Computer Science and Application 计算机科学与应用, 2019, 9(7), 1296-1308
Published Online July 2019 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2019.97146

Hans汉斯

Research on Key Technologies of Anonymous Network Tor and I2P

Haizhou Wei, Lingyan Li, Yun Yang*

College of Information Engineering, Yangzhou University, Yangzhou Jiangsu
Email: *yyang@yzu.edu.cn

Received: Jun. 30th, 2019; accepted: Jul. 10th, 2019; published: Jul. 17th, 2019

Abstract

Multi-layered encrypted anonymous networks are designed to provide anonymous and hidden services to users by separating users from their final destination. Tor (The Onion Router) and I2P (Invisible Internet Project) are multi-layer encrypted anonymous networks, which have been highly valued by academics and industry, and are also welcomed by users. However, due to the distinction in design concept between Tor and I2P, there are obvious differences in the key technologies of the network. These differences are mainly reflected in the network architecture, network management, interface technology, switching technology, routing technology, password specification, node selection and discovery. Through the comparative analysis and research on the key technologies of Tor and I2P, the working principle of Tor and I2P networks can be comprehensively understood, and the technical characteristics, anonymity and security problems of the two kinds of networks can be understood as well, so as to lay a foundation for the research on Tor and I2P's de-anonymity and network measurement.

Keywords

Anonymous Network, Tor, I2P, Onion Routing, Garlic Routing

匿名网络Tor与I2P关键技术研究

魏海洲，李凌燕，杨　云*

扬州大学信息工程学院，江苏　扬州
Email: *yyang@yzu.edu.cn

收稿日期：2019年6月30日；录用日期：2019年7月10日；发布日期：2019年7月17日

摘　要

多层加密匿名网络旨在通过将用户与其最终目的地分离来为用户提供匿名和隐藏服务，Tor (The Onion

*通讯作者。

文章引用: 魏海洲, 李凌燕, 杨云. 匿名网络 Tor 与 I2P 关键技术研究[J]. 计算机科学与应用, 2019, 9(7): 1296-1308.
DOI: 10.12677/csa.2019.97146

Router)和I2P (Invisible Internet project)都是多层加密匿名网络，目前已受到学术界、工业界的高度重视，也受到用户的欢迎。但Tor和I2P之间由于其设计理念上存在差别，因此其网络关键技术存在明显差异，这些差异主要体现在网络体系结构、网络管理、接口技术、交换技术、路由技术、密码规格、节点选择与发现等方面。通过对匿名网络Tor、I2P的关键技术进行比较分析和研究，可以全面理解Tor和I2P网络的工作原理，了解两种网络各自的技术特点和匿名性与安全性上存在的问题，为Tor和I2P的去匿名化和网络测量等研究奠定基础。

关键词

匿名网络，Tor，I2P，洋葱路由，大蒜路由

Copyright © 2019 by author(s) and Hans Publishers Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY).
http://creativecommons.org/licenses/by/4.0/
Open Access

1. 引言

随着 Internet 应用的发展，匿名通信技术在保护个人隐私方面发挥着非常重要的作用。匿名通信的目的是隐藏每个最终用户的机密信息，包括身份和内容，并避免被第三方观察和发现。但是，对于匿名通信系统，匿名和通信效率一直是一种权衡。通常，系统具有更好的匿名性，通信效率越差。这是因为匿名增强通常伴随着通信过程的复杂性，这也将导致通信效率的降低。因此，如何满足不同用户的个性化需求已成为匿名通信系统的热门话题。

匿名网络通过将其数据中继到多个匿名节点，每个节点修改、填充和转发数据包，使得消息通过从发送者到接收者的若干节点，以便匿名地到达最终目的地来为用户提供隐私，通过多层加密用于保护用户的隐私免受攻击，从而实现对身份和通信关系的保护。Tor 和 I2P 是匿名网络的典型代表，它们允许用户访问不同的服务，同时保留其在线匿名性，其中用户的真实身份与其指定系统的身份分离。

Tor 和 I2P 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的互联网服务。因此，Tor 是一个“覆盖网络”，而 I2P 是一个“虚拟互联网”。

2. Tor 和 I2P 网络

Tor 和 I2P 网络有相似之处和不同之处[1]。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[2]。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，用户将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而不同。两种匿名服务的路由技术和路径选择也不同。

2.1. Tor 和 I2P 的匿名

作为最受欢迎的匿名通信系统 Tor 和 I2P，通过其加密和通信方案提供强大的匿名性[3]。

基于电路的通信是 Tor 匿名的核心[4]，其中 Tor 用户(Tor 节点)的身份与 Tor 应用程序的身份分离。

Tor 匿名是基于“集中式目录”、“全双工电路”、“洋葱路由”，隐私保护是通过“消息”、“电路交换”而实现的，密码规格使用流密码(AES128)、公钥密码(RSA1024，固定指数 65537)、Diffie-Hellman 协议(1024 位安全素数)和散列函数(SHA1)。Tor 支持两种操作模式：第一种操作模式“Web 代理”或“Service proxy”，它允许与非 Tor 启用的系统(普通的 Internet)进行传统通信；第二种操作模式称为“隐藏服务”，它消除了与普通 Internet 的传统通信，Tor 确保传输到网络中的数据永远不会离开混合，这意味着只能访问参与此类网络的服务，并且 Tor 内的用户对于 TCP/IP 的 2~4 层上可用的信息完全是匿名的[5]。

