

网络层匿名通信协议综述

王良民, 倪晓铃, 赵蕙

(江苏大学计算机科学与通信工程学院, 江苏 镇江 212013)

摘 要: 匿名通信系统是一种建立在应用层之上结合利用数据转发、内容加密、流量混淆等多种隐私保护技术来隐藏通信实体关系和内容的覆盖网络。然而, 作为覆盖网络运行的匿名通信系统, 在性能和安全保障上的平衡问题上存在不足。未来互联网架构的出现使构建基于基础设施的匿名通信系统成为可能。此类匿名通信系统将匿名设计为网络基础设施服务, 通过为路由器配备加密操作, 可解决匿名网络的可拓展性和性能限制的部分问题, 因此也可称它们为网络层匿名通信协议。对现有的网络层匿名通信协议(LAP、Dovetail、Hornet、PHI和Taranet)进行了研究, 介绍了网络层匿名通信协议的分类标准, 简述其创新点和具体加密思想, 并对它们如何在安全性和性能二者之间的权衡进行分析, 也指出了这几种网络匿名通信协议的优势和不足, 最后提出在匿名通信系统发展的过程中所面临的挑战和需要深入研究的问题。

关键词: 匿名通信; 协议; 网络层; 综述

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2020006

Survey of network-layer anonymous communication protocols

WANG Liangmin, NI Xiaoling, ZHAO Hui

School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang 212013, China

Abstract: An anonymous communication system is an overlay network built on the application layer and combining various privacy protection technologies such as data forwarding, content encryption, and traffic obfuscation to hide communication relationships between entities and forwarded contents. However, there is a deficiency in the balance between performance and security as an anonymous communication system operating over an overlay network. With the advance of the future internet architectures, it is possible to build an infrastructure-based anonymous communication system. Such anonymous communication systems design anonymity as network infrastructure services and provide encryption operations for routers, which can solve the part problem of scalability and performance limitations of anonymous network. They can also be called network-layer anonymous communication protocols. The existing network-layer anonymous communication protocols (LAP, Dovetail, Hornet, PHI and Taranet) were studied.

收稿日期: 2019-07-01; 修回日期: 2019-09-02

通信作者: 王良民, wanglm@ujs.edu.cn

基金项目: 国家自然科学基金资助项目(No.U1736216)

Foundation Item: The National Natural Science Foundation of China (No.U1736216)

论文引用格式: 王良民, 倪晓铃, 赵蕙. 网络层匿名通信协议综述[J]. 网络与信息安全学报, 2020, 6(1): 11-26.

WANG L M, NI X L, ZHAO H. Survey of network-layer anonymous communication protocols[J]. Chinese Journal of Network and Information Security, 2020, 6(1): 11-26.

The classification standard of network-layer anonymous communication protocols were introduced. Its innovation point and specific encryption ideas were briefly described, and how to keep balance between security and performance was analyzed. The shortcomings and advantages of these kinds of network anonymous communication protocols were also pointed out. Finally, the challenges faced in the development of anonymous communication systems and the problems that need to be studied in depth were proposed.

Key words: anonymous communication, protocol, network-layer, survey

1 引言

互联网作为通信与信息传播的途径在快速发展的同时, 隐私保护成为当今互联网发展过程中一个至关重要的问题。国内外一些调查机构的研究结果表明: 用户越来越关注自身的隐私是否被泄露。随着加密技术的深入研究, 用户通信数据的安全性得到了加强, 但传统加密技术很难对通信参与者身份、行为、网络地址等隐私信息进行强有力的保护。同时在一些特殊的应用领域, 如电子医疗、电子投票等系统, 用户身份、行为和网络地址等隐私信息的保护程度是评估整个系统安全性能的重要因素之一^[1]。为了解决上述问题, 研究者们提出了保护用户隐私的匿名技术。

匿名是指将用户的身份、行为和网络地址等隐私信息隐藏在特定的匿名集合之中, 令网络窃听者和攻击者无法识别通信行为的具体发起者, 通信双方的身份以及具体的网络地址信息。匿名技术主要是通过对通信参与者身份和数据的匿名化, 以及网络地址的匿名化来保护个人隐私信息^[2-3]的安全性。匿名通信系统是指采用匿名技术来保护通信双方身份、行为和网络地址等隐私信息的通信系统^[4], 而有关如何保护用户匿名身份的研究也成为公钥密码学的一个重要分支^[5]。

目前, 匿名通信技术的发展已具有一定的研究基础。其中, 安全性较高的匿名通信方案是混合网络^[6-9], 它们可以提供高延迟的异步消息传递。另一种则是洋葱路由网络(如 Tor, the second-generation onion router^[10])。洋葱路由采用密码学相关技术实现了在计算机网络上进行匿名通信的目标。在洋葱路由的网络中, 消息被一层一层地加密包装成像洋葱结构一样的数据包, 并经由一系列被称作洋葱路由的网络节点进行转发, 每经过一个洋葱路由就可以将数据包的最外层解密, 以此类推, 当数据包到达目的地时将最

后一层解密, 目的地就能获得原始消息。因为经过这一系列的加密包装, 每一个网络节点(包括目的地)都只能知道其相邻节点, 但无法知道整个发送路径, 从而达成了匿名通信的目的。Tor 可以在安全性和性能之间提供平衡, 实现典型的互联网活动(如网页浏览、即时消息传递等)的低延迟匿名通信。但研究人员也发现由于洋葱路由网络易受各种流量分析攻击^[11-15], 所以洋葱路由网络提供的匿名等级不足。同时基于覆盖网络的设计也为 Tor 带来性能和拓展性方面的问题: 在性能方面, 覆盖网络的设计——使用每跳可靠的传输, 增加了传播和排队延迟; 在拓展性方面, Tor 的设计要求中间节点维持每个链接状态, 从而限制了可以同时发生的并发匿名链接总数。此外, 传统的匿名通信系统是基于应用层从而实现匿名通信的目的。研究者们认为匿名通信应该成为互联网的内置服务, 以保证个人言论自由, 进行隐私保护, 而不是仅通过可选的应用层服务提供匿名性^[16]。

近年来, 研究人员发现网络层匿名通信系统^[17-21], 即通过在网络层中构建匿名通信协议可部分地解决匿名网络的可拓展性和性能限制问题。在当今的互联网中, IP 是基本的 3 层协议。而 IP 地址存在于每个数据包中, 攻击者通过记录用户的 IP 地址可以唯一地识别它, 将该身份和用户的在线活动联系起来, 关联到不同的服务, 并部分地揭示它的地理和网络位置。所以网络层匿名通信协议在不泄露用户的第 3 层身份标识(IP 地址)的前提下进行匿名通信, 同时也不像 Tor 一样产生大量的延迟和包头开销。网络层匿名通信系统将匿名通信作为互联网和下一代网络架构中的网络基础设施的服务。和基于覆盖网络的现有匿名系统相比, 网络层匿名通信协议具有 3 个优点: 首先, 网络层匿名通信协议只涉及传输层之下的层, 消除了覆盖网络中上层的处理和过多

的排队延迟;其次,此类协议可以使用源与目的地之间的较短路径(而不是覆盖网络中重定向所建立的长路径),从而减少传播延迟;最后,路由器可以提供比现有自愿贡献的服务器更高的吞吐量,并可增加匿名通信的吞吐量。现有的网络层匿名通信协议有以下5个:LAP(lightweight anonymity and privacy)^[17]、Dovetail(stronger anonymity in next-generation internet routing)^[18]、PHI(path-hidden lightweight anonymity protocol at network layer)^[19]、Hornet(high-speed onion routing at the network layer)^[20]、Taranet(traffic-analysis resistant anonymity at the network layer)^[21]。根据它们在计算量和数据包包头开销方面的不同需求以及是否对数据包负载提供完整性保护的特性,可将它们划分为两类:网络层轻量级匿名通信协议(包括LAP、Dovetail和PHI)和网络层洋葱路由匿名通信协议(包括Hornet和Taranet)。

