软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2023,34(1):404−420 [doi: 10.13328/j.cnki.jos.006513]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

匿名网络综述*

马传旺[1], 张 宇[1,2], 方滨兴[1,2], 张宏莉[1]

[1](哈尔滨工业大学 网络空间安全学院, 黑龙江 哈尔滨 150001)

[2](鹏城实验室, 广东 深圳 518055)

通信作者: 张宇, E-mail: yuzhang@hit.edu.cn

摘 要: 匿名网络旨在公开网络环境中保护用户通信隐私. 自 Chaum 提出 Mix 网以来, 相关研究在几十年中不断取得进展. 如今, 匿名网络已发展成以 Mix 网、DC 网或 PIR (private information retrieval) 为基础, 并结合多种设计要素, 使之适用于各种应用场景和威胁模型. 从匿名概念出发, 介绍匿名网络领域的发展情况, 分类阐述代表性研究工作及其设计选择, 并系统地从匿名性、延迟和带宽开销等角度进行分析.

关键词: 匿名网络; Mix 网; DC 网; PIR; 匿名性

中图法分类号: TP393

中文引用格式: 马传旺, 张宇, 方滨兴, 张宏莉. 匿名网络综述. 软件学报, 2023, 34(1): 404–420. http://www.jos.org.cn/1000-9825/6513.htm

英文引用格式: Ma CW, Zhang Y, Fang BX, Zhang HL. Survey on Anonymous Networks. Ruan Jian Xue Bao/Journal of Software, 2023, 34(1): 404–420 (in Chinese). http://www.jos.org.cn/1000-9825/6513.htm

Survey on Anonymous Networks

MA Chuan-Wang[1], ZHANG Yu[1,2], FANG Bin-Xing[1,2], ZHANG Hong-Li[1]

[1](School of Cyberspace Science, Harbin Institute of Technology, Harbin 150001, China)

[2](Pengcheng Laboratory, Shenzhen 518055, China)

Abstract: Anonymous networks aim to protect the user's communication privacy in open network environment. Since Chaum proposed Mix-net, related work has been progressing in decades. Nowadays, based on Mix-net, DC-net or PIR, many anonymous networks have been developed, for various application scenarios and threat models by integrating multiple design elements. Beginning from anonymity concepts, this paper introduces the overall development of anonymous network area. Representative works and their design choices are classified and articulated. The characteristics of anonymous networks are systematically analyzed from the perspectives of anonymity, latency, bandwidth overhead, etc.

Key words: anonymous network; Mix-net; DC-net; private information retrieval (PIR); anonymity

匿名网络是一种为用户提供通信隐私保护的技术与系统. 不同于传统端到端加密保护通信内容, 匿名网络保护通信元数据, 即关于通信本身的信息, 包括通信双方的身份、通信时间、消息数量等.

匿名网络起源于 1981 年 Chaum 提出的 Mix 网[1]. 目前应用最广泛的匿名网络——洋葱路由 (Tor)[2]就是基于 Mix 网思想. 1988 年, Chaum 基于密码学家晚餐问题提出 DC 网[3]. 2002 年, Kesdogan 等人[4]将私有信息检索 (private information retrieval, PIR)[5]技术应用于匿名网络中. 目前匿名网络研究主要以上述思想为基础, 面向特定应用, 如通用代理、即时通信、Web 浏览、邮件传输和 BT 下载等, 进行优化设计.

在以往匿名网络综述工作中, Edman 等人[6]按高延迟、低延迟和强匿名性的分类方法对匿名网络进行分析, 并总结去匿名技术. Ren 等人[7]根据匿名思想和网络结构对匿名网络进行分类. Shirazi 等人[8]从网络结构、路由信息、路由策略、网络性能和部署等方面进行分类. Unger 等人[9]综述了安全消息传递中匿名性技术. Sampigethaya

* 基金项目: 国家重点研发计划 (2018YFB1800702, 2016YFB0801303, 2016QY01W0103); 鹏城实验室项目 (PCL2021A02)
收稿时间: 2020-07-14; 修改时间: 2021-01-28, 2021-07-03; 采用时间: 2021-10-11; jos 在线出版时间: 2021-11-24
CNKI 网络首发时间: 2022-11-15

等人[10]分析 Mix 网中采用的加密策略、级联拓扑、消息验证机制, 总结一些提高 Mix 网性能的方法, 并对多种基于 Mix 网的匿名网络进行性能比较. 吴艳辉等人[11]总结了早期匿名性的评价指标及匿名技术的特点. 罗军舟等人[12]综述了 Tor、I2P 等 4 种典型匿名网络及去匿名技术. 赵蕙等人[13]从匿名集、概率分析、信息熵、通信双方关联性等多个角度综述了匿名度量方法.

本文涵盖新近的匿名网络研究进展, 依据设计思想对匿名网络进行分类, 归纳出若干匿名网络设计要素, 并借鉴 Hevia 等人[14]和 Das 等人[15]的工作分析比较各匿名网络的性能. 首先, 阐述匿名网络概念. 然后, 抽象出匿名网络设计要素. 接着, 按设计思想分类介绍, 并从设计要素及性能上对比分析. 本文不涉及去匿名技术, 对这方面感兴趣的读者可参考文献 [16].

1 匿名网络相关概念

1.1 基本概念

根据 Pfitzmann 等人对匿名网络概念的定义[17], 对手 (adversary) 感兴趣的事物分为实体、消息、行为、身份 4 类. 在实体中, 可产生行为的被称为主体 (subject), 发送消息的主体为发送者 (sender), 接收消息的主体为接收者 (recipient), 负责转发消息的为中间节点. 发送者和接收者统称为用户. 所有潜在发送者和接收者构成一个集合, 即匿名集 (anonymity set). 针对某个主体, 匿名性 (anonymity) 表示为对手不能充分地从匿名集中识别出该主体. 不可观测性 (unobservability) 是一个比匿名更强的概念, 要求对手不仅无法识别出参与通信的主体, 甚至无法判断主体是否真实参与通信, 即对手观测到每个主体似乎都在参与通信. Hevia 等人[14]将对手所能观测到的信息分为消息元数据和消息数量两类. 据此提出一种匿名性划分方法.

• 发送者 (接收者) 匿名性: 对手无法根据消息元数据从匿名集中识别发送者 (接收者), 但允许对手观测到发送者 (接收者) 发送 (接收) 的真实消息数量.

• 匿名性: 同时满足发送者匿名性和接收者匿名性; 换句话说, 对手无法根据消息元数据从匿名集中识别发送者和接收者, 但允许对手观测到真实消息数量.