基于隧道的通信是 I2P 匿名的核心[4]，I2P 的匿名性在于将用户的身份(由路由器信息提供)与其正在运行的应用程序(由其租赁集提供)分离。通过“分布式目录”、“单向隧道”、“大蒜路由”、“细胞”、“分组交换”而实现匿名和隐私保护，密码规格使用流密码(AES256-CBC)、公钥密码(ElGamal2048，DSA1024)、Diffie-Hellman 协议(2048 位安全素数)和散列函数(SHA256)。由于 I2P 网络可以集成各种应用程序，同时可以匿名的提供全部典型的 Internet 应用，所以 I2P 只提供“隐藏服务”一种操作模式[6]。I2P 也可以通过“out proxies”提供对公共互联网的直接访问，该功能由各种内部服务提供，主要目的是代理访问其他匿名系统。

Tor、I2P 的域名、节点和路由器采用了与位置无关的标识符(服务描述符－隐藏服务)加密密钥标识。

1) 域名生成算法步骤如图 1 所示。

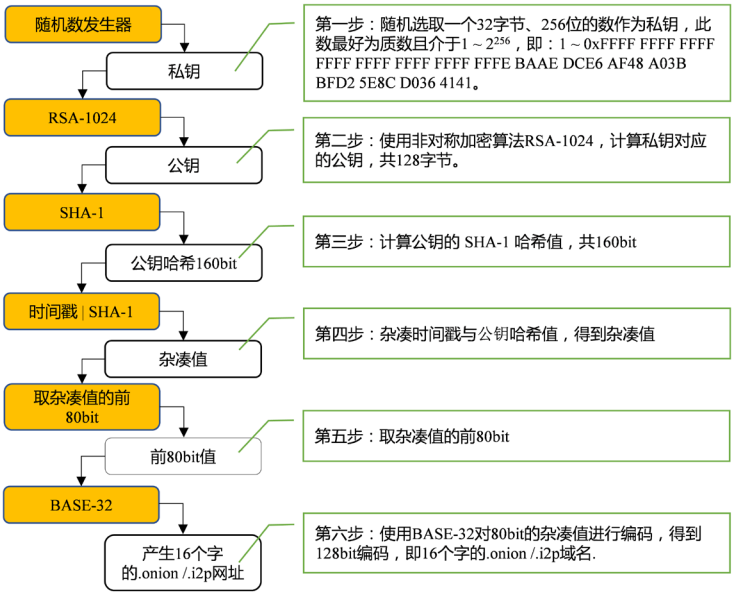


Figure 1. Algorithm process of anonymous domain generation
图 1. 匿名域名生成算法流程

由于域名是公钥的一部分，保证了网站的匿名性和安全性，可以提供隐藏服务。

2) I2P 中的节点标识符、路由标识符计算公式为：NetDB 中的节点标识符 Node_ID=SHA1(IP Number) || Random，路由标识符 Routing_id = SHA256(Node_ID || 时间戳)。

Node ID 和 Route ID 的生成算法关键程序如下：

```
public void ipDeal(ip){
    if(ipv4){
    long=iptolong(ipv4);
    binStr=ip.toBinaryString(long);
```

```
        randStr=rand.generateString(128);
        }else if(ipv6){
            big=ipv6toInt(ip);
            binStr=big.toString(2);
            randStr=rand.generateString(32);
         }
         result=binStr.concat(randStr);
         sha1=DigestUtils.sha1Hex(result);
  Str=result.concat(timestamp);
         sha256=DigestUtils.sha256Hex(Str)
}
```

在生成 Node ID 的时候，首先将 IP 地址(IPv4 或 IPv6)转化为十进制数，然后再转化为二进制数，当得到的二进制数不足 32 位(或 128 位)时，在二进制数的左边补 0，然后与用随机数发生器产生 128 位(或 32 位)的随机数“凑合”，再采用 SHA1 生成 160 位的 Node ID；再将 Node ID 与时间戳“凑合”，采用 SHA256 加密得到 Route ID。

在创建 Node ID 和 Route ID 时，由于 Node ID 为 160 位，Route ID 的位数为 256 位，160 位的 Node ID 与时间戳、随机数发生器产生的随机数“凑合”，组成 256 位的 Route ID，这样保证了路由器 IP 地址的匿名性和动态性，同时增加了攻击者的难度。

