务器中
电路交换	分组交换
仅通过TCP传输	通过TCP和UDP传输
在C中实施	在Java中实施

新窗口打开 (2096-109x-5-1-00066/T7.html) | 下载CSV (2096-109x-5-1-00066/T7.csv.zip)

5.1 工作流程

1) Tor工作流程

Tor网络工作流程如图1所示。

2) I2P工作流程

I2P网络工作流程如图2所示。

由图1、图2的工作流程对比可以看出，Tor网络工作依赖于集中式控制的目录服务器，而I2P网络工作依赖于分布式控制的网络数据库NetDB，I2P网络的可靠性比Tor网络高。

5.2 隧道技术

Tor 是通过“电路”双向传递消息的，即入站和出站消息是同一条电路，如图3所示；而I2P是通过“隧道”单向传递消息，即入站和出站消息是不同的两条隧道，并且这两条隧道每隔10 min重新建立，如图4 所示。Tor 的出站端点是公开的、未隐藏，而I2P的出站端点被隐藏。

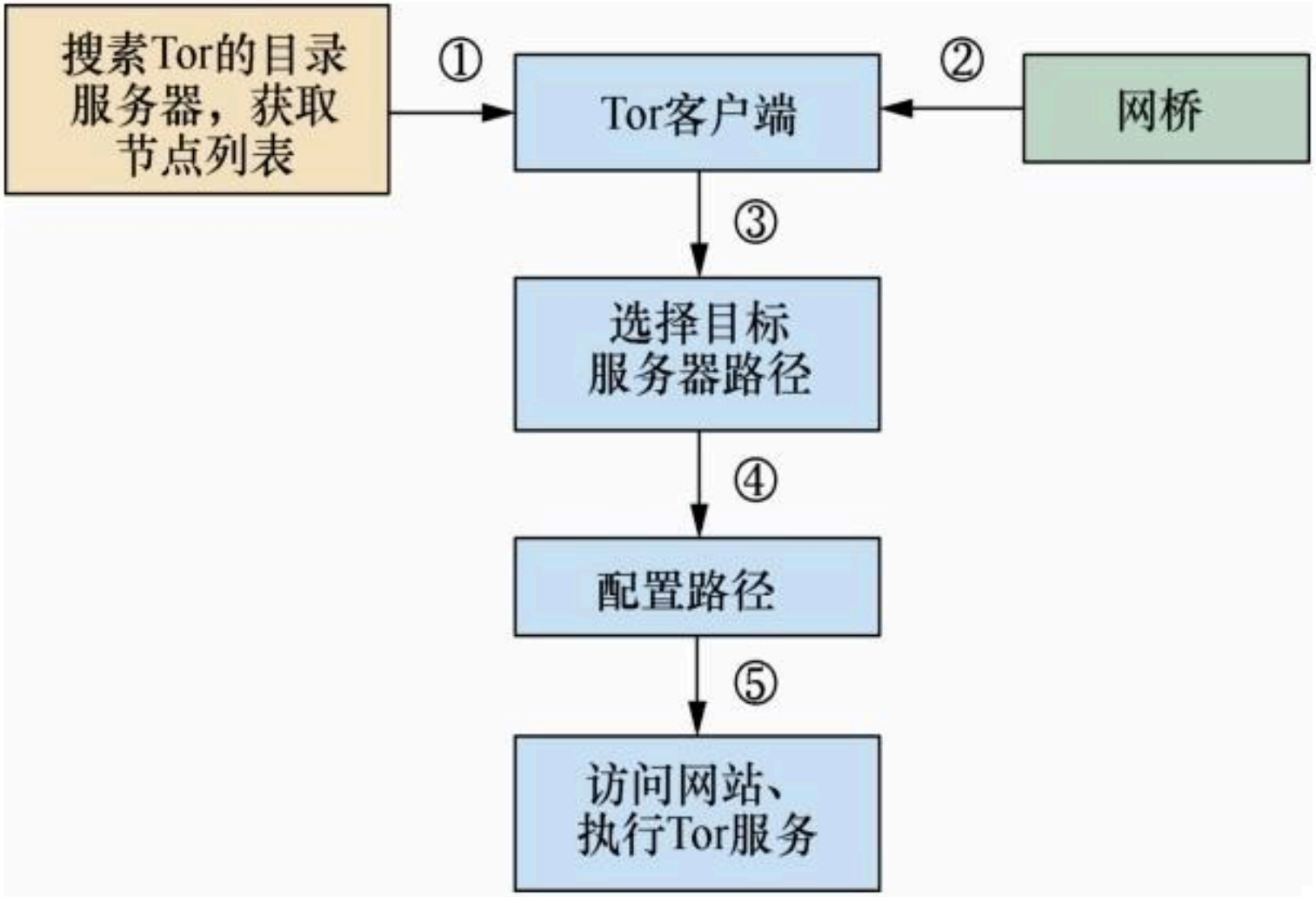


图1　Tor网络工作流程

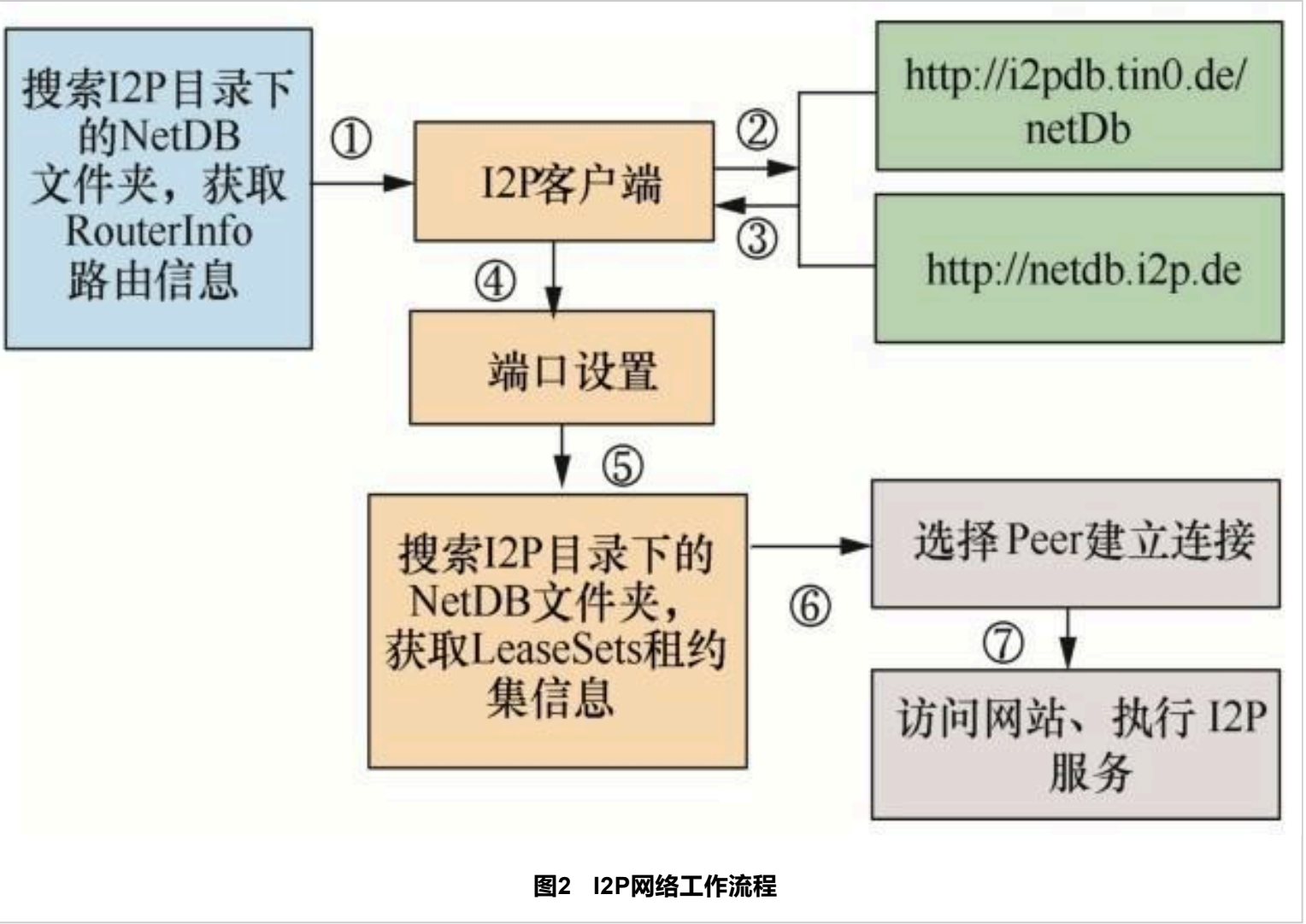
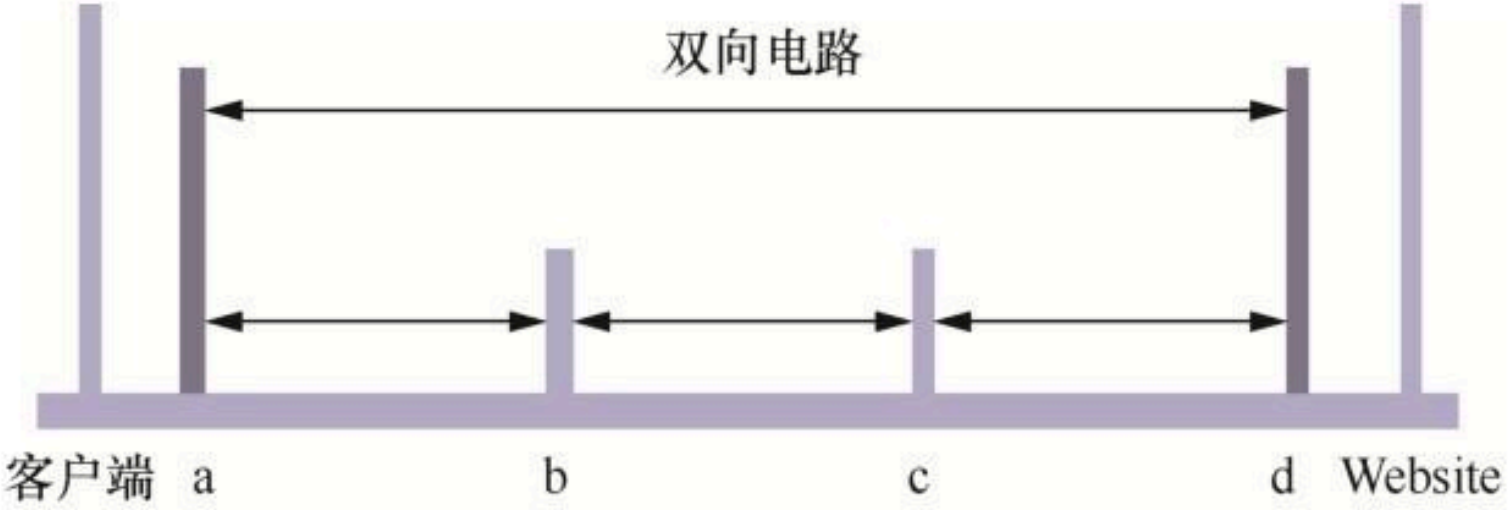
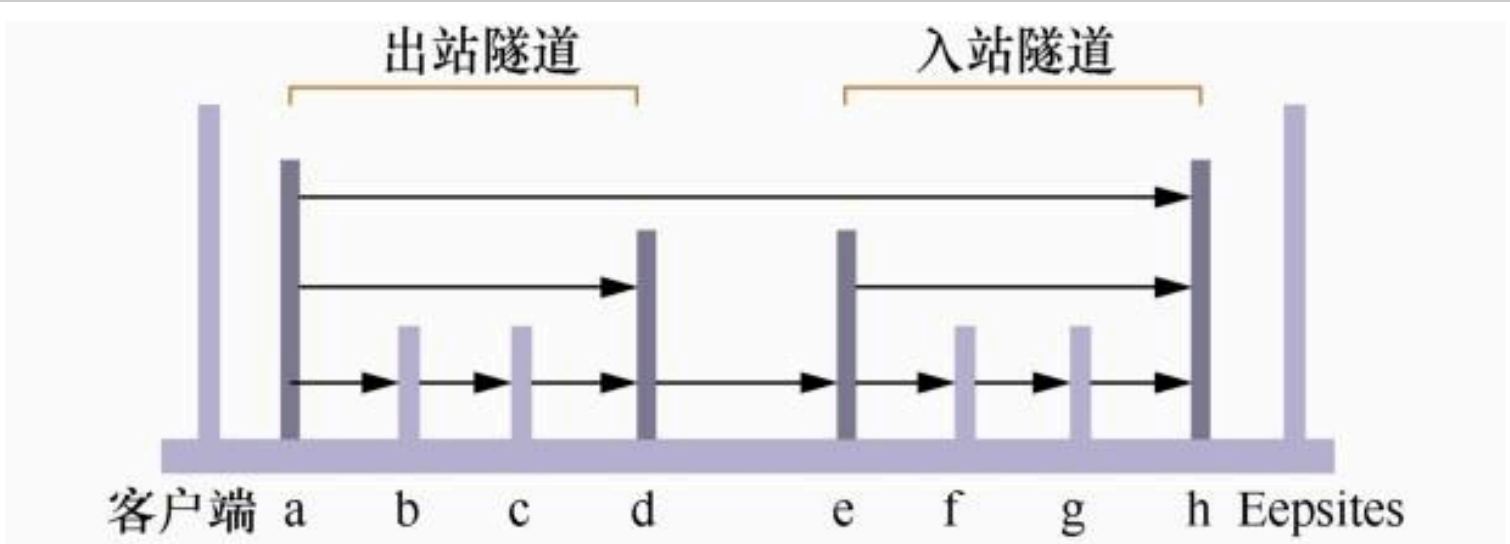


图2　I2P网络工作流程



端到出口端加密 {RSA1024+AES256}	客户端-d	电路加密 {私钥AES256}	a-d
洋葱加密 {RSA1024+AES256}	a-d	传输加密 {DHE+AES256}	a-b,b-c,c-d

图3　Tor的电路



端到端加密 {E1Gamal/Session Tag+AES}	客户端-Eepsites	隧道加密 {私钥AES}	a-d,e-h
大蒜加密 {E1Gamal/Session Tag+AES}	a-h	传输加密 {DH/STS+AES}	a-b,b-c,c-d,d-e, e-f,f-g,g-h