2 基于覆盖网络的匿名通信协议

2.1 基于覆盖的应用层匿名通信系统

匿名通信的相关研究开始于David关于Mix网络的提议^[22]:通过Mix的转接作用和对传送数据重新排序、延时和填充等淆乱手段隔断网络通信双方(或第三方)的逻辑联系,使信宿方(或第三方)获得只是信源身份的数据及Mix身份^[23]。自此,研究者们提出并部署了基于消息的Mix系统^[7-8,24-25]。这些系统通过使用昂贵的不对称原语、消息批处理和混合等技术可以承受主动攻击者和大部分的变节中继节点带来的威胁。由于它们会产生大量的计算开销并带来高延迟,适合于支持延迟容忍的应用如电子邮件等。但随着科技的进步,高延迟匿名系统并不能满足人们的更高要求。此后又提出了低延迟洋葱路由系统^[9,26-28]来有效地支持交互式流量。洋葱路由系统是由志愿者服务器组成的,它们自愿为其他服务器转发流量。它的思想是用户选择一组服务器来匿名地转发流量。在数据包转发的过程中,每个服务器可以独立地进行加/解密,防止攻击者通过观察关联出入口流量。此外,低延迟洋葱路由系统在数据包转发期间仅需要对称加密操作,并且避免使用导致延迟的批处理和混合技术。然而,低延迟洋葱

路由系统容易受到端到端的确认攻击,如时序攻击等,因此与Mix网络相比,它的匿名性保证较弱。为了实现强大的匿名性和良好的性能,研究者们继而提出了比原始洋葱路由网络具有更高的抗流量分析能力和性能更高的协议^[9]。综上所述,从基于覆盖的匿名系统的功能上来看,可分为低延迟洋葱路由系统和抵制流量分析的高延迟匿名系统。其中低延迟洋葱路由系统包括I2P^[29]、JonDO^[30]、Freedom^[26]、Tor^[9]。而抵制流量分析的匿名系统也可分为两类:Mix网络^[31-34]和DC(dining cryptographer)网络^[35-38]。虽然二者的思想和采用的抵制流量分析的方式不同,但其本质都是为了抵制流量分析并提供更高性能。

2.2 基于覆盖网络的匿名系统的主要问题(以Tor为例)

Tor是目前最流行的基于覆盖网络的低延迟洋葱路由匿名系统之一。它是一种基于电路的低延迟匿名通信服务,Tor网络的客户端基于加权随机的路由选择算法随机选取的中继节点构成了加密的通信链路,并引入完美的前向安全、拥塞控制、共享虚电路、分布式目录服务、端到端的完整性检测和可以配置的出口策略等机制,此外还加入了接收者匿名的实用设计,提高了Tor的匿名性和传输性能。Tor网络可以直接运行在现有的互联网架构上,运行时不需要特殊的权限,几乎不需要节点之间的同步或协调,并在匿名性、可用性和效率之间提供了合理的权衡。但其作为覆盖网络的设计存在性能和拓展性方面的问题。这样的覆盖系统试图使用通过间接路由传输的分层加密数据包来达成匿名通信的目的。但是,由于较长的端到端路径长度和间接通过3个Tor中继节点的加密操作都会使运行速度变慢,从而带来额外的延迟。Tor网络要求中间节点保持每个匿名连接的状态从而受到可拓展性限制的影响。除此以外,Tor也容易受到流量分析的影响^[39-42]。简言之,当前传统的匿名技术难以保障系统的绝对安全性,尤其是在低延迟匿名通信系统(如Tor)中,其难以抵抗在具有强攻击性的攻击者进行全局攻击时的外部攻击,而且在系统的通信过程中存在网络开销较大的缺陷,还不能保证为用户提供可靠并且高性能的匿名通信服务。目前已有研

gateway protocol)或者边界网关协议(BGP, border gateway protocol), 保证全网路由可达。

2) 为网络中的每个节点配置 Node-SID (Node-SID 可以单独表示一台设备, 而且全局有效并唯一), 并且通过 IGP 或者 BGP 进行扩散, 保证 Node ID 全网唯一, 且 Node ID 全网可达。

3) 生成 Adj-SID (Adj-SID 则是本地有效, 本地唯一标识一条链路), Adj-SID 可以通过手动配置生成, 也可以通过控制器进行分配。

4) 控制器向设备收集全网的拓扑和标签信息, 这些信息可以通过 IGP 或者 BGP 上报给控制器。

5) 如某应用向控制器请求, 要求网络提供一条带宽不低于 20 Mbit/s, 时延不高于 10 ms 的链路。控制器收到请求后将告诉 A 收到一条流量, 这条流量从 A 到 F 要求带宽 20 Mbit/s, 时延 10 ms 等。

6) A 向控制器请求路径计算, 由于控制器已经掌握了全网的拓扑和标签信息, 于是计算得知, C 到 F 的路径拥塞, 最优路径应该是 A-C-E-F。

7) 控制器给 A 下发标签栈, 标签栈为 (16001, 30002, 16002)。

8) A 收到标签栈后, 发现第一跳标签是 16001, 则根据路由将报文同时发往 B 和 D, B 和 D 收到后, 发现标签为 16001, 于是根据路由, 将报文发往 C。

9) C 收到报文后, 发现第一个标签是自身的标签, 则将标签弹出, 发现内层标签是 30002, 是自身的 Adj-SID, 于是将 30002 弹出, 并将报文发往 30002 对应的链路。

10) 当 E 收到该报文之后, 根据标签 16002 将报文发往 F, 这样整个流的转发完成。

同时下一代互联网架构, 如 NEBULA^[52]、Mobility First^[53]、XIA^[54]、SCION^[55-56]等网络架构的出现也使网络层匿名通信协议的实现成为可能。NEBULA 提供符合策略的路径, 并使每个路由器能够验证所携带数据的来源。MobilityFirst 专注于适应动态主机, 并实现可拓展的网络移动性。XIA 旨在提供灵活、可拓展的网络架构, 集成了内容, 服务或用户等备用一流主机的丰富寻址。SCION 提供隔离、路径控制、可拓展性以及

可获得性等特性。本文以 SCION 为例进行详细阐述。2019 年开始开发的 SCION 是一种路径感知网络架构, Hornet、PHI、Taranet 这几个项目都可以在 SCION 上首先获取到路径信息。多项新兴技术的出现, 如 segment routing 可支持采用路径感知架构作为互联网部署的可行性。它与传统的互联网架构之间的区别在于: 当前的网络架构是假设数据包将被发送到预期的目的地, 传输层的一些协议的目的也是保证传输的可靠性, 但新型的网络架构是将路径感知加入到网络架构中, 这样的网络体系结构使端点可以获得有关路径及其属性的信息。然后, 这些端点可以使用该信息来选择给定目的地、流甚至数据包的路径。如当源 S 和目的地 D 要进行通信的时候, 首先源会获取到此过程中源到目的地的所有路径信息段, 如果需要进行匿名的通信, 就需要对这些路径信息段进行不同的加密操作等。和 SDN 相比, SDN 中的大多数工作主要适用于域内通信, 而 SCION 主要涉及改进域间通信, 使每个域内的网络变化最小。SCION 可以利用 SDN 提供域内通信, 因此, 这两种方法相互补充。虽然一些新兴的 SDN 项目试图在现有的互联网架构中提供域间属性, 如显式多路径支持, 但它们缺乏 SCION 提供的安全性和拓展性等属性。

与软件定义网络类似, SCION 也存在控制平面和数据平面。控制平面用来探索和传播可达性信息, 数据平面的功能是如何转发数据包。现有的网络层匿名通信协议可以在 SCION 架构上获取到路径信息后, 再进行匿名的会话通信。网络层匿名通信协议也可以称作基于网络基础设施(如路由器)的匿名协议。与基于覆盖网络的现有匿名系统相比, 基于基础设施的匿名系统有 3 个优点: 首先, 使用源和目的地之间的较短路径, 可以减少传播延迟; 其次, 仅涉及网络模型中传输层下方的层; 最后, 路由器可以提供比现在自愿提供资源服务器更高的吞吐量, 并且也致力于增加匿名通信中的吞吐量。对两类匿名通信协议的比较如表 1 所示。

3.2 网络层匿名通信协议的简介

根据现有的网络层匿名通信协议对计算量和

表 1 基于覆盖网络的匿名通信协议和网络层匿名通信协议的比较
Table 1 Comparison of anonymous communication protocols based on overlay networks and anonymous communication protocols at the network layer

类别 (性质)	在当前网络中所处的位置	可拓展性	延迟	吞吐量	安全性	目前的部署规模
基于覆盖网络的匿名通信协议(以 Tor 为例)	应用层	低	高	低	高	全球用户大规模使用
网络层匿名通信协议	网络层	高	低	高	低	尚未大规模部署