2.2. Tor 和 I2P 的体系结构

1) Tor 系统架构和协议层次

Tor 是用 C 语言编写的匿名 P2P 网络的多应用程序，图 2 表示了 Tor 网络体系结构、协议层次模型。

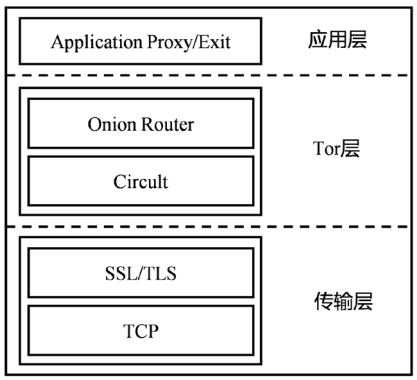


Figure 2. Tor protocol hierarchy model
图 2. Tor 协议层次模型

在图 2 中，Tor 层是 Tor 网络的关键部分，由 Tor 路由节点建立通信电路，可以将其看作为代理服务器，是它将客户端数据传输到网络中，并从网络中获取服务器端数据。应用层主要有应用代理和退出的连接功能；Tor 协议层主要有洋葱路由、电路创建协议；传输层有 TCP、SSL/TLS 协议，TLS 的主要功能是用于电路的加密。

2) I2P 系统架构和协议层次

I2P 是用 Java 编写的匿名 P2P 网络的多应用程序框架[12]，图 3 概述了 I2P 架构、I2P 协议层次模型。

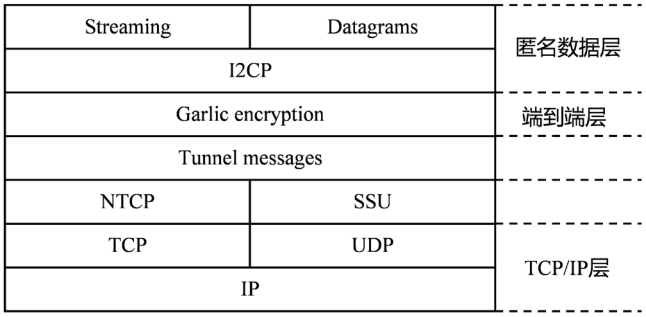


Figure 3. I2P protocol hierarchy model
图 3. I2P 协议层次模型

I2P 框架的核心是 I2P 路由器，它是 I2P 协议的关键组件。I2P 是围绕所谓的 I2P 路由器构建的应用程序框架(或中间件层)，路由器是一个在主机上运行的软件组件，为本地 I2P 应用程序提供连接，应用程序可以访问隐藏服务(作为客户端)，也可以托管服务(作为服务器)。应用程序之间的连接通过完全分散的对等网络实现，该网络作为 IP 上的覆盖层运行。应用程序可以使用称为 NTCP 的类 TCP 协议，也可以使用称为 SSU 的类 UDP 协议，路由器将这些连接映射到基于数据包的 I2P 隧道，这些 I2P 隧道使用标准大蒜路由提供匿名性，隧道由链中最外层的对等体和唯一的 Tunnel ID 标识。

3) Tor 和 I2P 架构比较

Tor 和 I2P 架构体现了两个匿名网络的设计理念差别，Tor 允许匿名访问分别实施和操作外部的互联网服务，解决“匿名性”和“隐藏服务”，侧重应用层设计，构建了一个“覆盖网络”。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，提供匿名文件共享和匿名网络托管，解决“匿名性”、“隐藏服务”和“安全性”，侧重网络层设计，构建了一个“虚拟互联网”[7]。