• 发送者 (接收者) 不可观测性: 满足发送者 (接收者) 匿名性, 同时要求对手无法观测到发送者 (接收者) 发送 (接收) 的真实消息数量.

• 不可观测性: 同时满足发送者不可观测性和接收者不可观测性; 换句话说, 满足匿名性的同时, 对手无法观测到真实消息数量.

图 1 表示不同匿名性概念间关系, 箭头由匿名性较强的一方指向较弱的一方. 例如, 若某匿名网络具有不可观测性, 则该匿名网络满足发送者不可观测性和接收者不可观测性, 进而可知该匿名网络满足发送者匿名性和接收者匿名性.

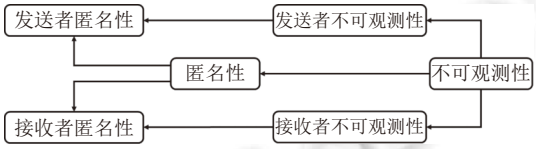

图 1 匿名性概念关系图

1.2 威胁模型

对手能力由 3 个维度构成.

• 角色: 将对手分为窃听者、恶意节点和恶意发送者/接收者 3 类角色. 窃听者可获取并分析流量, 通过交叉攻击等[18]识别主体. 恶意节点参与消息转发, 相比窃听者会获得更多信息[19], 如会话信息、上一跳和下一跳地址等. 最坏的情况是对手扮演恶意发送者或接收者, 此时要保证通信另一端的匿名性较为困难.

• 能力: 分为被动对手和主动对手. 前者只能窃听, 而后者可对消息进行增、删、改操作. 例如, 对手通过在流量中加入水印并在出口处识别水印来关联发送者和接收者[20,21].

• 范围: 分为全局对手和局部对手. 前者能力范围可作用于整个网络, 而后者仅限于局部.

2 匿名网络设计

匿名网络的本质是隐藏发送者、接收者及消息三者之间在网络层上的关系. 目前实现匿名大致有两种思路.

• 消息中转: 消息不由发送者直接发送给接收者, 而是经过若干中间节点变换后到达接收者. 对于发送者而言, 除非对手处于发送者和首跳节点之间, 否则不能识别发送者. 对接收者的分析, 与之类似. 然而, 当对手能够同时窃听首跳节点和末跳节点时, 可通过关联攻击识别发送者与接收者. 为此, 需采用进一步的匿名设计, 如时间同步假设、选路策略、转发混合和流量混淆. 这类匿名网络的设计关键在于发送者/接收者与中间节点之间消息交互, 及防止关联攻击, 其代表工作为 Mix 网.

• 逻辑广播: 消息以逻辑广播形式传输. 若存在多个潜在的发送者, 其中仅有一个真实发送者, 其他发送者发送虚假消息, 则实现发送者匿名性. 若发送者将消息广播给潜在的接收者, 而仅有真实接收者能识别消息, 则实现接收者匿名性. 这类匿名网络将全体发送者或接收者作为匿名集, 在对手看来所有用户均有相似行为. 由于广播开销较大, 因此其设计关键在于高效实现逻辑广播, 其代表工作为 DC 网.

目前大多数匿名网络设计基于上述思路, 并发展为以 Mix 网、DC 网和 PIR 这 3 种匿名网络设计为核心, 以应用场景为驱动, 针对网络结构、时间假设、路由策略、转发混合、流量混淆等设计要素进行优化.

2.1 基础匿名网络设计

下面阐述 Mix 网、DC 网和 PIR 这 3 种基础匿名网络设计.

2.1.1 Mix 网

Mix 网[1]是一种基于消息中转思想的基础匿名网络. Mix 网结合了级联代理与公钥加密体系. 发送者不直接将消息发送给接收者, 而是在本地选取若干用于变换消息的中间节点, 并对消息根据路由进行多层加密后发送. 密文按照既定的路由转发, 每经过一个中间节点将消息解密一层得到新的密文, 最后一跳中间节点解密得到明文, 再转发给接收者. 这些中间节点也被称为 Mix 节点. 如图 2 所示, 发送者 S 先使用接收者 R 公钥 PK_R 将明文加密, 再将密文和接收者地址按消息路由顺序的逆序使用各中间节点的公钥 PK_2 和 PK_1 逐层加密并转发给 $Mix1$. $Mix1$ 收到消息后解密并将余下部分转发给下一跳 $Mix2$, 再由 $Mix2$ 解密并将密文转发, 接收者解密即得到明文.

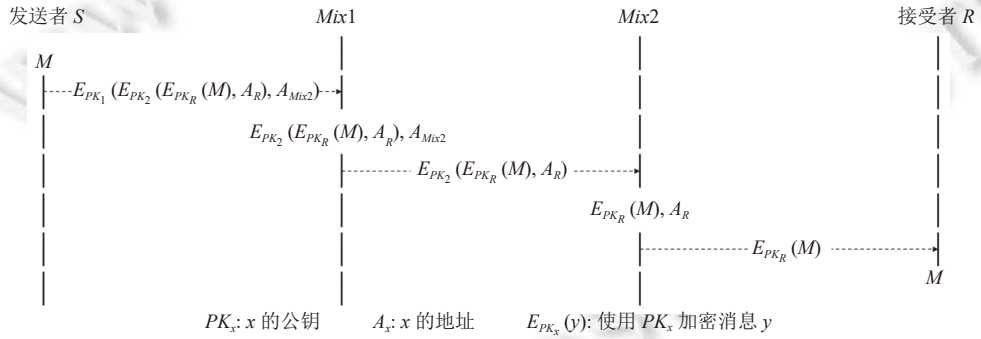

图 2 Mix 网基本原理

与发送者直接相连的中间节点称为入口节点, 与接收者直接相连的节点称为出口节点. 对手在发送者和接收者之间的任意一点窃听时, 其能观测到的均为外表无差别的密文, 无法确定其前一跳/后一跳是其他 Mix 节点还是发送者/接收者. 当对手扮演恶意接收者时, 由于消息经过若干 Mix 节点转发, 其无法得知发送者的真实身份. 但由于发送者必须知道接收者地址才能构造密文, 当对手扮演恶意发送者时, 无法隐藏接收者身份. 因此 Mix 网具有发送者匿名性.

Mix 网是由发送者发起的端到端匿名通信, 侧重于保护发送者隐私. 其具有低延迟和低带宽开销的特性, 在用户规模较大时不会严重降低通信效率, 适用于大规模匿名网络应用. 同时, Mix 网是一种较为灵活的基础匿名网络设计, 针对各种网络应用场景, 对不同设计要素的优化会使 Mix 网在匿名性和延迟、带宽开销的表现之间做出一个良好的折衷. 因此基于 Mix 网的匿名网络覆盖即时通信、Web 浏览、邮件传输、BT 下载等众多网络应用场景.