包头开销的不同要求, 将它们划分为轻量级匿名协议和洋葱路由匿名协议。网络层轻量级匿名协议(如 LAP、Dovetail 和 PHI)只需要网络设备来解密和验证路径段, 而这个路径段是包含了转发数据包所需的基本信息, 并使用端到端的数据包加密来提供保密性。相比之下, 洋葱路由匿名协议(如 Hornet、Taranet)需要路径上的网络设备进行昂贵的加密操作来建立流, 并对每个数据包使用每跳认证加密。每个路径上的节点还需要在其路径段内存储必要的密钥, 这使数据包包头开销增大。除此以外, 轻量级匿名协议之所以轻量也在于这类匿名协议没有对数据包的负载进行加密操作。

网络层匿名通信协议所期望达到的隐私和性能属性根据每个协议的设计而有所不同。本文根据现有的期望属性可对协议进行评估和分析。

隐私属性如下。

1) 发送者/接收者匿名。匿名是指将用户的身份、行为和网络地址等隐私信息隐藏在特定的匿名集合中, 令网络窃听者和攻击者无法识别通信行为具体是由哪一个体发起, 识别通信双方的身份以及具体的网络地址信息。发送者/接收者匿名是指攻击者无法通过捕获到的数据包链接发送者/接收者。

2) 会话不可链接性。会话不可链接性则是确保如果给定来自两个不同会话的两个数据包, 攻击者无法确定这些数据包是否和同一个发送者(或接收者)相关联。

3) 地理位置隐私。当用户隐藏他的地理位置时, 攻击者无法追踪用户的位置。

4) 路径信息机密性/真实性。攻击者根据路径上的变节点无法揭示路径上的节点总数或其余任一端的终端主机的距离。除此以外, 攻击者也无法修改现有路径或伪造新路径。

5) 数据包有效负载保密和端到端的完整性。

在终端主机不变节的情况下, 攻击者无法从数据包负载中学习任何信息, 除了数据包序列之间的长度和时间。

6) 抵制流量分析。流量分析是指通过元数据(如流量模式、时序等), 来识别通信端点。而根据攻击者是否操纵流量, 可以将流量分析技术分为主动和被动。而为了提高匿名性, 抵制流量分析攻击具有重大意义。

性能属性如下。

1) 低性能开销。为了达到低带宽开销和低延迟的目标, 在加密方面操作一般仅使用对称加密。

2) 可拓展性。为了避免状态爆炸问题, 保持最小或者无每流状态来减少攻击面积, 提高可拓展性。

3) 低路径延伸。由于等待时间随着路径上中间跳数(中间节点)的增加而增加, 所以尽量保持低路径延伸。

4) 高吞吐量。吞吐量是指对网络、设备、端口、虚电路或其他设施, 单位时间内成功地传送数据的数量(以比特、字节、数据包等测量)。而网络层匿名通信协议则希望达成高吞吐量的目标来满足用户的需求。

3.2.1 网络层轻量级匿名协议

一般地, 轻量级匿名协议有以下 3 点特征: 首先, 这类协议可以提供高速的数据包转发, 速度可达到 100 Gbit/s; 其次, 此类协议通过不需要在每个中间节点上维持流状态从而实现高拓展性; 最后, 它们可以融入不同的网络架构中。目前存在的轻量级匿名协议有 LAP、Dovetail 以及 PHI。

(1) LAP

Hsiao 等^[17]提出的 LAP 协议是一种可以实现实时双向匿名通信的轻量级协议, 有两个基本属性: 低延伸匿名和宽松的攻击者模型。低延伸匿名是指用于匿名和私人通信的数据包应该经过几

乎最佳的路由。而宽松的攻击者模型（如终端服务器攻击）则是区别于现有匿名系统所考虑的强攻击者模型（如全球或政府级攻击者）。

本文将对 LAP 进行概述，并解释终端主机如何建立加密路径以及自治域（AS, autonomous system）如何沿着加密路径转发数据包以实现中等级别的匿名性。如用户（或发送者） S 想要和目的地（或接收者） D 进行匿名会话，假设所使用的拓扑结构如图 2 所示，LAP 协议的目的则是隐藏 S 发起的路径并到达目的地，换句话说 LAP 协议是通过模糊终端主机的拓扑位置来加强匿名性。而其中的关键点在于每个数据包都包含加密的数据包包头，包头中包含路由信息。为了实现匿名性，每个 AS 在数据包包头内只能了解到关于其本身的信息。

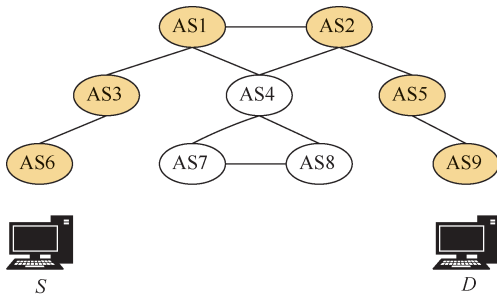


图 2 LAP 网络拓扑模型
Figure 2 The model of LAP network topology

当 S 想要和 D 进行通信时，首先 S 发送空的数据包用于与目的地 D 建立连接。在图 3 中展示了该协议对于数据包包头的具体加密过程。LAP 协议中有这样的定义：该数据包中已经事先包含

了目的地 D 的地址，所以每个 AS 均可以独立地决定如何转发数据包。比如 AS3 在了解到目的地的地址的情况下知道它需要转发数据包给 AS1。LAP 协议假设每一个 AS 都有一个本地密钥。首先，AS6 使用自己的本地密钥 $K6$ 对转发信息（即 AS 的路由决策）进行加密，比如 AS6 中的 a 就是 AS6 的出口接口。随后 AS6 将加密后的路径信息添加入数据包包头的路径段中。对于其他 AS 也进行类似的操作，直至 AS9 也完成此操作之后，此时的数据包包头中就包含了所有的加密的转发信息。而这样的数据包包头可以添加进所有的数据包中，每一个 AS 只需用自己的密钥进行解密便可得到转发信息来转发数据包。

在 LAP 协议中，segment 的具体构造如下：

$$x_i = \text{ENC}(k_i^e; M_i) \quad (1)$$

$$S_i = x_i \parallel \text{MAC}_{k_i^s}(x_i \parallel S_{i-1}) \quad (2)$$

其中， M_i 表示 AS 的路由决策（如出入口接口）， $\text{ENC}(k_i^e; M_i)$ 表示用密钥 k_i^e 加密 M_i ， $\text{MAC}_k(m)$ 表示使用密钥 k 的 m 的消息认证码， k_i^e 表示由随机数衍生出的对称密钥， k_i^s 表示 AS 的当前的短期密钥。

LAP 数据包包头格式

LAP 属于网络层的路由协议，并且主要是对数据包的包头格式进行了修改。图 4 展示了 LAP 数据包的包头格式。LAP 协议的数据包有两种类型：会话请求过程中的请求数据包和用来回复信息的回复数据包。从图 4 中可以看出，请求数据包表示的是 S 打算与 D 匿名通信。为了发起请求，

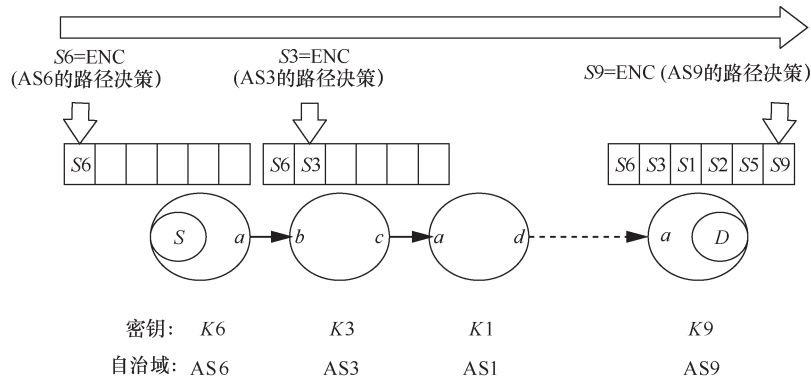


图 3 包头中加密路径的形成过程
Figure 3 Formation of E-PATH in the packet header

S 在 32 位目的地址中指定 D 的地址。在请求数据包经过多个自治域并到达 D 的过程中, 每个中间 AS 域将自己的加密路径段添加入“加密路径”字段中。而回复数据包的包头中不包含 IP 地址, 这是因为可以从相应的请求数据包中直接复制双向的加密路径来转发回复数据包。此外, 包头中还包括一个“长度”字段来指示数据包的大小。加密路径中则包含的是一组段, 每一个段的大小默认为 128 bits。如图中所示, 每个段都包含一个入口端口、一个出口端口、段的大小, 用来存放其他信息的保留位以及消息鉴别码 (MAC, message authentication code)。