2.3. 工作流程

1) Tor 工作流程

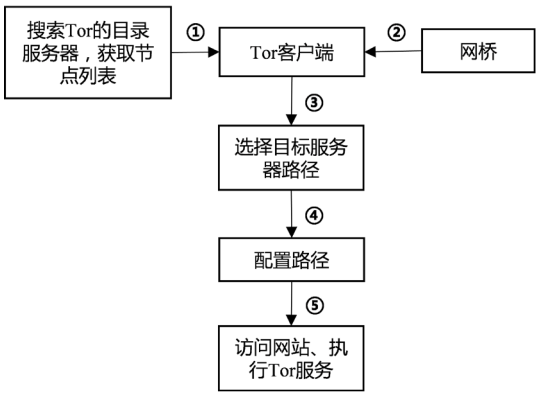


Figure 4. Tor network workflow
图 4. Tor 网络工作流程

图 4 说明了 Tor 网络的工作流程，用户可以通过搜索 Tor 目录服务器或网桥登录 Tor 网络。

2) I2P 工作流程

图 5 说明了 I2P 网络的工作流程，用户可以通过搜索 I2P NetDB 的路由器联系信息和目的地联系信息登录 I2P 网络。

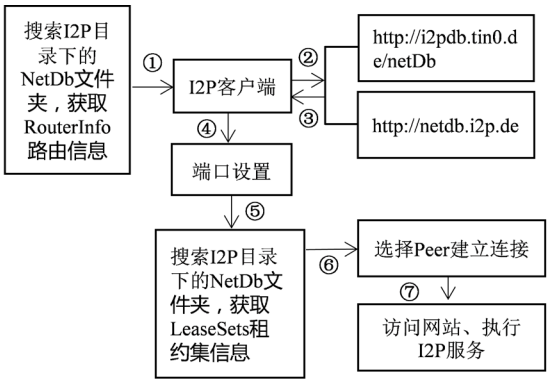


Figure 5. I2P network workflow
图 5. I2P 网络工作流程

由图 4、图 5 的工作流程对比可以看出，Tor 围绕可信赖的权威服务器构建进行集中式设计。这些服务器中的每一个都跟踪网络中的所有节点及其性能。权限服务器定期发布此列表供客户端使用。客户端从此列表中选择节点以创建加密隧道，直到它们到达出口节点。然后，这些出口节点充当代理，允许 Tor 用户访问公共 Internet (称为 clearnet)，而不会泄露其身份。由于只有少数可信任的授权服务器，因此这些节点的完整性对整个网络至关重要，使其成为攻击的重要目标。此外，由于所有权威机构都需要跟踪整个网络并定期就其状态达成一致，因此该设计的可扩展性有限。

用户使用 I2P 时，首先访问分布式数据库 NetDB，NetDB 保留两种类型的记录：路由器联系信息和目的地联系信息，路由器联系信息存储在 RouterInfo 结构中，该结构包含到达对等方所需的信息：路由器标识、IP 地址、端口、公钥等。leaseSets 结构中存储目的地信息，该结构包含：隧道网关路由器标识符、域名标识符、公钥等。如果应用程序想要访问 I2P 服务，首先需要找到该服务，它要求路由器提供服务信息，路由器可以在本地存储该服务信息并且能够立即将其返回给应用程序。

3. Tor 与 I2P 的关键技术

由于 Tor 与 I2P 在开发理念不完全相同，因此两个网络在一些网络关键技术上存在差异[8] [9]，表 1 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。

Table 1. Tor vs I2P: key technologies
表 1. Tor 和 I2P 比较：关键技术

技术	Tor	I2P
端口	SOCKS	I2P API
电路/隧道配置	三跳电路	用户可随机配置隧道数
单向/双向	双向电路	单向隧道
对等体选择	基于带宽的对等体选择	基于性能的对等体选择
目录服务器	7 个完整数据的目录服务器	分布式 DHT(NetDB)
端到端加密	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
退出节点/隐藏服务	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
隐藏服务提供方式	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
数据交换	电路交换	分组交换
数据传输	仅通过 TCP 传输	通过 TCP 和 UDP 传输
系统实现	在 C 中实施	在 Java 中实施

3.1. 接口技术

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，这表明，采用 SOCKS 的应用程序无需任何更改，可以直接使用。另一方面，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地调整。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，这可以使 I2P 在使用某些应用程序时提供更好的性能。

Tor 主要是为匿名访问公共互联网而设计的，因此它设计了许多退出节点和代理，而 I2P 网络的核心设计目标是允许匿名托管服务(隐藏服务)，并不是专注于匿名访问公共互联网。I2P 可以通过“out proxies”提供对公共互联网的直接访问，但该功能由各种内部服务提供，以代理到其他匿名系统[10]。

I2P API 专为匿名和安全而设计，而 SOCKS 专为功能而设计。在 I2P 中，确保总安全性不会检测到客户端活动。

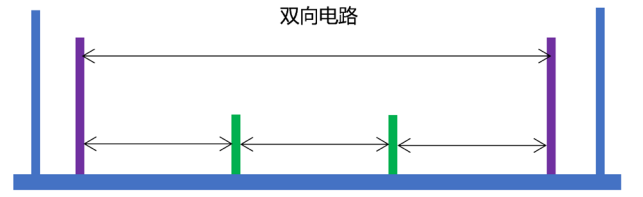
Tor 使用 SOCKS 有两个缺点：

1) 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，这可以使 I2P 在使用某些应用程序时提供更好的性能。

2) 应用程序发送的消息可能仍包含可识别发件人的信息。为了防止这种情况，需要使用具有过滤功能的应用程序级代理 Privoxy。

3.2. 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 6 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 7 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。

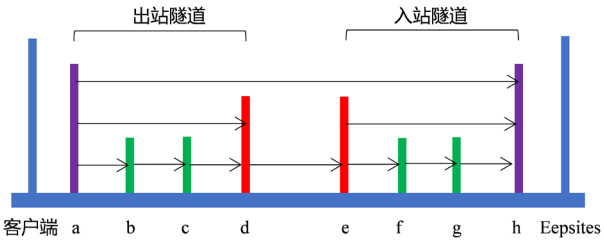


端到出口端加密 {RSA1024+AES256}	客户端 - d	电路加密 {私钥AES256}	a - d
洋葱加密 {RSA1024+AES256}	a - d	传输加密 {DHE+AES256}	a - b, b - c, c - d