2.1.2 DC 网

DC 网[3]是一种基于逻辑广播思想的基础匿名网络. DC 网在每个时段内只允许一个节点发送消息. 发送者将消息加密后广播给其他节点. 同时, 其他节点广播各自生成的密钥, 这就起到了掩盖发送者身份的作用. 接收者收到密文和所有密钥后解密消息. 可见, 一次 DC 网通信需要全体节点参与. 如图 3 所示, 假设任意两点间均有可靠信道和共享密钥. 发送者 a 将消息 M 与其持有的所有共享密钥 k_{ab}、k_{ac}、k_{ad} 进行异或后广播. 同时, 其他节点将各自持有的所有共享密钥异或并广播. 接收者 d 收到来自其他所有节点的广播消息并异或后获得消息 M. 若 M 是使用接收者公钥加密的消息, 则只有接收者可解密.

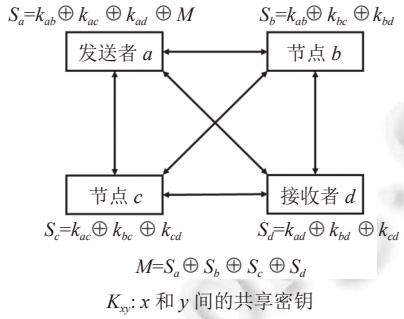

图 3 DC 网基本原理

在对手全局窃听情况下, 每个节点均进行相同的广播操作, 同时如果对手不知道足够多的共享密钥, 则无法识别发送者; 广播后, 包括接收者在内的所有节点均可计算出明文. 因此, DC 网实现匿名性.

DC 网中的广播通信模式使得全体用户构成一个匿名集, 对手难以识别用户间的通信关系, 这使其天然具有较强的匿名性. 然而, 广播通信也带来了高昂的带宽开销, 使其难以具有可扩展性. 另外, DC 网要求在实际通信前各用户间均持有共享密钥, 因此 DC 网只适用于网络规模小、用户成员相对固定、但有强匿名性需求的应用场景, 如小规模匿名通信/广播.

实现 DC 网需解决 3 个问题: (1) 协商同一时刻唯一的发送者; (2) 广播导致的可扩展性问题; (3) 任意单点故障或延迟过高影响通信.

2.1.3 PIR

PIR[5]是一种应用于数据库检索的隐私保护技术, 它能实现在不向数据库泄露用户检索的内容的条件下对数据库进行检索操作. 在基于 PIR 的匿名网络中, 均存在一个数据库用于暂存发送者和接收者之间的消息. 发送者将消息发送并暂存到服务器上, 接收者再使用 PIR 技术从数据库中检索该消息. PIR 可以保证数据库无法得知接收者检索的究竟是哪条消息, 进而无法将接收者与发送者相关联. 所有接收者均从数据库检索消息, 因此共同构成一个匿名集. 其具体原理如图 4 所示, 存在一个包含 n 个副本 (图中为 3) 的分布式服务器, 每个副本存储相同数据全集 S. S 被划分为若干位置 (slot). 发送者与接收者事先协商一个在 S 中保存消息的位置 p, 以向量 d 表示, 其中第 p 个分量为 1, 其余置 0. 发送者将消息发送并存储到所有副本的位置 p 上. 接收者为隐藏检索的消息位置, 在本地随机构造 n 个与 d 维数相同的掩码向量 $d_1, d_2, \ldots, d_n$, 且它们的异或结果为 d. 接收者分别使用掩码向量 d_i 检索副本 i, 从副本 i 中获取向量 d_i 中所有分量为 1 的位置上的消息并将这些消息的异或结果 S_i 返回给接收者. 接收者再将所有检索结果异或得到消息 M.

发送者通过非匿名网络将消息上传到服务器, 且所有潜在的接收者均可检索消息, 可看作一种逻辑广播. 当对手无法知道所有掩码向量 d_i 时, 则无法确定位置向量 d, 进而无法将消息与接收者关联, 因此 PIR 具有接收者匿名性.

PIR 强调接收者匿名性, 而完全不考虑为发送者提供匿名, 这在当前以端到端通信模式为主的网络环境下, 难以单独使用, 实际中通常将 PIR 与其他匿名网络结合, 来同时提供发送者和接收者匿名性. 另外, 由于接收者无法准确预知消息到达服务器的时间, 因此 PIR 的即时性一般, 适用于非延迟敏感的应用场景, 如邮件传输、非即时通信等.

表 1 对上述 3 种基础匿名网络进行比较, 延迟和带宽开销分析方法见第 2.3 节. 依据设计思想, 图 5 描述了相关工作分类及关系.