LAP 实现发送者匿名和对地理位置的保护。为了实现接收者匿名, 可以采用约会节点的方式, 参考 Tor 中的机制, 该协议可以和当前 IP 网络相适应, 也可以与未来网络架构 SCION 等相融合。LAP 是网络层匿名通信领域的首创之举, 为之后该领域的研究提供了很多的灵感。但对于 LAP 协议也存在一个明显的问题: AS6 作为第一跳, 同时知道了源和目的地的地址, 那么此时就必须信任第一跳, 否则将会破坏匿名性。为了改进这一缺陷, Sankey 等^[18]在 Dovetail 协议中采用一种间接的思想进行改进。

(2) Dovetail

Dovetail 协议的思想是在 LAP 协议的基础上通过使用间接节点来隐藏目的地。由于源的网络服务提供商能够链接源和目的地, 因此从源不能直接构建到目的地的路径。在 Dovetail 中采用了随机选择且不被信任的第三方节点作为辅助节点。在图 5 中, 源会选择另一个节点如 M 作为自

己的辅助节点。需要说明的是源 S 和辅助节点 M 采用的是公钥加密操作, 而作为中间节点的路由器则使用的是对称加解密操作和简单的散列链。首先, 源 S 和辅助节点 M 可协商密钥对, 在不泄露目的地地址的前提下建立一条到达目的地 D 的路径。路径建立过程如下。首先, 源 S 会使用 M 的公钥加密目的地地址, 即得到 $m = \text{ENC}(K^+; D)$ (其中 K^+ 表示公钥, K^- 表示私钥) 并且建立一条到达 M 的路径, 这样源就可以建立如图 5(a) 所示的路径。然后, 当到达辅助节点 M 之后, 辅助节点可以使用自己的私钥解密出 D 的地址, 即 $D = \text{DEC}(K^-; m)$, 但此时辅助节点并不知道源 S 的地址。同时辅助节点 M 可以到达 D 的路径, 如图 5(b) 所示。综合图 5(a) 和图 5(b) 可看出两张图中的两个路径都经过节点 AS4, 并将该节点 AS4 称为 Tail 节点, 而 Tail 节点也是形成最后完整路径的关键。最后完整路径的形成如图 5(c) 所示。而此处的 Tail 节点是由源选择的, 并将其提供给辅助节点 M 。Tail 节点的存在可以弱化路径在建立过程中对辅助节点 M 的依赖性。在 Dovetail 协议中没有 AS 同时知道源和目的地的地址, 从而保证了安全性。

通过对以上两个协议的比较, 可以发现 LAP 协议的缺点是需要信任第一跳, 而优点则是可以适用于没有源控制的网络架构; 而在 Dovetail 协议中, 其优点是没有 AS 能够同时知道源和目的地的地址, 但缺点就在于它需要源控制的网络架构。除此以外, 两者的数据包格式都存在一个共同的问题: AS 位置的泄露。如当攻击者攻击了图 5(c) 的 AS9 之后, 它可以分析并学习到在其本

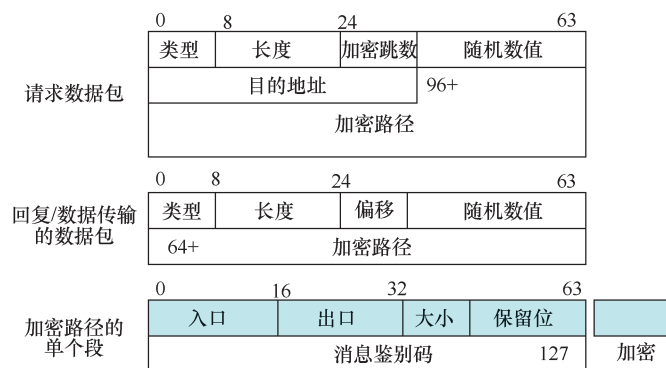


图 4 LAP 数据包包头格式和 segment 的格式
Figure 4 Formats of packet headers and a path segment of LAP

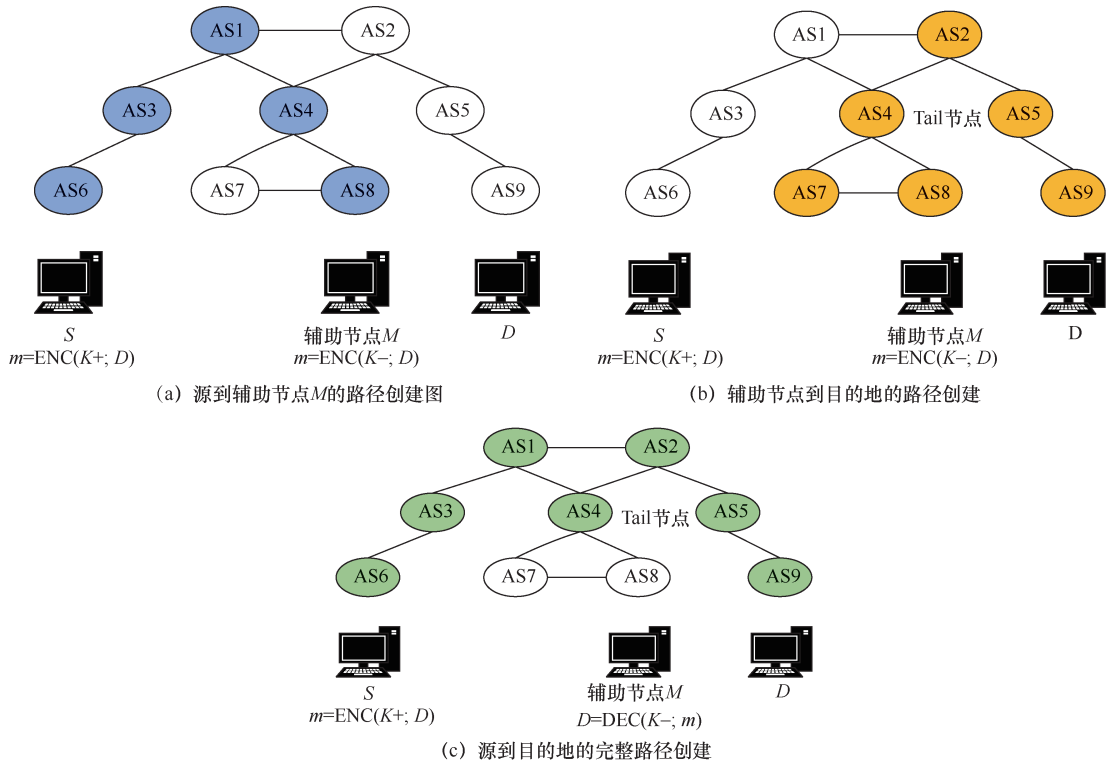


图 5 Dovetail 连接的构造过程

Figure 5 Construction of a Dovetail connection

身之前还存在 5 个段，那么攻击者就可以了解到自己处于第 6 跳的位置，并且它知道了目的地的地址，从而会损坏匿名性。因此对于轻量级匿名协议的更严格的要求也就应运而生。对于一个新的匿名协议，希望可以达到以下 3 点要求：第一，AS 的位置不被泄露；第二，没有 AS 同时知道源和目的地的位置；第三，可以适应于没有源控制的转发路径。而 2017 年 Chen 等^[19]提出的新路由协议 PHI 则达到了以上 3 个要求。

(3) PHI

在网络层隐藏路径的轻量级匿名协议简称 PHI。PHI 不仅解决了在 LAP 和 Dovetail 中存在的问题，同时也保持了与 LAP 和 Dovetail 相同的效率水平。PHI 提出了一种隐藏路径信息的有效包头格式和一种新的可与当前及未来网络架构兼容的后退路径建立方法。实验分析表明 PHI 将 LAP 和 Dovetail 的匿名集扩展了 30 多倍，并在商用软件路由器上达到 120 Gbit/s 的转发速度。

为了使 AS 的位置不被泄露，PHI 中采用段

位置随机化的思想。当要插入一个段到数据包的包头时，以密钥键入的伪随机函数来计算出伪随机位置，随后进行插入操作。如图 6 所示，比如 AS6 计算出的位置号是 3，则将 S6 插入到数据包包头中的确定位置。对于其他 AS 也进行相同的操作。这种方法可以防止攻击者捕捉到包头中段位置之间的关联。