Figure 6. Tor circuit
图 6. Tor 的电路

基于电路或隧道的通信是 Tor 或 I2P 匿名的核心，其中 I2P 用户(I2P 路由器)的身份与 I2P 应用程序的身份分离。从匿名的角度看，I2P 的单工隧道暴露的流量数据，是 Tor 的双工电路暴露的一半，而在 I2P 中，构成请求的数据包将通过一个或多个出站隧道传出，构成响应的数据包将通过一个或多个不同的入站隧道返回。

Tor 依靠志愿者提供的服务器来构建电路，但 I2P 使用具有足够性能特征的对等体参与网络来构建隧道。从技术角度来看，由于具有更好的内存管理和低客户端带宽开销，Tor 显得更高效，但在 I2P 中实现了性能排名机制、允许分析节点的实际性能等，I2P 服务比 Tor 中的隐藏服务更快。



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

Figure 7. I2P tunnel
图 7. I2P 的隧道

在 Tor 中，由于缺少覆盖流量，攻击者可能会使用流量分析和定时攻击来监控流量模式，跟踪消息流并识别通信方。I2P 隧道中的跳数在 0 到 7 之间变化，其中隧道中的更多跳数会增加匿名性，但因为数据需要遍历更多中间节点会降低性能[11]。

3.3. 对等体选择

Tor 和 I2P 都运行特定的节点选择算法，以提高性能并防范攻击者。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。对等体选择的目的是快速地构建电路或隧道[12]。

在 Tor 网络中，它的目录服务器使用有源带宽探测来测量和记录每个 OR (Onion Routers)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)。

在 I2P 网络中，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，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。

由于 Tor 在选择 OR 时仅考虑带宽，而忽略其他属性(如 OR 的实际位置、时延)，这可能导致高延迟和网络的负载不均衡，现有资源可能无法得到最佳利用。在 I2P 中，由于隧道的生命周期较短，一些 I2P 用户很可能会使用一个或多个损坏的对等体来构建隧道，快速响应故障节点的这种行为存在安全问题，同时，I2P 在选择对等体时也不考虑 I2P 对等体的位置，这会导致高时延，所构建的隧道也不是最佳的。

3.4. Tor 目录服务器与 I2P NetDB

Tor 和 I2P 的主要区别在于两个网络如何管理参与者。Tor 和 I2P 都使用目录来存储网络元数据，即：维护网络运行所需的元数据(参与者或应用程序的信息、部署在网络中的服务) [10] [13]。

Tor 使用中央服务器目录协调其 Tor 节点，该目录包含每个列出的 OR (Onion Router)的路由器描述符和网络状态文档，每个 OR 还维护两个密钥：一个长期身份密钥，用于签署 TLS 证书、路由器描述符和目录；一个短期的洋葱密钥，用于解密用户建立电路的请求并协商短期对称密钥。路由器描述符唯一地标识每个 OR(Onion Router)并包含要联系的所有相关数据：公钥、IP 地址、带宽、退出策略等，网络状态文档包含 OR 的测量带宽，提供网络的整体视图和统计检索。

I2P 网络使用分布式目录协调其 I2P 路由器，基于分布式 Kademlia 数据库和用于对等选择的对等分析算法，构建具有自组织的网络数据库 NetDB，协调和存储所有系统元数据。I2P 的 NetDB 存储由 Leasesets

和 Routerinfos 组成的网络元数据，它是一个分布式哈希表，由填充节点组成。由于 Floodfill 节点是具有高带宽速率的普通 I2P 路由器，因此 NetDB 不是由整个网络构成的，而是仅由所有 I2P 路由器的子集构成。有关 I2P 路由器的信息收集在称为 Routerinfo 的结构中，该数据结构保存该特定 I2P 路由器的所有联系信息。I2P 应用程序不是通过普通的 ＜IP 地址，端口号 ＞ 元组来识别，而是通过与位置无关的标识符(称为 I2P 目标)来识别。I2P 目的地连同一组加密密钥(用于将加密数据发送到应用程序)、签名密钥和用于接收数据的网关列表收集在称为 Leaseset 的结构中。I2P 路由器由 Routerinfo 标识，而 I2P 应用程序由租赁集 Leaseset 标识。

集中式架构存在单点故障的风险，I2P 使用分布式哈希表(DHT)，每个对等方负责分析其他路由器，以确定如何最好地利用可用资源，分布式组件可以加强网络并使其更有弹性，同时分布式架构系统消除了单点故障风险。

3.5. 路由方法

由图 8、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。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，用户将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[14]。