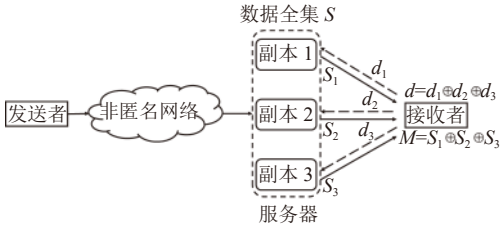

图 4 PIR 基本原理

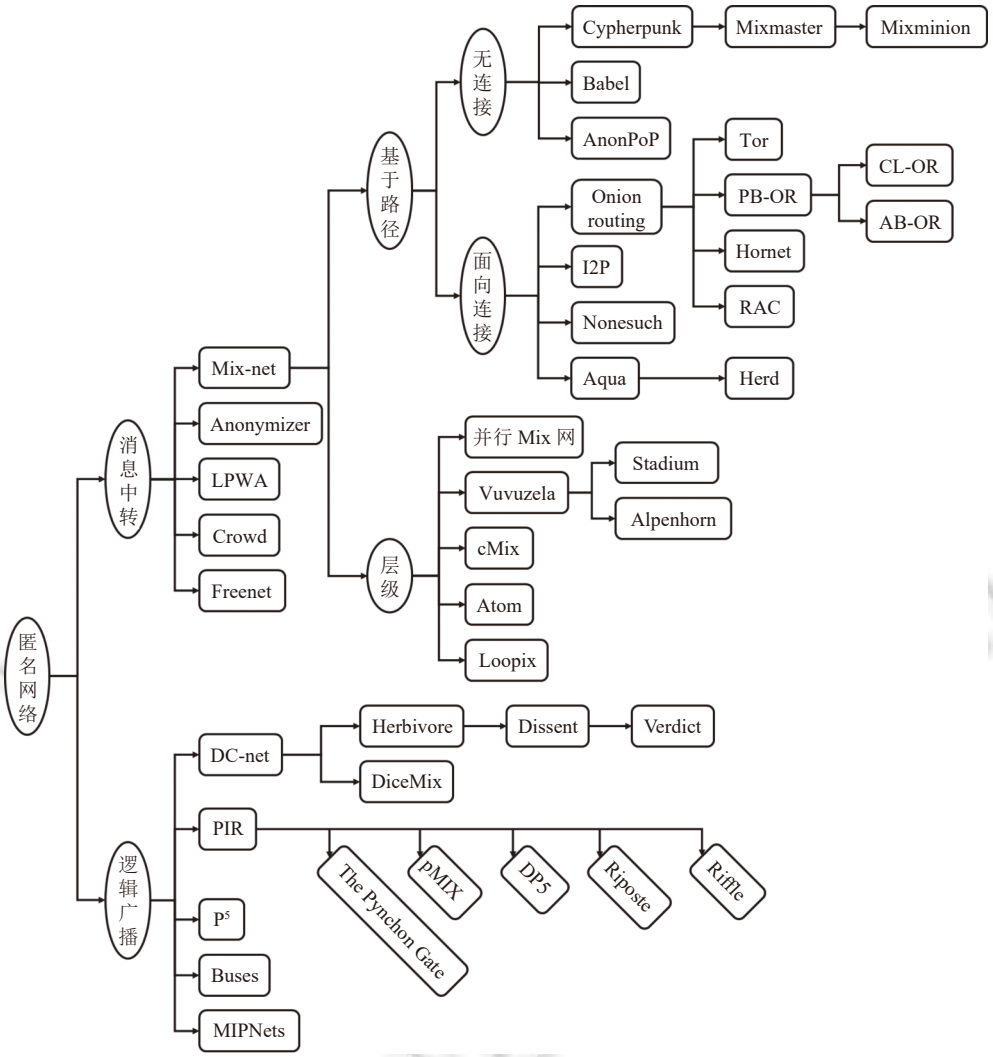

图 5 匿名网络间关系图

表 1 匿名思想分析

匿名网络	设计思路	匿名性	延迟	带宽开销	应用场景
Mix网[1]	消息中转	发送者匿名性	$\theta(1)$	$\theta(1/N)$	即时通信、Web浏览、邮件传输、BT下载等
DC网[3]	逻辑广播	匿名性	$\theta(1)$	$\theta(N/N)$	小规模匿名通信/广播
PIR[5]	逻辑广播	接收者匿名性	$\theta(1)$	$\theta(1/N)$	邮件传输、非即时通信等

2.2 设计要素

本节从当前各种匿名网络设计中提炼出关键设计要素, 第 3–6 节总结了本文涵盖的匿名网络在这些设计要素上的具体方案.

2.2.1 网络结构

从网络结构上可分为 C/S 结构和 P2P 结构. 在 C/S 结构下, 服务器为中间节点, 客户端仅作为发送者或接收者, 不参与消息转发. 相比之下, P2P 结构中所有节点可作为发送者、接收者和中间节点. 若系统是开放的, 则对手可部署恶意中间节点实施去匿名. P2P 结构的匿名网络中通常设计了特殊节点来负责维护网络状态和节点信息, 如 Tor[2]中目录权威 (directory authority).

2.2.2 同步假设

从消息传递时间上可分为异步系统和同步系统. 前者不要求连接建立和消息发送满足时间约束, 用户可以随时通信, 适用于 Web 浏览、即时通信等低延迟应用. 然而, 对手可以根据发送消息和接收消息的时刻来实施关联攻击. 为防御关联攻击, 后者存在全局时钟并将通信过程划分为回合, 所有节点必须在每个回合内执行规定操作, 适用于非延迟敏感场景, 如邮件系统、文件传输.

2.2.3 路由策略

基于消息中转的匿名网络中路由策略可分为 5 种: (1) 随机, 中间节点随机选取; (2) 加权, 依据节点性能 (包括延迟、吞吐量等参数) 选路; (3) 分批, 将消息分割成多个数据包并选取不同路径, 由接收者重组; (4) 受限, 只允许从部分中间节点中选路, 例如中间节点被限制对特定用户服务; (5) 固定, 通常出现在层级 Mix 网中, 中间节点仅为固定的高可用节点. 基于逻辑广播的匿名网络本身不涉及路由策略, 但当两种基础匿名网络思想结合使用时, 采用与基于消息中转的匿名网络相同的分析策略.

2.2.4 转发混合

在基于消息中转的匿名网络中, 转发混合将保留在中间节点缓冲区中的消息根据特定策略转发至下一跳, 来混淆消息转发时间信息, 防止基于时刻的关联攻击. Serjantov 等人[22]和 Edman 等人[6]总结了 4 种基本策略: (1) 阈值混合 (threshold mix), 当缓冲的消息数量达到阈值后转发; (2) 定时混合 (timed mix), 在间隔固定的时刻转发, 同步网络通常采用该类混合; (3) 池混合 (pool mix), 当满足时间或数量条件后转发部分消息, 其余继续保留; (4) 停启混合 (stop-and-go mix), 每条消息在随机延迟后转发.

2.2.5 流量混淆

流量混淆是匿名网络实现不可观测性的一种方法. 通过注入虚拟流量隐藏真实消息数量, 令对手无法判断用户是否参与通信. 虚拟流量会增加带宽开销, 且当带宽开销超过链路带宽时还会影响延迟. 一种常见的流量混淆策略是匀速混淆, 即节点生成虚拟流量来保证任意时刻网络中的流量恒定, 但这种方式对带宽消耗较大. 另一种方式是虚拟流量的生成服从某特定分布, 在不牺牲匿名性的情况下减少带宽消耗.

2.3 性能分析

针对匿名网络性能, Das 等人[15]提出了 3 个指标: (1) 匿名性, 见第 1.1 节; (2) 延迟, 即消息从发送到接收所需时间, 分析时需考虑延迟与用户数量 N 以及仅用作转发的中间节点 K 之间的关系, 若延迟与二者无关, 则延迟为常数, 即 $\theta(1)$; (3) 带宽开销, 一次通信 (同步系统中一个回合) 中平均每个用户发送消息数量. 分析带宽时需考虑其与用户数量的关系, 例如 Mix 网中一次通信的消息数量为常数, 则带宽开销为 $\theta(1/N)$. 分析广播操作的带宽开销时, 仅考虑真实发送者发送的消息数量, 其他节点的广播不计入带宽开销, 例如 DC 网在一次通信中发送者需向全体 N 个节点发送消息, 因此 DC 网的带宽开销为 $\theta(N/N)$. Das 等人已证明上述 3 个性能指标构成一个三难困境. 例如, Mix 网为兼顾低延迟和低带宽开销而牺牲匿名性, 而 DC 网则以高带宽开销为代价实现低延迟和较强匿名性. 对于延迟和带宽开销, 本文采用与之相同的分析方法及其部分匿名网络的分析结果, 并对其未覆盖的匿名网络工作进行补充分析.