图4　I2P的隧道

I2P 的隧道具有多样性特点[14]：入站隧道和出站隧道、探索隧道和客户端隧道。从客户端到服务器的路由分为两个隧道：由客户端控制的出站隧道和由服务器控制的入站隧道，这两条隧道之间是直接连接的，即出站隧道的出站端点直接连接到入站隧道的入站网关。隧道通过将目标的入站网关和出站端点与目标路由器分开来提供匿名性。

探测性隧道通常是低带宽的，并且由路由器本身使用，包括构建和测试其他隧道、发送网络数据库（NetDB）查询以及构建客户端隧道。客户端隧道通常是高带宽的，用于所有用户客户端和服务器流量，包括访问内部I2P网络目标或“隐藏服务”，如Eepsites，与外部网关的连接（Inproxies 和 Outproxies）以及其他用途。

5.3 对等体选择

Tor是基于带宽的对等体（Peers）选择，I2P是基于性能的对等体选择[15,16]。对等体选择的目的是快速地构建电路或隧道。

1) Tor：基于带宽的对等体选择

Tor 的目录服务器使用有源带宽探测来测量和记录每个OR（onion router）能够提供的带宽，如果没有针对此特定OR的探测数据，Tor还必须依赖各自发布的带宽值。带宽信息用于以加权概率方式选择中间路由器和出口路由器。

Tor 客户端使用路径选择算法来选择用于构建电路的OR，只要测量值可用就优先采用。Tor中的所有其他OR都选择时的概率与其带宽成正比，这意味着仅考虑带宽，而忽略其他属性（如OR的实际位置）。

2) I2P：基于性能的对等体选择

I2P 客户端依赖于先前监控的性能值和网络的当前状态，不使用有效带宽探测。 I2P 节点选择算法还能够非常快速地对失败的对等体和网络拓扑中的其他变化做出反应，通过不断分析和排名性能来选择对等体，而不是信任所声称的容量。

表8　Tor目录

Tor版本	昵称	IP地址	洋葱路由端口	位置	具体位置
	morial	128.31.0.39	9101	美国	麻省理工学院
	Tor26	86.59.21.38	443	奥地利	维也纳
	dizum	194.109.206.212	443	荷兰	多德雷赫特
	Tonga	82.94.251.203	443	荷兰	阿姆斯特丹
	gabelmoo	212.112.245.170	443	德国	RIRE网络协调中心
Tor0.2.8	dannenberg	193.23.244.244	443	德国	RIRE网络协调中心
	urras	208.83.223.34	80	美国	旧金山
	maatuska	171.25.193.9	80	SE	瑞典

Tor版本	昵称	IP地址	洋葱路由端口	位置	具体位置
	Faravahar	154.25.32.5	443	美国	华盛顿
	Longclaw	199.254.238.52	443	美国	西雅图

新窗口打开 (2096-109x-5-1-00066/T8.html) | 下载CSV (2096-109x-5-1-00066/T8.csv.zip)

性能指标主要为速度、容量。

速度定义：通过该对等体在1 min内测量的最快3个隧道带宽的平均值。

容量定义：在一段时间内通过对等体成功隧道构建的数量，令 r(t)是在一定时间段 t 内的成功构建数，则容量

$$R(t) = 4r(10\text{min}) + 3r(30\text{min}) + 2r(1h) + 1 \times (24h) \quad (1)$$

如果在给定时间段内没有成功构建，则该值为零，即永远不会发送构建请求，仅用于构建评级。评级还包括每次增加少量的“增长因子”，以便定期尝试通过新对等体构建。

每个时间t的当前容量计算r(t)为

r(t)=接受-拒绝-加权超时-4×加权失败+增长因子(2)

5.4 Tor目录与I2P NetDB

1) Tor目录

在Tor源代码或/ config.c中有许多默认目录。

这些目录权限由Tor项目的成员和受信任的外部个人/组运行。

2) I2P NetDB

Tor 通过连接目录服务器得知所有中继、进入/退出节点的存在，I2P 通过本地网络数据库NetDB得知其他节点的存在，NetDB通过Kad算法在连接其他节点时获悉更多节点的存在。

I2P NetDB 是一个分布式网络数据库，主要提供路由器联系信息和目标联系信息， 每一条数据都由适当的一方签名，并由使用或存储它的任何人进行验证。

NetDB由RouterInfos、LeaseSet这两个数据结构组成，RouterInfo存储有关特定I2P路由器的信息以及如何联系它，包括路由器标识符（route ID）、连接方式（UDP+port）、发布时间（release time）、密钥（非对称加密）等。LeaseSet存储特定目的地的信息，包括入站网关ID、服务、密钥（对称加密）。

图5和图6分别表示NetDB中的RouterInfo路由器联系信息用于构建隧道、LeaseSet 租约集用于连接出站和入站隧道。

图7说明了FloodFill NetDB的工作原理，用户节点在客户端下的NetDB目录下的RouterInfo文件中进行查找，找到一个FloodFill NetDB下的Peer1。然后FloodFill可以使用深度优先或广度优先进行遍历，Peer1告知在FloodFill NetDB内所有它已知的Peer。