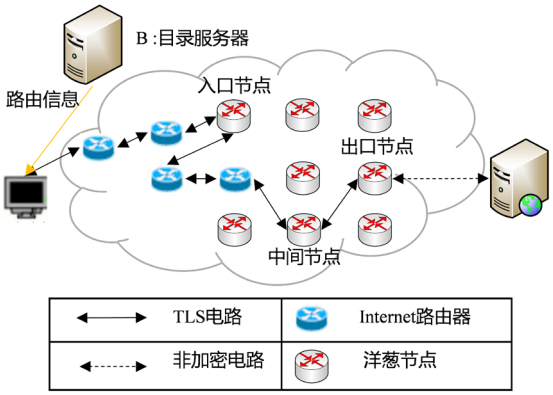


Figure 8. Onion routing
图 8. 洋葱路由

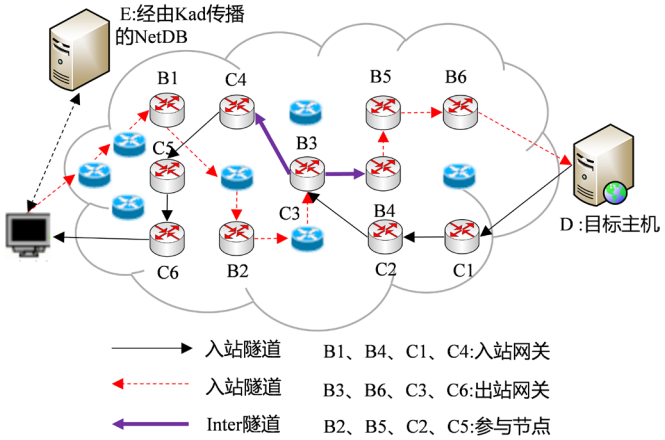


Figure 9. Garlic routing
图 9. 大蒜路由

洋葱路由的目的是让对手更难以进行流量分析，同时首先要保护两个与第三方相互认识的参与者的不可链接性，其次是保护身份。由图 8 可知，只有电路中的第一个 OR 知道客户端的 IP 地址，并且只有电路的最后一个 OR 知道消息的接收者，所有中间 OR 只知道它的前身及其后继者，甚至不知道哪些其他 OR 正在参与电路，通过三个节点间的双向电路构成网络。由于缺少覆盖流量，攻击者可能会使用流量分析和定时攻击来监控流量模式，跟踪消息流并识别通信方。

大蒜路由是洋葱路由的扩展，消息通过使用分层加密的几个中间节点，从其始发者路由到最终端点。由图 9 可知，通过单向隧道将 I2P 路由器连接起来，每个隧道由网关(入口点)，一组参与者(中间节点)和一个端点组成，隧道中的 I2P 路由器均不知道客户端的 IP 地址和消息的接收者，构成输入隧道和输出隧道的 I2P 路由器至少有 6 个。由于所有的 I2P 流量均在网络内部，因此 I2P 具有很强的匿名性和对抗“流量分析”、“Sybil 攻击”的能力。

大蒜路由与洋葱路由非常相似，但其技术上存在一些差异。一是大蒜路由中，可以聚合多条消息，二是大蒜路由中隧道是单向的。

I2P 中的大蒜路由主要采用三个不同的阶段：一是通过单向隧道构建路由(分层加密)；二是对于消息进行捆绑，通过分组交换，确定端到端消息传递的成功或失败；三是用于发布一些网络数据库 NetDB 条目，进行数据库维护。

3.6. 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的是固定长度的 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 字节数据。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)，包含了一个 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。

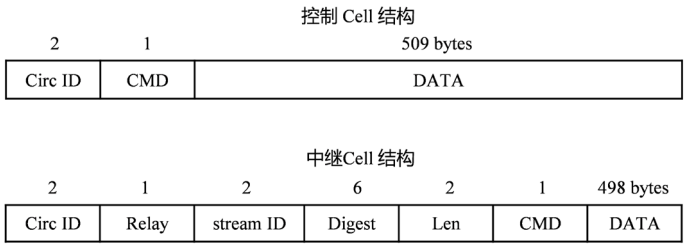


Figure 10. Cell structure of the tor network
图 10. Tor 网络的 Cell 结构

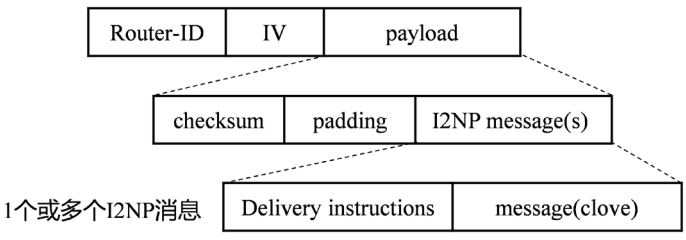


Figure 11. Message structure of the I2P network
图 11. I2P 网络的 message 结构

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

将其组合成所谓的隧道消息。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”)。

同一个连接中的指令与数据，在Tor中沿着通过TCP协议建立的电路(Ciruit)流动至目的节点，而在I2P中，连接被消息机制(Message)打散为数据包，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。

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(使得两个1024字节的消息与一个2048字节的消息无法区分)，所以外部攻击者也无法访问消息。

虽然Tor和I2P都使用分层和有序路径(隧道和电路/流)，Tor是一个电路交换网络，但I2P是一个分组交换网络，允许I2P透明地路由拥塞或其他网络故障、操作冗余路径，并跨可用资源负载平衡数据[14]。