3 Mix 网

根据网络结构划分, Mix 网可分为基于路径的和基于层级结构的两类. 前者通常选取常数个中间节点作为路

由节点, 不同消息的传输路径相互独立; 后者将 Mix 网看作一个具有层次结构的整体, 消息在各层变换和重新排列并分发到下一层, 消息的传输路径相对固定. 表 2 对基于 Mix 网的工作进行比较分析.

表 2 基于 Mix 网的匿名网络分析

匿名网络	匿名性	网络结构	同步假设	路由策略	转发混合	流量混淆	延迟	带宽开销
Cypherpunk[23]	发送者匿名性	C/S	异步	随机	无	无	$\theta(1)$	$\theta(1/N)$
Mixmaster[24,25]	发送者不可观测性	C/S	异步	分批/随机	池	几何分布	$\theta(1)$	$\theta(N/N)$
Mixminion[26]	发送者不可观测性 接收者匿名性	C/S	异步	分批/随机	池	几何分布	$\theta(1)$	$\theta(N/N)$
Babel[27]	匿名性	C/S	异步	随机	无	无	$\theta(1)$	$\theta(1/N)$
AnonPoP[28]	不可观测性	C/S	同步	随机	定时	匀速	$\theta(K)$	$\theta(N/N)$
洋葱路由[29]	发送者匿名性	P2P	异步	随机	无	无	$\theta(1)$	$\theta(1/N)$
Tor[2]	发送者匿名性	P2P	异步	受限/加权/随机	无	无	$\theta(1)$	$\theta(1/N)$
PB-OR[30]	发送者匿名性	P2P	异步	随机	无	无	$\theta(1)$	$\theta(1/N)$
CL-OR[31]	发送者匿名性	P2P	异步	随机	无	无	$\theta(1)$	$\theta(1/N)$
AB-OR[32]	发送者匿名性	P2P	异步	随机	无	无	$\theta(1)$	$\theta(1/N)$
HORNET[33]	发送者匿名性	P2P	异步	随机	无	无	$\theta(1)$	$\theta(1/N)$
RAC[34]	不可观测性	P2P	异步	随机	无	匀速	$\theta(1)$	$\theta(RG/N)$
I2P[35]	匿名性	P2P	异步	受限/加权/随机	无	无	$\theta(1)$	$\theta(1/N)$
Nonesuch[36]	发送者匿名性	C/S	异步	随机	停启	无	$\theta(1)$	$\theta(1/N)$
Aqua[37]	不可观测性	C/S	同步	分批/随机	定时	匀速/动态	$\theta(1)$	$\theta(N/N)$
Herd[38]	不可观测性	C/S	异步	分批/随机	无	匀速/动态	$\theta(1)$	$\theta(N/N)$
并行Mix网[39]	发送者不可观测性	C/S	同步	固定	无	匀速	$\theta(K')$	$\theta(N/N)$
Vuvuzela[40]/Alpenhorn[41]	不可观测性	C/S	同步	固定	定时	拉普拉斯分布	$\theta(K)$	$\theta(N/N)$
Stadium[42]	不可观测性	C/S	同步	固定	定时	泊松分布	$\theta(K)$	$\theta(N/N)$
cMix[43]	发送者不可观测性	C/S	同步	固定	阈值定时	匀速	$\theta(K)$	$\theta(N/N)$
Atom[44]	发送者不可观测性	C/S	同步	随机	阈值	匀速	$\theta(K)$	$\theta(N/N)$
Loopix[45]	不可观测性	C/S	异步	分批/随机	泊松	泊松分布	$\theta(\sqrt{K}\ell')$	$\theta(\beta')$

注: $\theta(RG/N)$中R表示组内虚拟环数量, G表示组内节点数量; $\theta(K')$中 K'表示恶意服务器数量; $\theta(\sqrt{K}\ell')$ 中 ℓ' 表示消息的期望延迟[15]; $\theta(\beta')$ 中 β' 表示虚拟流量生成速率[15]

3.1 基于路径的 Mix 网

基于路径的 Mix 网中每次通信仅有少量中间节点参与. 对手的主要攻击途径是部署大量恶意中间节点, 通过控制发送者和接收者的首跳和末跳节点实施关联攻击. 实现方式可分为无连接的和面向连接的.

3.1.1 无连接的 Mix 网

无连接的 Mix 网无需在实际通信前建立连接, 且均为 C/S 网络结构, 可通过流量混淆来实现不可观测性. 无连接的 Mix 网需解决匿名回复问题, 即在保持发送者匿名情况下, 实现接收者回复消息.

Cypherpunk[23], 也称一型匿名重邮器 (remailer), 它是一个实现发送者匿名性的早期匿名邮件系统, 其中中间节点功能由重邮器实现. 将邮件发送者地址移除后进行传输. 邮件假名服务器 (email pseudonym server)[46]在 Cypherpunk 的基础上解决匿名邮件回复问题. 发送者需预先建立一条到达自身的路径, 与路径上中间节点协商会话密钥, 并将中间节点地址和会话密钥按路由顺序构造成洋葱结构的回复块 (reply block), 然后将假名、公钥和回复块上传到假名服务器 (nymserv) 上. 接收者回复时, 将发送者假名对应的回复块附加在消息头部, 消息按回复块中既定路径返回给发送者.

Mixmaster[24,25], 也称二型匿名重邮器, 它从 3 方面改进 Cypherpunk: (1) 路由策略采用随机和分批方式; (2) 转发混合采用一种池混合策略; (3) 流量混淆采用几何分布生成虚拟流量实现发送者不可观测性.

Mixminion[26], 也称三型匿名重邮器, 它为在 Mixmaster 基础上进一步为提供接收者匿名性, 将路径分割成两段, 第 1 段由发送者选取, 第 2 段使用接收者的一次性回复块. 一次性回复块避免了重复使用相同回复块而暴露接收者, 为通信双方提供匿名性.

Babel[27]使用返回路径信息 (return path information, RPI) 实现匿名回复. RPI 与回复块区别在于, 不必事先协商会话密钥, 而是由发送者通过密钥生成器直接为每个中间节点生成密钥. RPI 被直接附加在发送者的消息中, 相比上述工作, 无需从假名服务器上下载回复块.