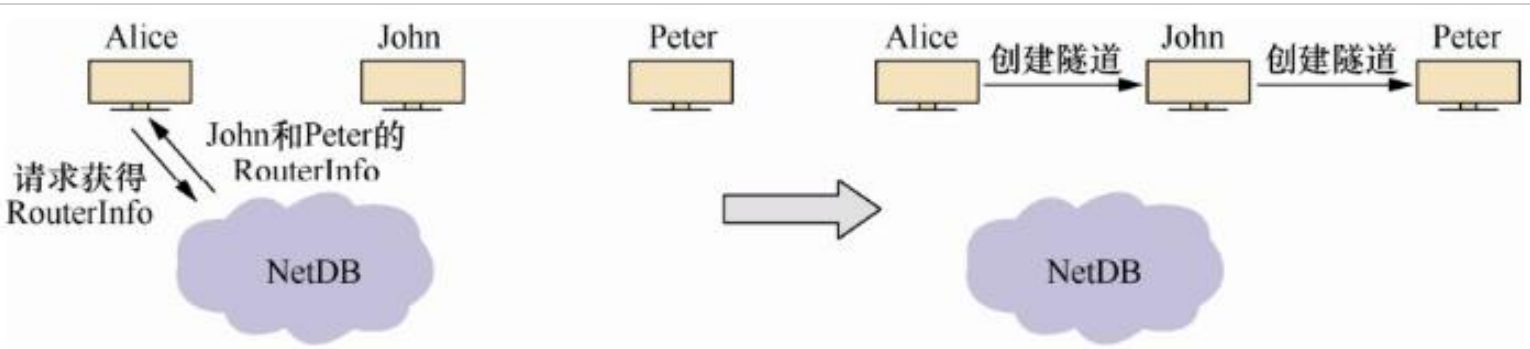


图5　RouterInfo用于构建隧道

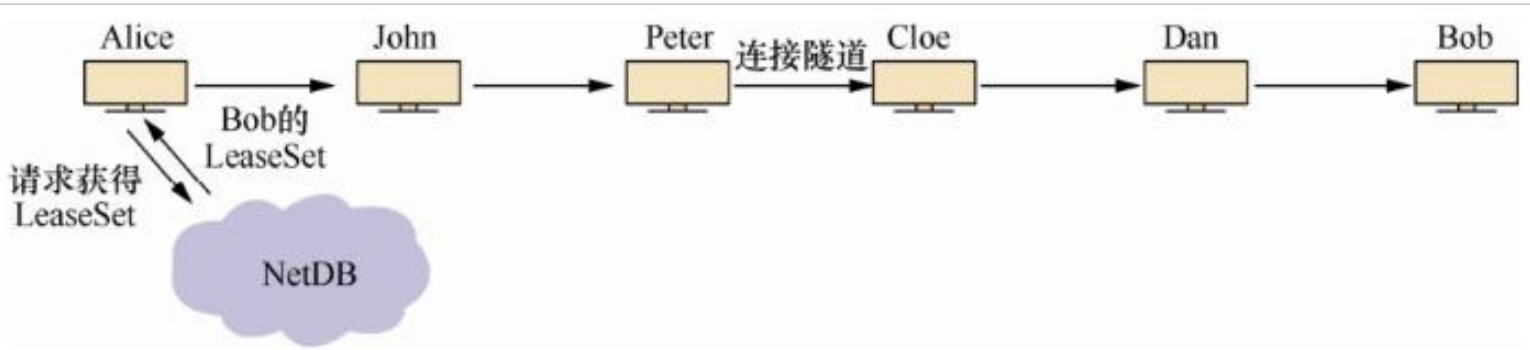


图6　LeaseSet用于连接出站和入站隧道

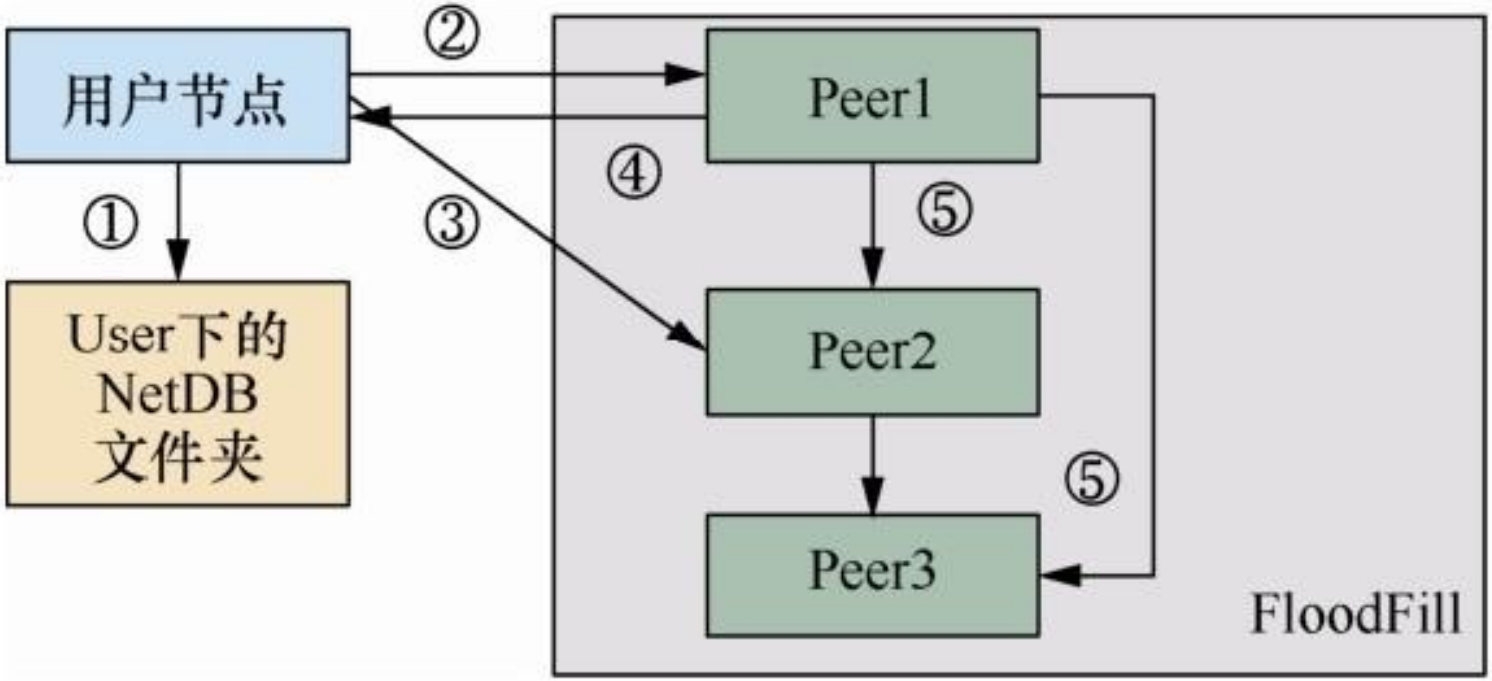


图7　FloodFill NetDB工作原理

表9说明了NetDB的物理视图，它是由行键（256 bit的摘要）、时间戳、节点ID（160 bit）、连接方式（IP地址+UDP端口号）、传输密钥（256 bit的对称密码）、入站网关ID、I2P匿名服务和大蒜密钥等构成。

5.5 路由方法

由图8和图9对比可知，Tor和I2P网络有相似之处和不同之处。这两个匿名服务的共同目标是通过使用多层加密，将流量中继到多个站点来提供匿名性，多层加密用于强化和拒绝用户与其消息之间的链接。Tor主要致力于为用户提供匿名访问网络以外的网站，而I2P提供匿名访问在I2P网络本身内私下托管的网站。与此同时，Tor还在Tor 网络中托管了网站（隐藏服务），而 I2P 支持访问Internet上托管的网站，但不支持使用外部代理访问I2P网络。就用于中继流量的路径而言，Tor网络和I2P网络上的路径发生变化并且不固定，用户保持连接到一个路径（电路隧道级联）的持续时间根据匿名系统的不同而不同，两种匿名服务的路由技术和路径选择也不同。

表9　NetDB物理视图

行键	时间戳	RouterInfo			LeaseSet		
		Node ID	连接方式	密钥	入站网关	I2P服务	密钥
	1527991262	SHA1（IP1 | random())	IP1+UDP port	AES256/CBC1	Gateway ID1	I2P-Syndie	ElGamal 公钥1
SHA256（节点ID | 时间戳)	1528085415	SHA1（IP2 | random())	IP2+UDP port	AES256/CBC2	Gateway ID2	I2P-Messanger	ElGamal 公钥2
	1528210926	SHA1（IP3 | random())	IP3+UDP port	AES256/CBC3	Gateway ID3	I2P-Hex	ElGamal 公钥3

新窗口打开 (2096-109x-5-1-00066/T9.html) | 下载CSV (2096-109x-5-1-00066/T9.csv.zip)

5.6 消息机制和交换方法

如图10所示，Tor协议中的协议数据交换使用固定长度的Cell，流量在网络中以固定大小的单元进行传输，每个单元是包含头和有效载荷的12 byte数据。头包括一个线路标识符（这个单元使用哪条线路）和一个指令（指明将要对这个单元的数据做什么）。中继单元在有效载荷数据之前有额外的头（中继头），包含一个stream ID、一个端到端的校验和、中继负载的长度和一个中继命令。