在密钥管理部分，网络中的每个节点都维护一个主密钥，从中可以导出 3 个密钥：节点的位置密钥 k^{pos} 、加密密钥 k^{enc} 以及 MAC 密钥 k^{mac} 。3 个密钥的作用各不相同： k^{pos} 是节点用来确定其路径段在数据包包头中的位置； k^{enc} 用来加密路径段中的路由信息； k^{mac} 计算 MAC 以帮助节点验证其路径段。此外，目的节点需要生成一对 Diffie-Hellman 密钥。为了匿名地与目的地进行通信，源节点需要通过外部通道获取目的地的公钥。

在 PHI 中隐藏路径信息的核心思想是在数据包包头中随机化每个节点的段的位置。具体的随机化过程如下。首先，节点会使用伪随机函数（PRF, pseudo-random function）来计算其段在包

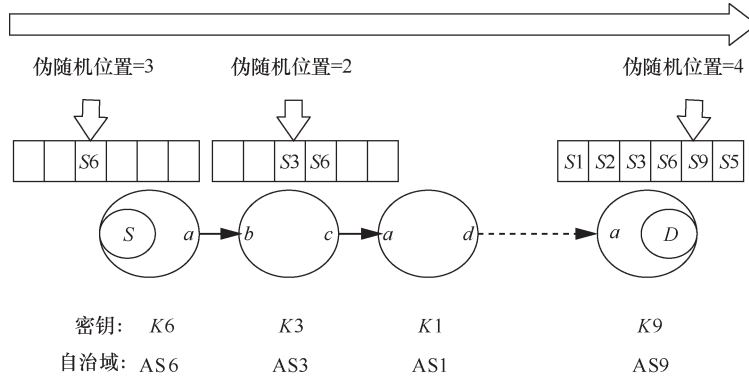


图6 PHI中段位置随机化的过程
Figure 6 The process of randomizing path-segment positions in PHI

头中的位置。函数的输入是该节点的本地密钥 (k_i^{pos}) 和会话 id (sid), 输出则是计算出的该节点要插入的位置 (pos)。表示为

$$\text{pos} = \text{PRF}(k_i^{\text{pos}}; \text{sid}) \quad (3)$$

然后, 每个节点生成自己的段, 段的构造公式如式(4)~式(6)所示。

$$E_i = \text{ENC}(k_i^{\text{enc}}; R_i \parallel \text{pos}_{\text{prev}} \parallel \text{flags}) \quad (4)$$

$$M_i = \text{MAC}(k_i^{\text{mac}}; E_i \parallel M_{i-1}) \quad (5)$$

$$S_i = E_i \parallel M_i \quad (6)$$

其中, k_i^{enc} 表示本地加密密钥, R_i 表示节点的路由信息, pos_{prev} 表示前一个节点的段, k_i^{mac} 表示本地 MAC 密钥, M_{i-1} 表示前一个节点的 MAC。

最后, 节点将自己的段插入计算好的位置中。但这种操作会带来一个冲突问题: 当两个 AS 计算的位置号相同时, 就会产生冲突。如 AS6 计算出的位置号是 3, AS1 的位置号也是 3, 那么后者将把前者覆盖掉。针对这种冲突问题, 研究者们提出两种解决方案。第一种方案是进行多次试验, 同时发送多个会话建立请求数据包。第二种方案是采用更大的包头空间。如对于 4 跳的路径, 需要 12 个段的空间。

而在 PHI 中为了与当前的互联网架构兼容, 即在没有源控制转发路径的情况下工作, 采用的方案是建立后退路径。首先, 源 S 是建立一条到达辅助节点 M 的路径, 这部分路径的构建过程与 Dovetail 类似。而与 Dovetail 的不同之处在于, Dovetail 中需要辅助节点 M 来拓展一条不同的路径, 而 PHI 是由辅助节点沿着前向的路径的相反

方向发出请求, 从而寻找中间节点。每一个在路径上的 AS 都可以独立地检查其本身是否可以转发数据包给目的地。当一个节点成为中间节点之后, 如图 6 中的 AS1, 则可以创建一个新路径段, 并且将出口端口的字段更改为朝向目的地, 同时在自己的段中设立“中间”标志。最后 AS1 便可以建立到达 D 的路径。

PHI 数据包包头格式

PHI 的数据包共有两种类型: 会话请求过程中请求数据包和回复/数据传输数据包。PHI 的请求数据包中包括以下几个部分: 数据包类型、数据包长度、前一跳的位置、计算出的段位置号、加密段形成的路径、S 的 DH 公钥以及地址位。而回复数据包中也有相同的部分: 数据包类型、数据包长度、前一跳的位置、计算出的段位置号以及加密段形成的路径。具体数据包格式如图 7 所示。

和 Dovetail 中建立路径的过程相比, 在 PHI 的后退路径建立的过程中, 每一个 AS 都可以独立地决策自己是否要成为中间节点, 而 AS 也不需要去控制哪个节点去成为 Tail 节点, 因此不需要源去控制整条转发路径。最后 Chen 等^[19]的实验结果也表明了 PHI 的匿名集的规模比 LAP 和 Dovetail 的匿名集大 30 多倍, 从而也抵抗了基于拓扑的攻击。

3.2.2 网络层洋葱路由匿名协议

和网络层轻量级匿名协议相比, 网络层洋葱路由匿名协议就显得复杂些。虽然前者在下一代网络架构上提供网络层低延迟匿名通信, 但这 3 种方案的高性能导致安全性保障严重下降, 同时对

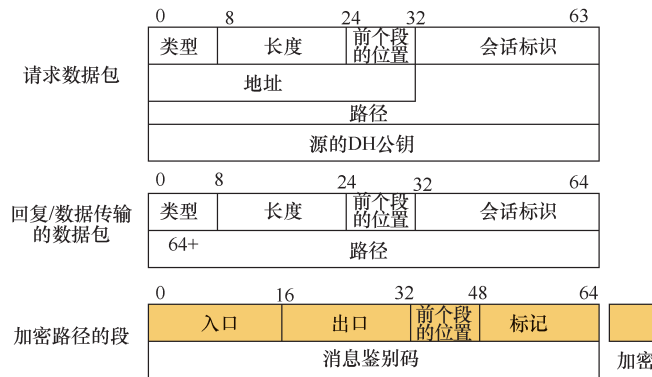


图 7 PHI 数据包包头格式和 pathsegment 的格式
Figure 7 Formats of packet headers and a pathsegment of PHI

数据包有效负载的保护依赖于上层协议，这也就增加了整体复杂性。而网络层洋葱路由协议针对这些缺陷进行了改进。此类协议默认提供数据包有效负载的保护，也可以抵御利用多个网络观察点的攻击。换言之，该类协议有以下 3 点的显著特征：首先，和轻量级匿名协议一样，为了实现高拓展性，节点转发数据包所需要的状态一般由数据包携带，会话状态卸载至终端主机，这样中间节点也可以快速转发流量；其次，为了实现高效的数据包处理，中间节点在数据传输阶段仅采用对称加密的方式处理数据包；最后，在会话建立成功之后，在数据传输过程中，数据有效负载使用洋葱加密的方式进行加密保护。

(1) Hornet

Chen 等^[20]提出的 Hornet 协议的基本目标是实现可拓展性和高效性。为了实现因特网规模的匿名通信，Hornet 中间节点必须避免保持每一会话状态（如加密密钥和路由信息等）。会话状态被卸载至终端主机，终端主机将该状态嵌入到数据包中，使每个中间节点可以在数据包转发过程中提取自己的状态。

卸载会话状态会带来两个问题。第一，节点需要防止它们的卸载状态泄露信息（如会话的加密密钥）。为了解决这个问题，每个 Hornet 节点都通过使用一个本地密钥来加密被卸载的每个会话状态，并将此加密后的状态称为转发段（FS, forwarding segment）。FS 允许构建它的节点来检索嵌入信息（即下一跳、共享密钥、会话到期时间等），同时对于未授权的第三方，该信息不可见。以上操作实现了 Hornet 流量的

位模式不可链接性和数据包路径信息的机密性，并且 Hornet 协议可以防御基于数据包内容匹配数据包的被动对手。然而，该协议容易受到更复杂的主动攻击。

FS 作为 Hornet 协议中重要的转发单位。与 LAP 和 PHI 的段类似，有其特殊的定义方式，表示为

$$FS = FS_CREATE(SV, s, R, EXP) \quad (7)$$

$$\{s \| R \| EXP\} = FS_OPEN(SV, FS) \quad (8)$$

其中， SV 表示只有创建出该 FS 的节点所知道的秘密值（secret value）， s 表示节点与源共享的密钥， R 表示路由信息， EXP 表示会话到期时间，而节点通过 FS_CREATE 和 FS_OPEN 两个功能相反的函数来加解密出节点转发数据包时所需的转发状态。