AnonPoP[28]中包含客户端、中间节点和邮局 (post office, PO) 这 3 类角色. 客户端通过由 K 个中间节点构成的 Mix 网连接到 PO, 按同步网络方式每回合向 PO 发送消息读写请求; 无请求情况下, 生成虚拟请求. 采用 3 种增强匿名性的方法: (1) 采用 request-pool 技术, 在客户端离线时由入口节点代替客户端发送消息读请求, 隐藏客户端离线的事实; (2) 通过时间戳验证防止对手复制或延迟消息; (3) 当路径出现故障时, 中间节点向目录服务器报告故障路径, 避免后续使用.

Mixminion (Mixmaster) 根据几何分布生成虚拟流量, 而 AnonPoP 则采取匀速混淆策略. Mixminion、Babel 和 AnonPoP 分别采取不同的匿名回复策略: Mixminion 在通信前需协商密钥并构造回复块; Babel 在发送消息时将密钥附加到包头部; 而 AnonPoP 则引入邮局暂存消息, 发送者和接收者均通过 Mix 网与邮局通信, 这变相解决了匿名回复的问题. 综上所述, 此类方案按匿名性强弱排序, 最高的是 AnonPoP 的不可观测性, 但需要以延迟和带宽为代价. Mixminion 和 Mixmaster 都采用流量混淆来实现发送者不可观测性, Mixminion 和 Babel 还实现了接收者匿名性.

3.1.2 面向连接的 Mix 网

3.1.2.1 洋葱路由

洋葱路由 (onion routing, OR)[29]于 1996 年由美国海军实验室提出, 具有面向连接的特点. 洋葱路由不同于传统 Mix 网, 发送者先通过代理建立虚电路: 选取若干洋葱路由器作为中间节点, 并按照路由顺序分别与路径上的每个 OR 协商会话加密算法和密钥. 实际通信时使用会话密钥代替传统 Mix 网的节点公私钥.

第二代洋葱路由 (Tor)[2]对洋葱路由的主要改进如下: (1) 使用 Diffie-Hellman 密钥交换协议建立虚电路, 使用对称加密算法 (AES) 替代洋葱路由中非对称加密, 实现前向保密; (2) 使用目录权威存储网络全局状态, 包括 OR 地址信息、状态和标识位等; (3) 提供隐藏服务提供接收者匿名性; (4) 使用更具通用性的 SOCKS 接口, 作为应用层协议匿名代理. 此外, Tor 的隐藏服务 (hidden service) 解决了洋葱路由不具备接收者匿名性的问题. 归功于低延迟和通用性, Tor 是目前应用最广泛的匿名网络.

为降低 Tor 建立虚电路的开销, 若干研究采用更先进的密码学方案. 基于配对的洋葱路由 (pairing-based onion routing, PB-OR)[30]将非交互的密钥交换协议[47]和基于身份的加密 (IBE)[48]应用于虚电路建立. 一个第三方可信密钥生成机构采用 IBE 根据节点 ID 为每个节点生成公私钥对, 每个节点用自己的私钥和对方 ID 生成会话密钥. 构建虚电路时采用非交互密钥交换, 发送者将自己的 ID 告知每个 OR 即可协商会话密钥, 而无需采用逐级扩展方式. 缺点是密钥生成机构知道所有节点的私钥, 可以解密所有通信. 无证书洋葱路由 (certificateless onion routing, CL-OR)[31]采用基于无证书的公钥加密 (CL-PKC)[49]改进 PB-OR, 第三方可信密钥生成机构只为每个节点生成部分私钥, 再由节点以此自行生成公私钥对, 并自行更新密钥, 防止密钥生成机构解密.

基于属性的洋葱路由 (attribute based onion routing, AB-OR)[32]采用基于密文策略属性的加密 (CP-ABE)[50]以广播方式在相邻节点间传输消息以有效解决单一 OR 故障的情况. 发送者将所有节点分为 3 种角色: 非传输节点、传输节点和接收者. 发送者只需对消息进行两层加密, 外层可被传输节点或接收者解密, 而内层只能被接收者解密. OR 尝试对密文外层解密, 若成功, 则将原密文广播到相邻节点, 否则丢弃密文; 接收者可解密内外层密文得到明文.

HORNET[33]中 OR 不再维护会话状态, 包括虚电路 ID, 会话密钥, 后继节点 IP 地址等, 而将会话状态存储在紧凑加密消息格式 Sphinx[51]的转发段中, 告知发送者. 发送者在构造密文时将每个 OR 的转发段以洋葱形式加密存储在消息头部, 为 OR 提供转发所需的会话状态.

RAC[34]结合洋葱路由和广播思想来实现匿名性. 为降低广播对可扩展性的影响, 将节点分组, 在组内生成若干

虚拟环, 虚拟环为组内节点的一个有向环排列. 组内通信时, 发送者随机选择若干节点作为洋葱路径的中间节点并构造密文, 将消息广播到所有虚拟环中的后继节点. 节点尝试解密消息, 若成功则将解密后的消息转发给后继节点, 否则转发原消息, 直到接收者收到消息. 消息在虚拟环中需按预设的均匀速率传播, 当真实消息速率低于预设速率时, 以虚拟流量补充. 组间通信时, 发送者在消息的最内层加入接收者的组 ID, 由发送者的组内末跳节点将消息广播到发送者和接收者所在组中所有节点. RAC 带宽开销取决于虚拟环数量 R 和组内节点数量 G, 为 $\theta(RG/N)$.

洋葱路由的网络结构均为 P2P, 且大多采用随机的路由策略. 为实现其低延迟性, 均采用异步网络, 且基本不使用转发混合策略和流量混淆策略 (RAC 除外), 因此其延迟和带宽开销分别为 $\theta(1)$ 和 $\theta(1/N)$. 此类匿名网络的设计关键在于如何建立虚电路及协商会话密钥, Tor 采用了一种较为安全的虚电路建立方式, 而 PB-OR、CL-OR 和 AB-OR 则通过改进虚电路建立方式来提高通信效率. 另外, HORNET 还降低中间节点维护会话状态的负载, 而 RAC 和 AB-OR 通过广播来提高匿名性.

3.1.2.2 其他面向连接的 Mix 网

此类匿名网络与洋葱路由相比, 均在实际通信前需先建立端到端连接. 但区别在于此类匿名网络并非直接建立从发送者到接收者之间的完整连接.

I2P[35]相比 Tor 中发送者独自选取路径, 由发送者和接收者共同选取, 实现匿名性. 用户事先建立多条发送隧道 (outbound tunnel) 和接收隧道 (inbound tunnel), 隧道建立方式与虚电路建立类似 (也称大蒜路由). 发送者将其发送隧道出口与接收者的接收隧道入口相连建立完整路径.