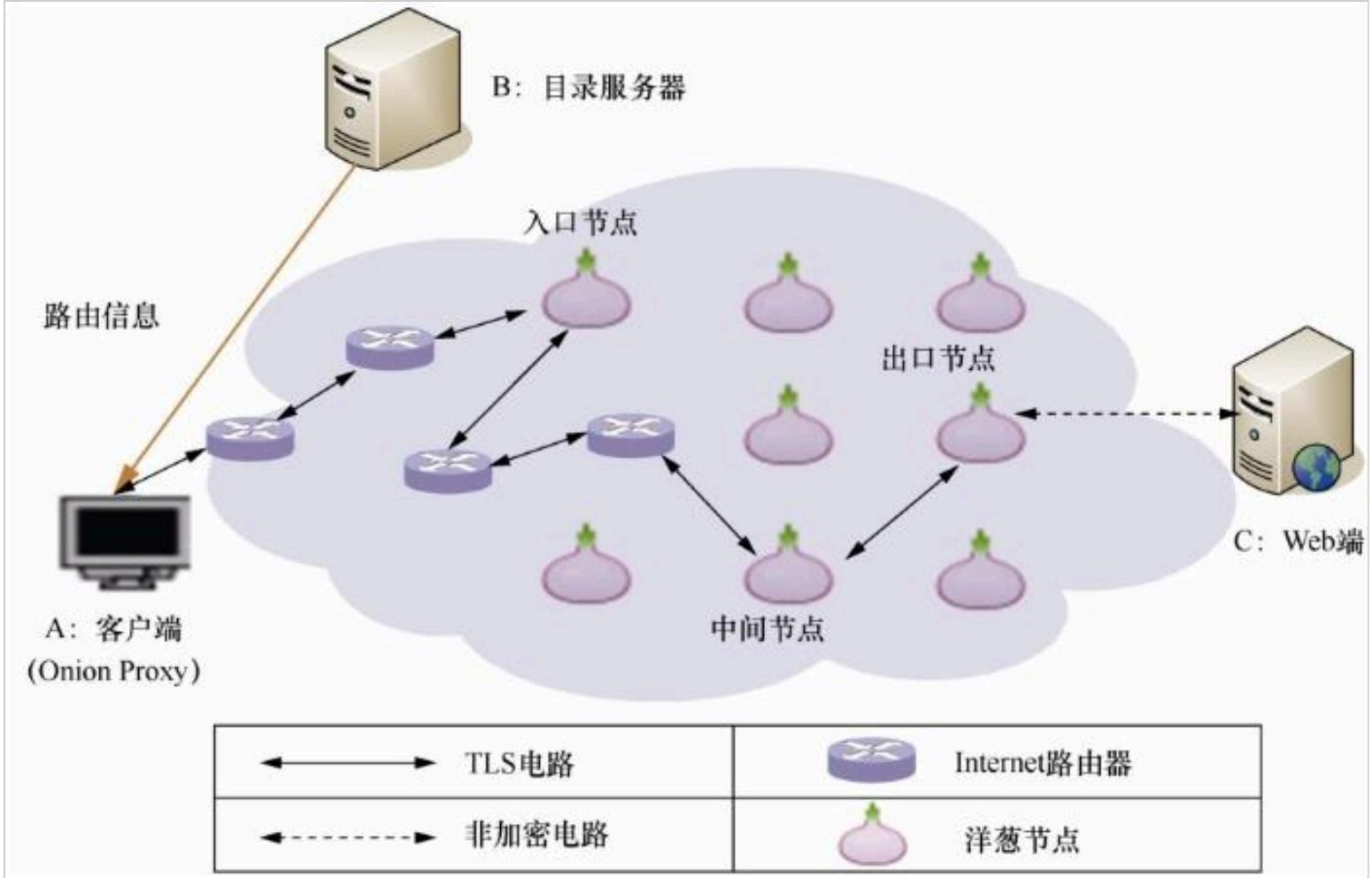

B：目录服务器
入口节点
路由信息
出口节点
C：Web端
A：客户端
(Onion Proxy)
中间节点
TLS电路
Internet路由器
非加密电路
洋葱节点

图8　洋葱路由

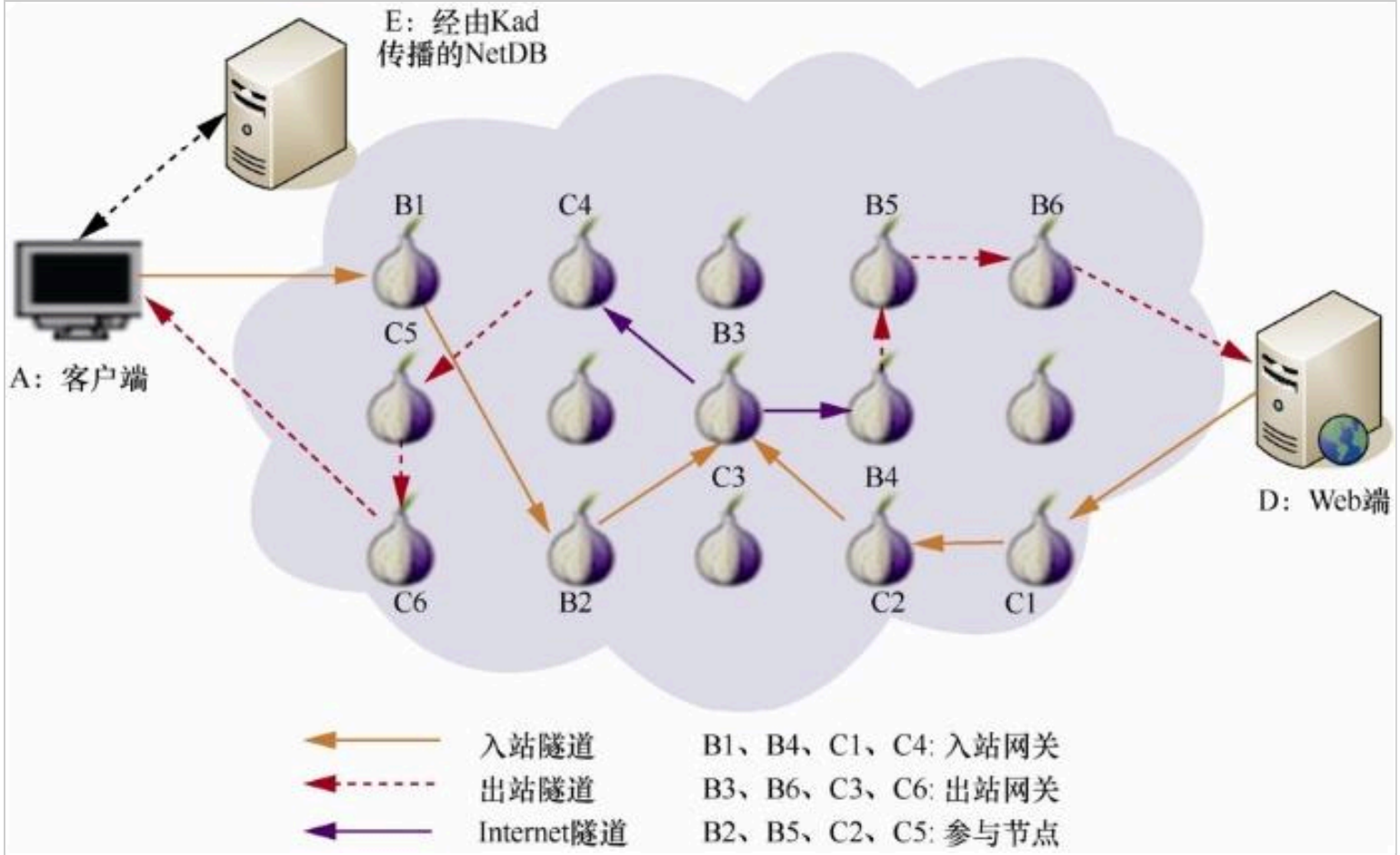

E：经由Kad
传播的NetDB
B1
C4
B5
B6
C5
B3
A：客户端
C3
B4
D：Web端
C6
B2
C2
C1
入站隧道
出站隧道
Internet隧道
B1、B4、C1、C4: 入站网关
B3、B6、C3、C6: 出站网关
B2、B5、C2、C5: 参与节点