Hornet 数据包格式

Hornet 数据包分为两种格式：会话建立时期的数据包和数据传输过程的数据包。具体格式如图 8 所示。

Hornet 的数据包包头重用于会话中的所有数据包，并且有效载荷不受完整性保护，因此 Hornet 无法防止数据包重放。攻击者可以任意更改有效载荷，使数据包看起来与处理节点合法的新数据包无法区分。这种重放攻击可以和流量分析结合使用，将可识别的指纹插入流中，有助于对通信端点进行去匿名化。基于此，为了可以抵制流量分析，在 Hornet 的基础上进行改进，Chen 等^[21]在 2018 年提出了新的匿名协议——Taranet。

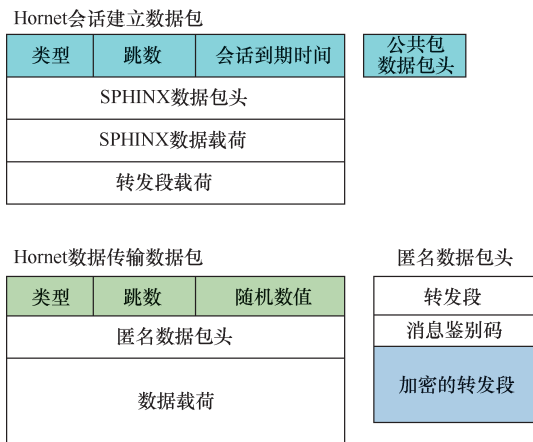


图8 Hornet 数据包格式
Figure 8 Hornet packet formats

(2) Taranet

一方面,现代低延迟匿名通信系统无论是构建为覆盖网络还是在网络层实现,在抵制流量分析的安全保障方面的能力都有限;另一方面,高延迟匿名系统以计算开销和长延迟为代价提供强大的安全保证,但这对于交互式应用来说代价太大。为了在网络层实现抵制流量分析的保护,并控制发生的延迟和开销,Chen 等^[21]提出了Taranet。在Taranet的会话建立阶段使用混洗^[50]来抵制流量分析^[22];在数据传输阶段,终端主机和AS协调使用数据包分割技术将流量整形为恒定速率传输。而Chen 等^[21]人的实验表明Taranet可以以超过50 Gbit/s的速度转发匿名流量。

图9和图10表示的是Taranet协议在会话建立阶段和数据传输阶段的流程。

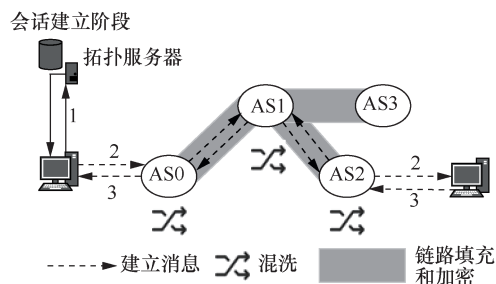


图9 Taranet 会话建立阶段
Figure 9 Setup phase of Taranet

与先前描述的网络层匿名通信协议类似,Taranet 协议也分为两个阶段:会话建立阶段和数据传输阶段。在会话建立阶段,每个Taranet 节点处理会话建立消息时使用混洗。在中间节点处理

会话建立消息之后,节点将消息在本地组合成大小为 m 的批次中。一旦有足够多的消息就可形成批处理,节点首先在每个批处理中随机化消息顺序,然后发出批处理。通过批处理和命令随机化,Taranet 节点便可以模糊消息的时间和顺序。通过观察非受损节点的输入和输出数据包对手无法将输出数据包与批处理中相应的输入数据包进行匹配,从而抵制了流量分析。但因为建立消息需要等到累积到足够多的消息,所以这种批处理技术也会带来额外的延迟,但鉴于网络中大量的同时链接,所以引入的延迟非常低。

数据传输过程

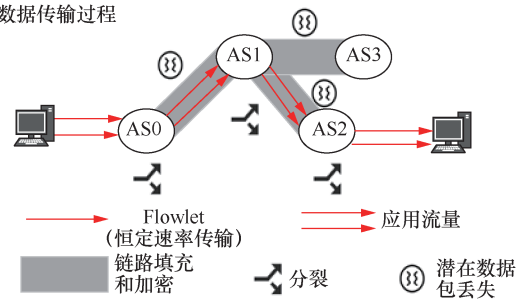


图10 Taranet 数据传输阶段设计流程
Figure 10 Data transmission phase of Taranet

在数据传输阶段免受流量分析的基本思想是将流量整形为恒定速率传输。Flowlet 是基本传输单元,终端主机以恒定的速率 B 和最大生命周期 T 来传输数据包。在Flowlet的生命周期 T 内,终端主机始终以速率 B 来传输数据包,必要时添加垃圾包。Flowlet的关键属性是不仅在终端主机上而且在所有遍历的链路上保持恒定的传输速率,Flowlet 依赖于端到端填充而非链路填充。为了实现恒定速率的传输,理想情况下每个Flowlet 应在每个节点以速率 B 到达和离开。然而抖动、丢弃可能导致速率变化,但数据包分裂技术可以使一个数据包在特定中间节点处分裂成两个数据包,所得的数据包和其他不可分离的数据包无法区分,生成的数据包仍经过相同的路径并且到达接收者的终端主机。

Taranet 数据包格式

Taranet 数据包包含数据包包头和数据包负载。其中包头包括初始向量(IV, initial vector),转发段、消息鉴别码、控制位(CTRL BIT, control bits)、会话到期时间(EXP, expiration time)和不透明头部信息(opaque header information)。除

此外，在数据包包头和数据包负载之间的区域为填充位区域，用于将数据包包头拓展到相同的大小，防止不同的数据包因规格不同而容易被区分。具体格式如图 11 所示。

尽管 Taranet 在 Hornet 的基础进行了改进，但 Taranet 依旧存在局限性，如 Taranet 本身无法抵制来自底层的路由攻击等。Taranet 依赖于底层网络架构来转发数据包，攻击者可以攻击底层网络架构，将自己置于架构之中从而进行流量分析攻击。这种攻击不在 Taranet 的防御范围内，但新兴网络架构等可以针对此类攻击进行强大的保护。

3.3 网络层匿名通信协议的整体分析

本文阐述的第一类网络层匿名通信系统是轻量级匿名系统，其目的是通过隐藏数据包包头内的转发信息来打败单个恶意服务提供商。与 Tor 之类的洋葱路由方案相比，轻量级匿名系统避免了对数据包有效载荷进行加密操作，从而提高了效率。

Hsiao 等^[17]的开创性工作 LAP 首先讨论了如何设计一个高效且可扩展的网络层匿名系统，该系统的数据包包头隐藏了网络位置信息。为了实现可扩展性，LAP 转发节点不需要维持每个流转发状态，相反，由每个 LAP 数据包携带转发状态。每个节点维护一个本地密钥，并通过使用该密钥解密数据包携带状态从而检索转发状态。由于 LAP 在建立数据包包头时会显示目的地的地址，因此 LAP 总是假设第一跳节点是良性节点，这就给攻击者带来了破坏匿名性的机会。

Sankey 等^[18]提出的 Dovetail 是在数据包包头

建立时引入了辅助节点从而消除了 LAP 中需要信任第一跳节点的假设。发送方使用辅助节点的公钥加密目的地地址，并建立到辅助节点的一半路径。辅助节点解密目的地地址并创建到目的地的后半路径。为了减小路径伸展因子，发送方确保前半路径和后半路径在 Dovetail 节点处相交。发送方通过移除 Dovetail 节点和辅助节点之间的节点从而组合这两个半路径。

但是，LAP 和 Dovetail 数据包包头格式都会泄露有关发送方和接收方之间总跳数以及发送方/接收方与转发节点之间跳数的信息。路径上的敌手节点可以通过结合相关的网络拓扑的知识，使用泄露的信息来减少发送方（或接收方）的匿名集。针对 LAP 和 Dovetail 的局限性，Chen 等^[19]提出 PHI，它可以通过段位置随机化和后退机制来达到更好的性能。另外，PHI 除了可以防范基于拓扑的攻击以外，还可以抵御观察数据包负载和会话链接等类型的被动攻击以及会话劫持攻击、数据包包头修改、重放攻击和预计算攻击等类型的主动攻击。PHI 可以说是提供了一种高效的可以隐藏路径信息的数据包包头格式。