Nonesuch[36]中发送者采用 Mix 网方式使用 Minx[52]加密消息格式生成密文并将其隐写入图片中, 发送到 Usenet Image Newsgroup. 中间节点从 Usenet 上下载可能包含消息的图片并试图用私钥提取密文, 若成功提取, 则后续操作与洋葱路由类似, 每个节点使用私钥解密密文头部, 得到一个对称密钥, 再用对称密钥解密密文余下的部分, 最后由出口节点转发给接收者.

Aqua[37]是一种适用 TCP 大流量传输服务的匿名网络. 先选择入口节点和出口节点建立会话, 消息在二者间传输时还会经过若干中转节点, 中转节点并不固定且对会话状态一无所知. 在流量混淆上, 在中间节点间使用匀速混淆策略; 中间节点根据客户端传输速率进行动态混淆, 保证各客户端和中间节点间传输速率相同.

Herd[38]是一种应用于 VoIP 的低延迟匿名网络. 采用区域化的网络结构, 用户选择加入多个域, 并使用域内中间节点建立部分路径. 通过将通信双方的部分路径连接来建立完整路径. 引入超级节点在入口/出口节点和客户端之间, 负责整合来自同一信道的多个客户端消息 (每个信道中仅有一个客户端真实参与通信), 提高系统可扩展性. 流量混淆上与 Aqua 相同.

在连接建立方式上, I2P 和 Herd 由发送者和接收者分别建立一部分连接后再对接, Aqua 只固定入口和出口节点, 而 Nonesuch 在发送者和入口节点之间额外加入隐写术来实现混淆. 综上所述, 此类匿名网络按匿名性强弱排序, 最高的是 Herd 和 Aqua 的不可观测性, 采用流量混淆技术以带宽消耗为代价. 其次是 I2P 的匿名性, 最后是 Nonesuch 的发送者匿名性.

3.2 层级 Mix 网

层级 Mix 网均为 C/S 结构, 中间节点被组成为若干层级, 每层包含若干中间节点, 每个中间节点参与多个层级. 发送者将消息发送给入口层中某节点后, 每层的节点对消息解密并重新排列, 转发到下一层. 最后, 出口层将解密的消息发送给接收者.

并行 Mix 网[39]如图 6 所示, 包含 K 个 (图中 K=3) 中间节点, 其中 K'个 (图中假设为 1) 恶意中间节点. 每层为全体中间节点的一个排列. 首先, 所有发送者将消息 (图中为 9 个消息) 均匀提交给入口层的节点 (图中每个中间节点收到 3 个消息). 然后, 进行消息轮转, 即每个中间节点 i 将消息随机排列后转发给节点 i+1 mod K. 需轮转 K'次, 令每条消息都至少被非恶意中间节点处理过一次. 接着, 每个中间节点将消息均匀地分发给下层所有中间节点 (图中每个中间节点将 3 个消息分别发给 3 个中间节点), 防止对手关联消息收发端. 最后, 再次进行 K'次消息轮转后发送给接收者. 该方案的延迟仅取决于恶意中间节点数 K', 与 K 无关, 为 $\theta(K')$.

Vuvuzela[40]中发送者通过层级 Mix 网将消息上传到 dead drop 的服务器, 再由接收者直接从 dead drop 下载. 通信分两阶段: 拨号协议用于发起会话请求, 发送者向接收者对应的 dead drop 发送邀请消息, 来建立双方通信关系; 会话协议根据双方的密钥和当前回合数确定会话密钥和使用的 dead drop. 中间节点根据拉普拉斯分布注入虚拟流量, 证明可实现差分隐私[53]. Alpenhorn[41]增加好友系统来完善 Vuvuzela 的拨号协议. 用户维护好友地址簿, 其中存储好友间的共享密钥. 为添加好友, 一位用户使用 IBE[48]根据好友 ID 构造一个包含自身 ID 的好友请求, 好友解密后得到该用户 ID 并计算共享密钥. 好友间根据共享密钥生成会话请求以及会话密钥.

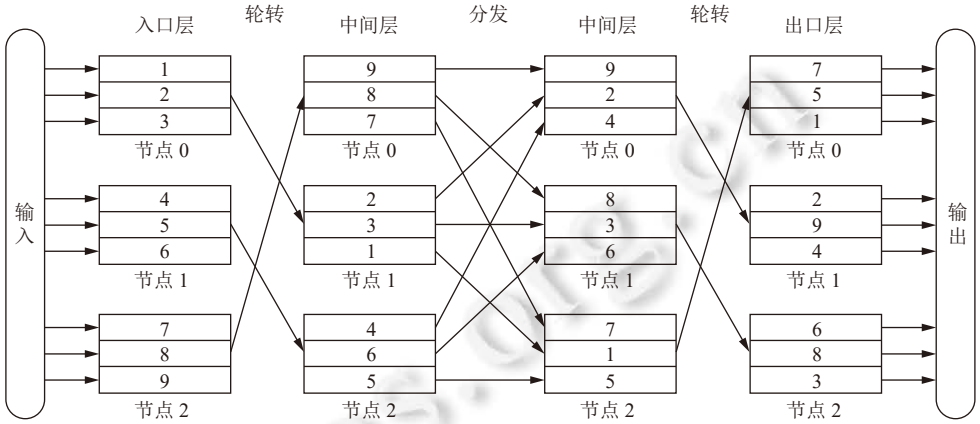

图 6 并行 Mix 网原理

Stadium[42]在 Vuvuzela 基础上使用并行 Mix 网思想, 在回合开始时, 随机将所有中间节点排列成多条输入链和输出链. 发送者选路时只需选择其中一条输入链和输出链, 消息经过输入链的出口后被均匀分配到所有输出链的入口, 最终到达 dead drop, 这种方式避免所有中间节点均需处理全部消息, 增强系统可扩展性. 使用可验证的洗牌[54]验证中间节点的消息正确性. 根据泊松分布生成虚拟流量, 并证明同样实现差分隐私.

cMix[43]采用一条由所有中间节点以固定顺序构成的 Mix 链. 发送者将消息加密并按照预先分配的位置写入一个“长消息”, 经过 Mix 链对消息解密、重新排列及转发. 使用基于 ElGamal 的多方参与的群同态加密算法[55], 每个中间节点持有部分密钥, 全部中间节点共同参与解密. 通过引入预计算来降低通信时计算负载, 在通信阶段利用预计算阶段计算出的中间值解密消息. 由于预计算的非敏感性, 可由第三方实现, 降低中间节点计算负载.