图9　大蒜路由

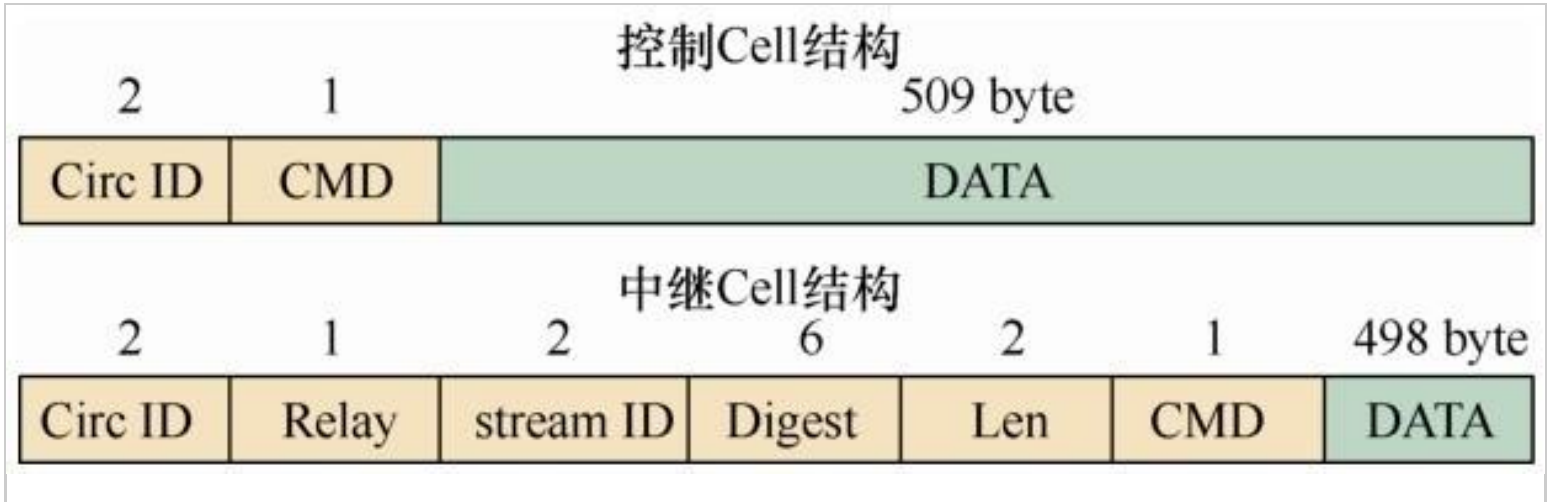

控制Cell结构
2
1
509 byte
Circ ID
CMD
DATA
中继Cell结构
2
1
2
6
2
1
498 byte
Circ ID
Relay
stream ID
Digest
Len
CMD
DATA

图10　Tor网络的Cell 结构

在图11中，I2P网络内的信息以I2NP（I2P网络协议）消息的形式交换，主要由传送指令和有效载荷组成，由于大小限制，它可以包含整个消息或仅包含部分消息。为了防止定时攻击，收集特定路由器的多个消息并将其组合成隧道消息。此消息包含该路由器的ID，用于加密有效负载的IV和有效负载本身，其中包含校验和、填充以及路由器收集的消息，格式为“交付说明”消息）和I2NP本身（称为“Clove”）。

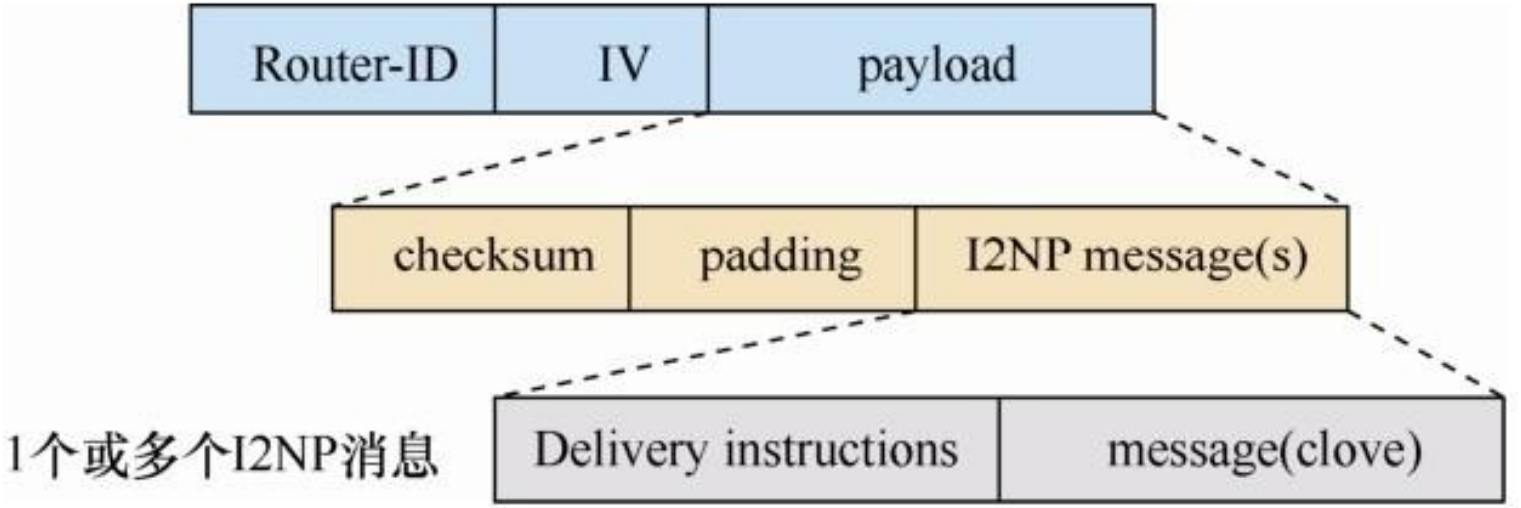


图11　I2P网络的message结构

同一个连接中的指令与数据，在Tor中沿着通过TCP建立的电路（Ciruit）流动至目的节点，而在I2P中，连接被消息机制（Message）打散为数据分组，经由不同的TCP或UDP隧道（Tunnel）交叉传输后，在接收方重组为数据流，即I2P基于包（分组）切换而Tor基于电路切换。因此， Tor经常应对高拥塞导致高延迟，而在I2P中，分组交换导致一些隐式负载平衡，并有助于避免拥塞和服务中断。这对于大型文件传输尤为重要，因此I2P更适合此类用途[17]。