3.7. 退出节点和隐藏服务

Tor网络中有许多退出节点，针对具有大量出口路由器的出口流量进行了优化和设计，主要原因是由于其设计理念决定的：Tor主要致力于为用户提供匿名访问网络以外的(Internet)网站，同时还在Tor网络中托管了网站(隐藏服务)。

但在I2P中，只有少数Outproxies (Tor术语中的退出节点)作为标准Internet的网关运行，这主要也是I2P网络设计理念决定的：I2P专为I2P网络内的匿名通信而设计，I2P提供多种应用程序，同时也在I2P网络中托管了部分网站(隐藏服务)，所提供的服务几乎覆盖了整个Internet，所以它的代理很少。

当使用实时交互式服务时，Tor和I2P都试图提供具有低延迟的强匿名性。由于Tor与I2P相比具有更多的退出节点，这些退出节点易于受到攻击，因此其安全性较差。

Tor与I2P都构建了匿名服务，I2P现有的应用几乎包括了绝大部分典型的因特网应用，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，Tor的规范用法是访问外部服务[15]，而I2P规范用法是访问内部服务[16]。

3.8. 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协议的，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。

I2P能够使用TCP以及不可靠的UDP进行传输，因此，I2P会话的设置速度比Tor隐藏的服务会话更快，并且具有更低的延迟[17]。

4. 结束语

匿名网络I2P是基于Tor的，它们之间有许多相似之处：基于TCP/IP的覆盖网络、提供低延迟匿名

服务、三层加密消息、大蒜路由是洋葱路由的变种、密码规格基本相同等，但由于它们设计理念存在本质差异，同时针对 Tor 存在的安全问题，I2P 在匿名性、隐私性、安全性、隐藏服务等方面进行了扩展或升级[18]：分布式网络数据库代替了集中式目录服务器，克服了网络单点故障隐患，可扩展性好；单向隧道代替了双向电路，匿名性更强；分组交换代替了电路交换，更好地平衡网络中的数据，有助于避免拥塞和服务中断；消息(消息捆绑)代替了细胞，可有效对付流量分析攻击；大蒜路由代替了洋葱路由，提高了匿名性和安全性；完全的端到端通信代替了局部的端到端通信，提高了通信的整体安全性；同时支持 TCP 和 UDP 传输代替了单一的 TCP 传输，提高了会话速度；很少的代理和出口节点代替了较多的代理和出口节点，网络流量保持在网络内部，有效地防止流量分析攻击和 DoS 攻击；按性能的路由器选择代替了按带宽的节点选择，可以有效地利用网络资源；ElGamal1024/SHA256/DHE/BASE64 的分层加密代替了 RSA1024/SHA1/AES/BASE32 的分层加密，提高了数据传输和隐藏服务的安全性、用户的匿名性；允许匿名托管服务代替了匿名访问互联网，减少了出口节点，保护用户和网络的安全。

I2P 受到与 Tor 相似的威胁，虽然 I2P 网络根据“威胁模型”，对 DoS 攻击、流量分析、时间攻击等威胁进行了防御设计，但是针对 I2P 网络的攻击依然层出不穷。

LIN YE [19]、C. Egger [20]、Juan Pablo Timpana-ro 等人[21] [22]的研究表明，I2P 的隐藏服务面临去匿名化风险、分布式哈希表(DHT)的 NetDB 存在安全隐患等，I2P 还需要进一步提高健壮性、可扩展性、匿名性和安全性。

基金项目

国家自然科学基金(No. 61872312)、江苏省产学研前瞻性联合项目(BY2016069-16)。

参考文献

[1] 周彦伟, 杨启良, 杨波, 吴振强. 一种安全性增强的 Tor 匿名通信系统[J]. 计算机研究与发展, 2014, 51(7): 1538-1546.

[2] 高俊杰. I2P 匿名通信系统优化与实现[D]: [硕士学位论文]. 北京: 北京大学, 2014.

[3] Montieri, A., Ciuonzo, D., Aceto, G. and Pescapé, A. (2017) Anonymity Services Tor, I2P, JonDonym: Classifying in the Dark. 2017 29*th International Teletraffic Congress* (*ITC* 29), Genoa, 81-89.

[4] 周勇. 基于 Tor 的匿名通信研究[D]: [硕士学位论文]. 西安: 西安电子科技大学, 2013.

[5] 罗军舟, 杨明, 凌振, 吴文甲, 顾晓丹. 匿名通信与暗网研究综述[J]. 计算机研究与发展, 2019, 56(1): 103-130.

[6] Ali, A., Khan, M., Saddique, M., Pirzada, U., Zohaib, M., Ahmad, I. and Debnath, N. (2016) TORvs I2P: A Comparative Study. *Proceedings of the* 2016 *IEEE International Conference on Industrial Technology*, Taipei, 14-17 March 2016, 3.