而另一类网络匿名通信协议是由 Chen 等^[20-21]定义的网络层洋葱路由匿名协议。该类协议针对网络层轻量级匿名通信协议进行改进。在轻量级匿名协议中，终端节点容易受到不局限于单个网络位置的攻击，并且对数据包负载的保护依赖于上层协议，这样就增加了复杂性。

Hornet 的基本设计目标是可扩展性和高效性，除此以外也提供了对数据包负载的保护。该协议提出一种由数据包携带加密状态的洋葱路由数据包格式。它采取了将会话状态卸载至

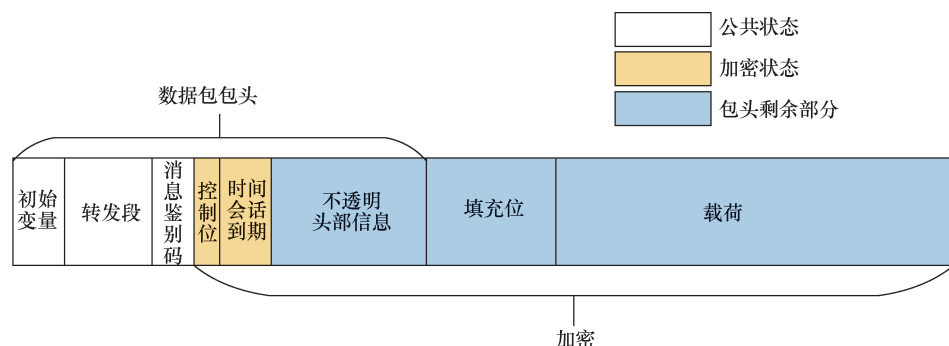


图 11 Taranet 数据包格式
Figure 11 Taranet packet formats

终端主机，并将它们自己的状态嵌入数据包以便中间节点在数据包转发过程中可以提取出自己的状态进行转发操作。Hornet 的协议过程一般存在两个步骤：会话建立（收集源和目的地之间的所有节点的会话状态）和数据转发（按照数据包中各自节点的会话状态进行转发数据包、传输数据）。但 Hornet 并不能抵制流量分析，这是它的一大缺陷。而 Taranet 除了可以达到 Hornet 的设计目标以外，还能够解决流量分析。为了达到此目标，Taranet 在会话建立阶段进行消息的混淆，而在数据传输阶段则提倡端到端的恒定速率传输，通过采用数据包分裂技术来适应网络抖动和数据包的丢失。但与 Hornet 相比，Taranet 也牺牲了部分吞吐量。

网络层匿名通信协议实则是基于基础设施（如路由器）的匿名网络协议。此类型的匿名通信协议寻求可以在可拓展性、安全保证和性能之间达到权衡。表 2 是对网络层匿名通信协议从匿名性和性能方面的总体分析^[15]。其中包括 8 个指标：吞吐量、是否信任第一跳节点、是否隐藏拓扑信息、是否需要源控制路径、是否达到低延迟目标、可拓展性、位模式不可连接性以及是否抵制流量分析。

4 结束语

匿名通信技术作为网络安全领域的一项关键技术，自出现以来一直是学术界研究的热点课题。在当前的互联网大环境下，匿名作为社会群众的一项基本权利，面临着来自私人公司和政府监督计划的挑战。在匿名通信系统的性能越来越好，提供的匿名等级越来越高的同时，匿名技术也存在被不法分子所利用从而进行破坏性活动的风

险。频频爆发的涉及用户隐私的安全事件使匿名通信受到了极大的关注。当前基于覆盖的应用层匿名通信解决方案无法同时提供强大的匿名性和高性能。随着对未来互联网架构的深入研究，研究者们提出了将匿名通信设计为网络架构的核心服务，并且支持在路由器上进行加密操作以及控制路径。本文阐述了网络层匿名通信协议的基本思想，给出了对网络层匿名通信协议进行分类的标准，并介绍了现有的网络层匿名通信协议的基本工作原理。此外，未来互联网架构可以提供当前互联网设计中所缺乏的理想属性，如故障隔离、路径控制和可信度等。目前已经出现的网络层匿名通信协议也表明了新兴互联网架构的可行性和优势。研究结果表明网络层匿名通信系统可以比当前最先进的基于覆盖的匿名通信系统达到更高的吞吐量，同时在面对攻击时也能够保证一定的匿名性。

但对于网络层匿名通信协议的设计中依然存在亟待解决的问题，并且也有值得深入研究的创新点。首先是匿名拓扑信息服务，拓扑信息服务可以将拓扑信息发给终端主机。对比 Tor 的权威目录服务器，其可存储管理所有中继节点的描述信息，所以在网络层的匿名通信系统中也应该有类似的服务。虽然存在多种解决方案来传播拓扑信息，但如何在新兴的互联网架构中以匿名、高效和可拓展的方式设计这样的服务器还需要深入的研究。其次，网络层匿名通信协议的实现也为在软件定义网络中如何实现匿名通信提供了宝贵的经验。新型网络架构的出现（如 SCION 等）使网络层匿名通信协议的实现成为可能。以往的匿名通信方案（如 Tor 等）凭借自身的特性在各个应用领域内发挥着各自的作用，SDN 所拥有的集

表 2 网络层匿名通信协议的性能分析
Table 2 Performance analysis of network-layer anonymous communication protocols

协议	吞吐量/ (Gbit·s ⁻¹)	是否信任 第一跳节点	隐藏 拓扑信息	是否需要 源控制路径	是否达到 低延迟目标	可拓 展性	是否实现位模式 不可链接性	是否抵制 流量分析
LAP	≈100	是	否	否	是	是	否	否
Dovetail	≈100	否	否	是	是	是	否	否
PHI	≈100	否	是	是	是	是	否	否
Hornet	92	否	是	是	是	是	是	否
Taranet	50	否	是	是	是	是	是	是

中控制和掌握全局视图的新特性为匿名通信领域的创新带来了新的机会,也值得做进一步的思考和研究。

参考文献:

- [1] DANEZIS G, DIAZ C, SYVERSON P. Systems for anonymous communication[J]. Handbook of Financial Cryptography and Security, Cryptography and Network Security Series, 2009: 341-389.
- [2] DIAZ C. Anonymity and privacy in electronic services[D]. Heverlee: Katholieke Universiteit Leuven, 2005.
- [3] 刘湘雯, 王良民. 数据发布匿名技术进展[J]. 江苏大学学报(自然科学版), 2016, 37(5): 562-571.
LIU X W, WANG L M. Advancement of anonymity technique for data publishing[J]. Journal of Jiangsu University(Natural Science Edition), 2016, 37(5): 562-571.
- [4] 赵福祥. 网络匿名连接中的安全可靠技术[D]. 西安: 西安电子科技大学, 2001.
ZHAO F X. Research on security and authentication techniques of anonymous network connection[D]. Xian: Xidian University, 2001.
- [5] 杨云, 李凌燕, 魏庆征. 匿名网络 Tor 与 I2P 的比较研究[J]. 网络与信息安全学报, 2019, 5(1): 70-81.
YANG Y, LI L Y, WEI Q Z. Comparative study of anonymous network Tor and I2P[J]. Chinese Journal of Network and Information Security, 2019, 5(1): 70-81.
- [6] GÜLCÜ C, TSUDIK G. Mixing email with BABEL[C]//1996 Symposium on Network and Distributed System Security. 1996.
- [7] LE BLOND S, CHOFFNES D, ZHOU W, et al. Towards efficient traffic-analysis resistant anonymity networks[J]. ACM SIGCOMM Computer Communication Review, 2013, 43(4): 303-314.
- [8] DANEZIS G, DINGLELINE R, MATHEWSON N. Mixminion: design of a type III anonymous remailer protocol[C]//IEEE S&P, 2003/O (SNAP'03). 2003.
- [9] DANEZIS G, GOLDBERG I. Sphinx: a compact and provably secure mix format[C]//IEEE Symposium on Security & Privacy. 2009.
- [10] DINGLELINE R, MATHEWSON N, SYVERSON P. Tor: the second-generation onion router[C]//The 13th USENIX Security Symposium. 2004.
- [11] ZHU Y, FU X W, GRAHAM B, et al. On flow correlation attacks and countermeasures in mix networks[C]//The Privacy Enhancing Technologies Symposium (PETS). 2004: 207-225.
- [12] MURDOCH S J, DANEZIS G. Low-cost traffic analysis of Tor[C]//The IEEE Symposium on Security and Privacy (Oakland). 2005: 183-195.
- [13] MITTAL P, KHURSHID A, JUAN J, et al. Stealthy traffic analysis of low-latency anonymous communication using throughput fingerprinting[C]//The ACM Conference on Computer and Communications Security (CCS). 2011.
- [14] B N LEVINE, M K REITER, C X WANG, et al. Timing attacks in low-latency mix-based systems[C]//The International Conference on Financial Cryptography (FC). 2004.
- [15] GILAD Y, HERZBERG A. Spying in the dark: TCP and Tor traffic analysis[C]//12th Privacy Enhancing Technologies Symposium (PETS 2012). 2012: 100-119.
- [16] CHEN C. Infrastructure-based anonymous communication protocols in future internet architectures[D]. Pittsburgh: Carnegie Mellon University, 2018.
- [17] HSIAO H C, KIM T J, PERRIG A, et al. LAP: lightweight anonymity and privacy. IEEE Security & Privacy, 2012, 19: 506-520.
- [18] SANKEY J, WRIGHT M. Dovetail: stronger anonymity in next-generation internet routing[M]//Lecture Notes in Computer Science. 2014.
- [19] CHEN C, PERRIG A. PHI: path-hidden lightweight anonymity protocol at network layer[J]. Nephron Clinical Practice 2017, 2017(1): 100-117.
- [20] CHEN C, ASONI D E, BARRERA D, et al. HORNET: high-speed onion routing at the network layer[J]. arXiv: 1507.05724, 2015.
- [21] CHEN C, ASONI D E, PERRIG A, et al. TARANET: traffic-analysis resistant anonymity at the network layer[J]. EuroS&P, 2018: 137-152.
- [22] CHAUM D L. Untraceable electronic mail, return addresses, and digital pseudonyms[J]. Communications of the ACM, 1981, 24(2).
- [23] 王继林, 伍前红, 陈德人, 等. 匿名技术的研究进展[J]. 通信学报, 2005, 26(2): 112-118.
WANG J L, WU J H, CHEN D R, et al. A survey on the technology of anonymity[J]. Journal on Communications, 2005, 26(2): 112-118.
- [24] GÜLCÜ C, TSUDIK G. Mixing email with Babel[C]//The Network and Distributed System Security Symposium (NDSS). 1996.
- [25] MÖLLER U, COTTRELL L, PALFRADER P, et al. Mixmaster protocol version 2[S]. Draft, 2003, 154: 28.
- [26] SHOSTACK A, GOLDBERG I. Freedom systems 1.0 security issues and analysis[Z]. White Paper, Zero Knowledge Systems, 2001, 10.
- [27] BROWN Z. Cebolla: pragmatic IP anonymity[C]//The Ottawa Linux Symposium. 2002.
- [28] REED M G, SYVERSON P F, GOLDSCHLAG D M. Anonymous connections and onion routing[J]. IEEE Journal on Selected Areas in Communications, 1998, 16(4): 482-494.
- [29] ALI A, KHAN M, SADDIQUE M, et al. Tor vs I2P: a comparative study[C]//2016 IEEE International Conference on Industrial Technology (ICIT). 2016.
- [30] REITER M K, RUBIN A D. Crowds: anonymity for web transactions[J]. ACM Transactions on Information and System Security, 1997, 1(1): 66-92.
- [31] FREEDMAN M J, MORRIS R. Tarzan: a peer-to-peer anonymous network layer[C]//The ACM Conference on Computer and Communications Security (CCS). 2002: 121-129.
- [32] BLOND S L, CHOFFNES D, CALDWELL W, et al. Herd: a scalable, traffic analysis resistant anonymity network for VoIP systems[C]//The ACM Conference of the Special Interest Group on Data Communication (SIGCOMM). 2015.
- [33] BLOND S L, CHOFFNES D, ZHOU W X, et al. Towards efficient traffic-analysis resistant anonymity networks[C]//ACM SIGCOMM. 2013.
- [34] SHERWOOD R, BHATTACHARJEE B, SRINIVASAN A. P5: a protocol for scalable anonymous communication[C]//The IEEE Symposium on Security and Privacy (Oakland). 2002.

- [35] CHAUM D. The dining cryptographers problem: unconditional sender and recipient untraceability[J]. *Journal of Cryptology*, 1988, 1(1): 65-75.
- [36] GOLLE P, JUELS A. Dining cryptographers revisited[C]//The International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT). 2004: 456-473.
- [37] WOLINSKY D I, CORRIGAN-GIBBS H, FORD B, et al. Dissent in numbers: making strong anonymity scale[C]//The USENIX Symposium on Operating Systems Design and Implementation (OSDI). 2012.
- [38] CORRIGAN-GIBBS H, BONEH D, MAZIÈRES D. Riposte: an anonymous messaging system handling millions of users[C]//The IEEE Symposium on Security and Privacy (Oakland). 2015: 321-338.
- [39] MURDOCH S J, DANEZIS G. Low-cost traffic analysis of Tor[C]//IEEE Symposium on Scrubby and Privacy. 2005: 193-195.
- [40] SYVERSON P, TSUDIK G, REED M, et al. Towards an analysis of onion routing security[M]//Designing Privacy Enhancing Technologies. 2001: 96-144.
- [41] MURDOCH S J, ZIELINSKI P. Sampled traffic analysis by internet-exchange-level adversaries[C]//The 2007 Privacy Enhancing Technologies Workshop. 2007.
- [42] SYVERSON P, TSUDIK G, REED M, et al. Towards an analysis of onion routing security[M]//Designing Privacy Enhancing Technologies. 2001.
- [43] SNADER R, BORISOV N. EigenSpeed: secure peer-to-peer bandwidth evaluation[C]//The International Workshop on Peer-to-Peer Systems (IPTPS). 2009: 9.
- [44] SHERR M, BLAZE M, LOO B T. Scalable link-based relay selection for anonymous routing[C]//The Privacy Enhancing Technologies Symposium (PETS). 2009: 73-93.
- [45] SHERR M, MAO A, MARCZAK W R, et al. A3: an extensible platform for application-aware anonymity[C]//The Network and Distributed System Security Symposium (NDSS). 2010.
- [46] TSCHORSCH F, SCHEUERMANN B. Mind the gap: towards a backpressure-based transport protocol for the Tor network[C]//The USENIX Symposium on Networked Systems Design and Implementation (NSDI). 2016.
- [47] PREVIDI S, SH R, HOMEFFER M, et al. SPRING problem statement and requirements[J]. *Der Orthopäde*, 2016, 36(4): 360-364.
- [48] FILSFILS C, NAINAR N K, PIGNATARO C, et al. The segment routing architecture[C]//2015 IEEE Global Communications Conference. 2015.
- [49] FILSFILS C, MICHELSEN K, TALAULIKAR K. Segment Routing 详解 (第一卷) [M]. 北京: 人民邮电出版社, 2017.
- [49] FILSFILS C, MICHELSEN K, TALAULIKAR K. Segment Routing part I[M]. Beijing: Posts & Telecom Press Co LTD, 2017.
- [50] YANG X, WETHERALL D. Source selectable path diversity via routing deflections. *ACM SIGCOMM Computer Communication Review*, 2006(36): 159-170.
- [51] ZHANG X, HSIAO H C, HASKER G, et al. SCION: scalability, control, and isolation on next-generation networks[C]//2011 IEEE Symposium on Security and Privacy. 2011: 212-227.
- [52] ANDERSON T, BIRMAN K, BROBERG R, et al. The NEBULA future internet architecture[J]. *The Future Internet*, 2013: 16-26.
- [53] D RAYCHAUDHURI, K NAGARAJA, VENKATARAMANI A. MobilityFirst: a robust and trust worthy mobility-centric architecture for the future internet[J]. *ACM SIGMOBILE Mobile Computing and Communications Review*, 2012, 16(3): 2-13.
- [54] ANAND A, DOGAR F, HAN D, et al. XIA: an architecture for an evolvable and trust worthy internet[C]//The ACM Workshop on Hot Topics in Networks (HotNets). 2011.
- [55] ZHANG X, C HSIAO H, HASKER G, et al. SCION: Scalability, control, and isolation on next-generation networks[C]//The IEEE Symposium on Security and Privacy (Oakland). 2011.
- [56] PERRIG A, SZALACHOWSKI P, M REISCHUK R, et al. SCION: a secure internet architecture[M]. Springer International Publishing AG, 2017.

[作者简介]



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。



倪晓铃 (1996-), 女, 江苏南通人, 江苏大学硕士生, 主要研究方向为网络安全。



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。