I2P 网络中的所有对等体经常发送消息（端到端和网络维护消息），端到端消息沿其路径改变大小和数据，路由器间通信既加密又流式传输（使两个1 024 byte的消息与一个2 048 byte的消息无法区分），所以外部攻击者也无法访问消息。

在图12和图13中，msg：message表示消息、Inf：Infos 表示信息或数据、Enc：Encryption 表示加密。

在洋葱路由中，Tor 目录服务器随机分配给客户端C 3 个节点：入口节点n1、中继节点n2和出口节点n3，客户端、n1、n2、n3互相经过密钥协商得到3个公钥：Enc n1、Enc n2、Enc n3，对消息 msg 进行三层加密，传递给n1，n1 用自己的私钥解密后再传递给n2，n2用自己的私钥解密后再传递给n3，由n3将信息msg最终传递给Web网站或服务器W。

大蒜路由中的消息是“大蒜消息”，它是由多个消息或流数据捆绑而成。在大蒜路由中，I2P的 NetDB 根据DHT 算法随机分配给客户端 S两个或3个节点：输出网关n1、中继节点n2和输入网关 R（或 X），客户端、n1、n2、R（或X）互相经过密钥协商得到3个公钥：Enc n1、Enc n2、Enc R（或Enc X），对消息msg进行三层加密，传递给n1，n1用自己的私钥解密后再传递给n2，n2用自己的私钥解密后再传递给R或 X，由 R 或 X 将信息msg 最终传递给 Web网站或服务器W。

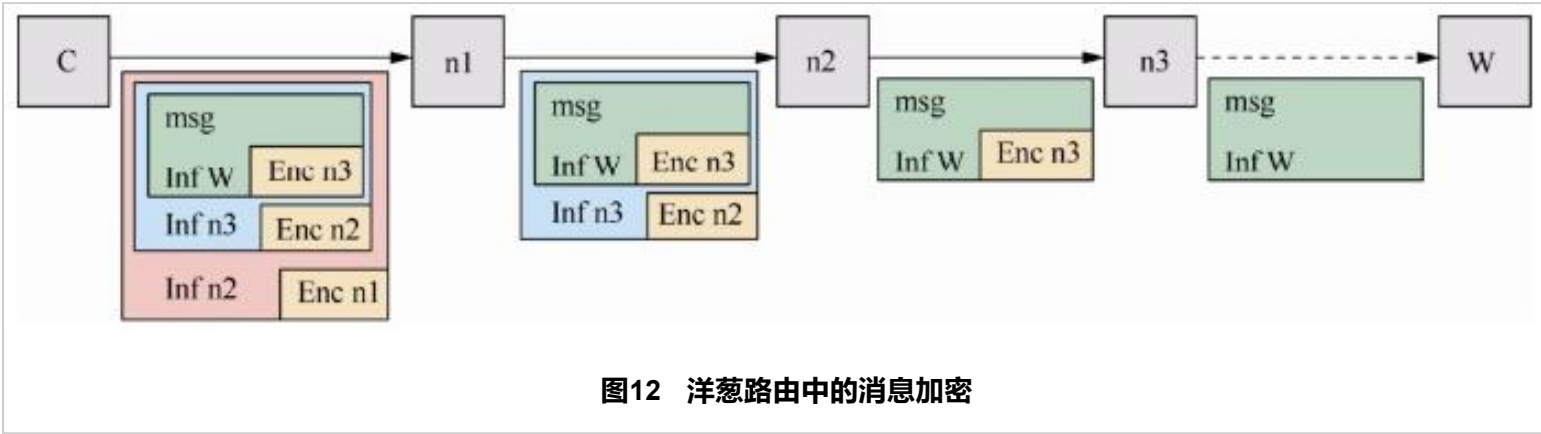


图12　洋葱路由中的消息加密

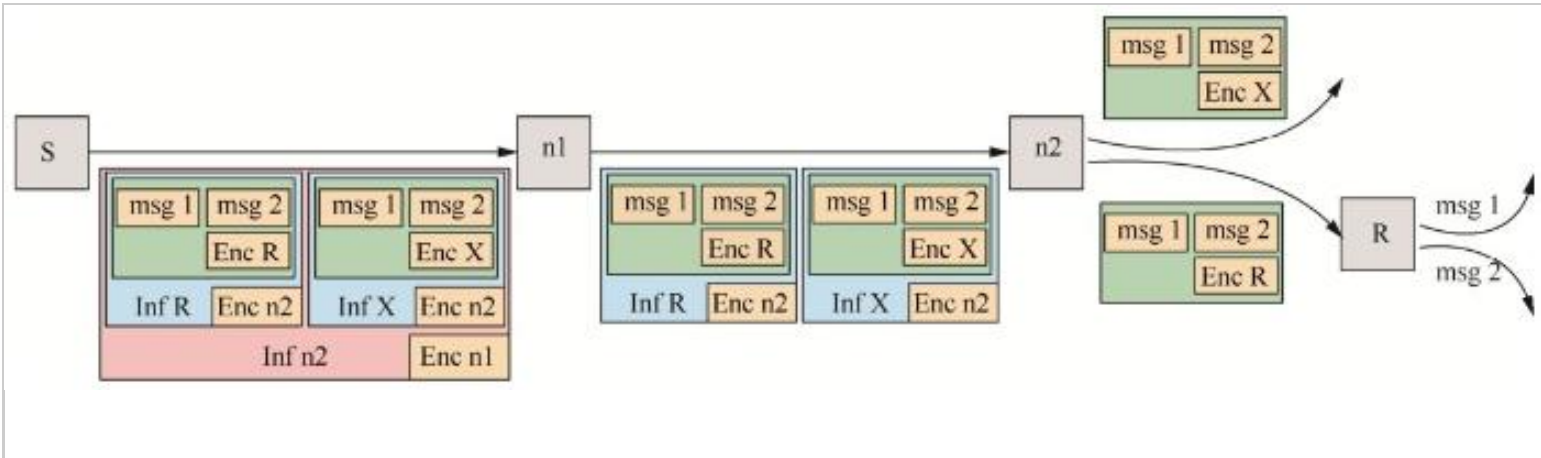


图13　大蒜路由中的消息加密

5.7 TCP/UDP传输

由于 Tor 网络中的节点间（除出口节点与服务器）使用TLS进行加密连接构建电路，TLS用于防止可能的攻击者修改数据，冒充洋葱路由器，提高网络效率和安全。Tor 使用 SOCKS接口与Internet进行交互，提高用户的匿名性。但 TLS、SOCKS 都是基于 TCP 的，所以 Tor的中继之间使用TCP连接，并且多个TCP流可以共享一个虚电路，每个OR都使用TLS连接到其他的OR。

而在I2P网络中，节点间全部使用TLS进行加密连接构建隧道，节点发现使用 Kademlia 的XOR 距离算法。TLS、Kademlia 分别基于 TCP和UDP，所以I2P的路由之间既使用TCP连接又使用UDP进行数据传输。I2P的传输连接是两个对等传输协议NTCP和SSU，NTCP是基于NIO的TCP，SSU是安全半可靠的UDP（它的主要目的是通过隧道安全地传输 I2NP 消息，仅加密 UDP 功能）。I2P同时使用TCP和UDP传输，对于某些深度包检测（DPI）设备来说，UDP可能更难以跟踪。