[7] 王有文. 第二代洋葱路由匿名系统 Tor 的性能改进研究[D]: [硕士学位论文]. 北京: 北京邮电大学, 2017.

[8] Conrad, B. and Shirazi, F. (2014) A Survey on Tor and I2P. *ICIMP* 2014: *The Ninth International Conference on Internet Monitoring and Protection*, Paris, 20-24 July 2014, 20.

[9] Timpanaro, J.P., Cholez, T., Chrisment, I. and Festor, O. (2015) Evaluation of the Anonymous I2P Network's Design Choices against Performance and Security. *ICISSP* 2015-*Proceedings of the* 1*st International Conference on Information Systems Security and Privacy*, Angers, France, 9-11 February 2015, 46-55.

[10] Müller, J. (2016) Analysis of the I2P Network-Information Gathering and Attack Evaluations. Bachelors Thesis, Bern University of Applied Sciences, Bern, Biel, Burgdorf.

[11] Vashi, D. and Khilari, G. (2015) Performance Improvement in I2P Using SSL. *International Journal of Science*, *Engineering and Technology Research*, **4**, 1454-1456.

[12] Shahbar, K. (2017) Analysis of Multilayer-Encryption Anonymity Networks. Ph.D. Thesis, Dalhousie University Halifax, Nova Scotia.

[13] Biryukov, A., Pustogarov, I. and Weinmann, R.-P. (2013) Trawling for Tor Hidden Services: Detection, Measurement, Deanonymization. 2013 *IEEE Symposium on Security and Privacy*, Berkeley, CA, 19-22 May 2013, 80-94.

https://doi.org/10.1109/SP.2013.15

[14] Biryukov, A., Thill, F., Pustogarov, I. and Weinmann, R.-P. (2014) Content and Popularity Analysis of Tor Hidden Services. 2014 *IEEE* 34*th International Conference on Distributed Computing Systems Workshops*, Madrid, Spain, 30 June-3 July 2014, 188-193. https://doi.org/10.1109/ICDCSW.2014.20

[15] Casenove, M. and Miraglia, A. (2014) Botnet over Tor: The Illusion of Hiding. 2014 6*th International Conference on Cyber Conflict*, Tallinn, Estonia, 3-6 June 2014, 273-282. https://doi.org/10.1109/CYCON.2014.6916408

[16] Astolfi, F., Kroese, J. and Van Oorschot, J. (2015) I2P-The Invisible Internet Project. Media Technology, Leiden University Web Technology Report.

[17] Timpanaro, J.P., Cholez, T., Chrisment, I. and Festor, O. (2015) Evaluation of the Anonymous I2P Network's Design Choices against Performance and Security. 2015 *International Conference on Information Systems Security and Privacy*, Angers, France, 9-11 February 2015, 9.

[18] Karthigeyan, A., Robinson Joel, M., Manikandan, S.P., Raja Guru, P. and Raman, S. (2014) A Comprehensive Behavior Analysis of TOR versus I2P. *International Journal of Applied Engineering Research*, **9**, 73337345.

[19] Lin, Y., Yu, X.Z., Zhao, J., Zhan, D.Y., Du, X.J. and Guiz-Ani, M. (2018) Deciding Your Own Anonymity: User-Oriented Node Selection in I2P. *IEEE Access*, **6**, 71350-71359. https://doi.org/10.1109/ACCESS.2018.2881719

[20] Egger, C., Schlumberger, J., Kruegel, C. and Vigna, G. (2013) Practical Attacks against the I2P Network. In: Stolfo, S.J., Stavrou, A. and Wright, C.V., Eds., *Research in Attacks*, *Intrusions*, *and Defenses*. *RAID* 2013. *Lecture Notes in Computer Science*, Springer, Berlin, Heidelberg, 432-451. https://doi.org/10.1007/978-3-642-41284-4_22

[21] Timpanaro, J.P., Cholez, T., Chrisment, I. and Festor, O. (2015) Evaluation of the Anonymous I2PNetwork's Design Choices against Performance and Security. TELECOM Nancy Universite' de Lorraine INRIA/LORIA, France.

[22] Timpanaro, J.P., Chrisment, I. and Festor, O. (2011) Monitoring the I2P Network. https://hal.inria.fr/hal-00653136

Hans汉斯

知网检索的两种方式：

1. 打开知网首页：http://cnki.net/，点击页面中“外文资源总库 CNKI SCHOLAR”，跳转至：http://scholar.cnki.net/new，搜索框内直接输入文章标题，即可查询；
   或点击“高级检索”，下拉列表框选择：[ISSN]，输入期刊 ISSN：2161-8801，即可查询。
2. 通过知网首页 http://cnki.net/顶部“旧版入口”进入知网旧版：http://www.cnki.net/old/，左侧选择“国际文献总库”进入，搜索框直接输入文章标题，即可查询。

投稿请点击：http://www.hanspub.org/Submission.aspx
期刊邮箱：csa@hanspub.org