6 Tor和I2P的威胁模型

威胁模型分析 （thread modeling）是寻找系统潜在威胁以建立对抗的策略，以建立安全的系统。Tor 项目没有指定明确的威胁模型，仅仅讨论常见的攻击和针对它们的现有防御措施。I2P指定了明确的威胁模型，并且针对这些威胁建立了对抗策略[18,19]。综合Tor和I2P的攻击类型和威胁模型，表10对Tor和I2P的威胁类型进行了比较，比较表明，I2P的安全性设计高于Tor。

表10　Tor与I2P比较：威胁类型

威胁类型	Tor	I2P
概率模型分析	数学模型的安全性和匿名性测量	数学模型的安全性和匿名性测量
DoS攻击	目录服务器、入口节点	NetDB、Floodfill路由器、入口网站
流量分析	出口节点	规模小，流量特征容易识别

威胁类型	Tor	I2P
时间攻击	入口/出口节点时间相关性	无固定的入口/出口节点，但应用程序的消息频率具有可识别模式
合谋攻击	植入大量受控节点	植入大量蜜罐节点
Sybil攻击	伪造大量洋葱路由器	密钥空间中创建大量填充路由器
局部视图攻击	用户并不能得到全局节点	控制网络中有限数量的对等体
全局攻击	监听或控制Tor网络上所有节点（包括目录服务器）	向I2P目的地发送5GB并监控每个人的网络连接
交叉口攻击	同时在电路的两端，定期与目标进行联系，并跟踪网络上的对等体	同时在隧道的两端，定期与目标进行联系，并跟踪网络上的对等体
协议漏洞	身份认证协议、桥接服务	随机选择算法、DHE /ECDHE 算法

7 结束语

Tor是目前最受欢迎和最常用的系统，但I2P是一个快速增长的竞争对手。Tor 致力于提供高速匿名互联网外包，而I2P本身则致力于提供分散的弹性网络。这两个系统都在不断更新，以提高性能并提供更好的匿名性，同时防止恶意攻击。

两个网络的关键区别在于它们在节点选择和客户端节点参与方面设置、使用其虚拟连接的方式。另一个重要的区别是，虽然Tor是为退出流量而设计的，但I2P寻求在网络内部提供服务，以便为服务提供商和用户提供更强的匿名性。

比较研究表明，确定Tor / I2P这两个系统在性能和匿名性方面哪个提供了更好的服务，与其应用领域密切相关：在浏览公共网络时， Tor能够提供更好的性能，而I2P几乎无法使用。另外，与 Tor 在与网络内的服务或用户交互时相比，I2P提供了更强的匿名性和更好的性能。总之，无论使用哪种系统，只能在性能和匿名性之间进行权衡。

The authors have declared that no competing interests exist.

作者已声明无竞争性利益关系。

参考文献 View Option

[9] CONTI M , CRANE S , FRASSETTO T ,et al.
Selfrando:securing the Tor browser against de-anonymization exploits
[J]. Proceedings on Privacy Enhancing Technologies, 2016(4): 454-459.
[本文引用: 1]

[10] CONRAD B , SHIRAZI F .
A survey on Tor and I2P
[C]// The 9th International Conference on Internet Monitoring and Protection (ICIMP 2014). 2014.
[本文引用: 1]

[11] TIMPANARO J P , CHOLEZ T , CHRISMENT I ,et al.
Evaluation of the anonymous I2P network's design choices against performance and security
[C]// The 1st International Conference on Information Systems Security and Privacy(ICISSP 2015). 2015: 46-55.
[本文引用: 1]

[12] ALI A , KHAN M , SADDIQUE M ,et al.
TOR vs I2P:a comparative Study
[C]// 2016 IEEE International Conference on Industrial Technology (ICIT). 2016.
[本文引用: 1]

[13] TIMPANARO J P , CHOLEZ T , CHRISMENT I ,et al.
Evaluation of the anonymous I2P network's design choices against performance and security
[C]// The 1st International Conference on Information Systems Security and Privacy (ICISSP 2015). 2015: 46-55.
[本文引用: 1]

[14] KARTHIGEYAN A , ROBINSON J M , MANIKANDAN S P ,et al.
A comprehensive behavior analysis of Tor versus I2P

[C]// International Journal of Applied Engineering Research, 2014,9(20): 7333-7345.
[本文引用: 1]

[15] HERMANN M .
Privacy-implications of performance-based peer selection by onion-routers:a real-world case study using I2P
[D]. TU-Munich, 2011.
[本文引用: 1]

[16] HERRMANN M , CHRISTIAN G .
Privacy implications of performance-based peer selection by onion routers:a real-world case study using I2P
[C]// 11th Privacy Enhancing Technologies Symposium (PETS 2011). 2011.
[本文引用: 1]

[17] KARTHIGEYAN A , ROBINSON J M , MANIKANDAN S P ,et al.
A comprehensive behavior analysis of Tor versus I2P
[J]. International Journal of Applied Engineering Research, 2014,9(20): 7333-7345.
[本文引用: 1]

[18] JEONG S H , .
A longitudinal analysis of I2P leakage in the public DNS infrastructure
[C]// 2016 Conference on ACM SIGCOMM. 2016: 557-558.
[本文引用: 1]

[1] SHAHBAR K , ZINCIR-HEYWOOD A N .
Weighted factors for measuring anonymity services:a case study on Tor,jondonym,and I2P
[R]. 2017.
[本文引用: 1]

[2] ZHOU Y W , YANG Q L , YANG B ,et al.
A Tor anonymous communication system with security enhancements
[J]. Journal of Computer Research and Development, 2014,51(7): 1538-1546.

[本文引用: 1]

[3] CONRAD B , SHIRAZI F .
A survey on Tor and I2P
[C]// The 9th International Conference on Internet Monitoring and Protection (ICIMP 2014). 2014.
[本文引用: 1]

[4] GAO J J .
Optimization and implementation of I2P anonymous communication system
[D]. Beijing:Peking University, 2014.
[本文引用: 1]

[5] TIMPANARO J P , CHOLEZ T , CHRISMENT I ,et al.
Evaluation of the anonymous I2P network's design choices against performance and security
[C]// The 1st International Conference on Information Systems Security and Privacy (ICISSP 2015). 2015: 46-55.
[本文引用: 1]

[6] ZHOU Y .
Research on anymous communication based on Tor
[D]. Xian:Xidian University,2013, 10.
[本文引用: 1]

[7] HUANG W J .
Uniform distribution routing algorithm based on Tor network
[D]. Shanghai:Shanghai Jiaotong University, 2012.
[本文引用: 1]

[8] LI J S .
Research on the Analysis of I2P anonymous communication protocol and flow identification
[D]. School of Computer Science ＆Engineering, 2015.
[本文引用: 1]

[19] SHAHBAR K .
Analysis of multilayer-encryption anonymity networks
[D]. Canada:Dalhousie University, 2017.
[本文引用: 1]

地址：北京市丰台区东铁匠营街道顺八条1号院B座“北阳晨光大厦”2层　邮编：100079
电话：010-53879136/53879138/53879139　电子邮件：cjnis@bjxintong.com