Atom[44]使用 ElGamal 变体加密方案, 发送者无需进行选路, 消息在每层需重新排列, 先用本节点私钥解密后再用下层节点公钥重新加密并转发到下一层. 为防止恶意节点主动攻击, 有两种解决方案: 一种是使用可验证的洗牌[54], 上层节点将消息发送给下层时需同时提交其证明, 这样每层中只要有一个诚实节点就能检测攻击, 但缺点是开销过高; 另一种安全性稍弱、适用于诚实节点较多情况的方法是使用基于消息的陷阱保护[56], 用户同时提交真实密文和陷阱密文, 对手主动攻击时可能篡改陷阱密文.

Loopix[45]是一个低延迟异步匿名网络, 每个用户通过服务商节点 (provider) 接入层级 Mix 网以及检索待接收的消息. “Loopix”的名字来自其流量混淆方式, 包含 4 种类型: (1) 用户遵循泊松过程向对方发送虚拟消息; (2) 用户以固定频率向服务商节点检索消息; (3)/(4) 用户/中间节点遵循泊松过程生成虚拟流量, 经过网络传递后返回到原用户/中间节点. 转发混合采用类似于停启混合的泊松混合, 消息随机延迟服从指数分布. Loopix 的延迟和带宽开销分析较为复杂, 依据 Das 等人[15]的分析, 假设消息经过的平均路径长度为 $\sqrt{K}$, 且每个节点对消息进行 ℓ' 平均延迟, 则延迟为 $\theta(\sqrt{K}\ell')$; 假设客户端的虚拟流量生成率为 β', 则带宽开销为 $\theta(\beta')$.

此类匿名网络通常会采用新型密码学技术增强安全性, 如通过零知识证明防止对手篡改消息排列和元数据; 采用更复杂的流量混淆策略提供不可观测性, 如 Vuvuzela 的拉普拉斯分布、Stadium 的泊松分布以及 Loopix 的 4 种流量混淆策略, 但这也导致此类匿名网络带宽开销较大. 从匿名性上来, Vuvuzela、Alpenhorn、Stadium 和 Loopix 均具有不可观测性, 而并行 Mix 网、cMix 和 Atom 仅具有发送者不可观测性.

4 DC 网

Herbivore[57]设计主要有 3 点: (1) 全局拓扑控制, 负责将所有节点分组, 组内使用 DC 网通信; (2) 回合协议, 组内采用星形拓扑, 每个节点轮流做中心节点收集各节点的异或加密信息并进行异或解密, 再将结果分发给各节点, 相比传统 DC 网减少了带宽消耗; (3) 将长消息划分为多个位置, 用户可随机选取消息写入位置, 并通过控制长消息的长度降低消息碰撞概率.

Dissent[58]保留 Herbivore 的分组设计, 但组内通信为 C/S 结构. 每组由大量客户端和少量服务器组成, 客户端和服务器、服务器和服务器之间均持有共享密钥. 客户端将消息与所有共享密钥进行异或后的密文发送给某一台服务器. 所有服务器将收到的多个密文的异或结果作为输入, 使用 DC 网在服务器间通信, 输出结果为所有明文, 最后分发给客户端. 由于服务器的数量远小于客户端, 因此可有效提高系统可扩展性, 且避免了 Herbivore 组内星型拓扑结构下中心单点故障.

Verdict[59]借鉴 Dissent 的 C/S 结构, 并引入可验证 DC 网来检测和排除恶意节点. 可验证 DC 网相比传统 DC 网的区别在于, 其使用新的密码学方案替代异或加密, 发送密文的同时需提交密文正确性证明. 密文构建方案分为 3 种: 基于 ElGamal 的构建、基于双线性映射的构建和基于 Hash 的构建. 为降低计算开销, 可验证 DC 网只在发现恶意节点时才使用.

DiceMix[60]使用流水线降低恶意节点对性能的影响. 在传统 DC 网中, 每回合只要有一个节点破坏通信, 那么通信必须从头开始. 而 DiceMix 将回合分为 4 个阶段: 密钥交换、提交明文、DC 网通信、确认/揭示密钥. 各回合之间相差两个阶段以流水线方式运行, 例如, 当某一回合开始“DC 网通信”阶段时, 下一回合开始“密钥交换”阶段, 以此类推. 当恶意节点篡改消息时, 发送者会发现消息未包含在输出中, 此时各节点公布本回合共享密钥来揭示恶意节点, 在下回合的“DC 网通信”阶段之前将该恶意节点排除在外, 而不必再从“密钥交换”阶段重新开始. 另外, 使用牛顿恒等式来构造长消息, 无需在通信前为客户端分配位置.

基于 DC 网的匿名网络的设计侧重于解决传统 DC 网存在的 3 个问题: (1) 可扩展性问题, 朴素的办法是将用户分组, 组内可采用通信复杂度更低的星型拓扑, 例如 Herbivore; Dissent 和 Verdict 则采用 C/S 结构, 通过将异或解密操作集中在少量服务器上来提高可扩展性; (2) 故障或恶意节点对性能的影响问题, 例如 Verdict 引入新的密码学方案来检测恶意节点; DiceMix 则通过流水线降低恶意节点的影响; (3) 同一回合只能有一个发送者的问题, 常用方法是长消息分割, 即所有节点复用同一个长消息, 但各节点将消息写入不同位置, 例如 Herbivore 由用户随机选取位置; Dissent 和 Verdict 使用可验证的排列为每个用户分配位置; DiceMix 采用牛顿恒等式构造长消息. 发送者可以选择发送真实消息或空消息 (虚拟消息), 从而隐藏网络中的真实消息数量, 因此均具有不可观测性. 时间假设、延迟与带宽开销则均与传统 DC 网相同, 分别为同步、$\theta(1)$ 和 $\theta(N/N)$. 表 3 对此类工作进行比较.

表 3 基于 DC 网的匿名网络分析

匿名网络	匿名性	网络结构	时间假设	延迟	带宽开销
Herbivore[57]	不可观测性	P2P	同步	$\theta(1)$	$\theta(N/N)$
Dissent[58]	不可观测性	C/S	同步	$\theta(1)$	$\theta(N/N)$
Verdict[59]	不可观测性	C/S	同步	$\theta(1)$	$\theta(N/N)$
DiceMix[60]	不可观测性	P2P	同步	$\theta(1)$	$\theta(N/N)$

5 PIR

The Pynchon Gate[61]是基于 PIR 的匿名邮件系统, 其中 nym 服务器负责暂存邮件. 在每个周期内, 发送者将邮件通过 Mix 网发送到 nym 服务器, 提供发送者匿名性. 整理器 (collator) 负责将本周期的所有邮件按用户 ID 的顺序生成多个带索引的消息块, 然后分发到多个相互独立的分发器 (distributor) 上. 接收者根据发送者的用户 ID 生成掩码, 再使用 PIR 从若干个分发器检索消息.

pMIX[62,63]使用 cPIR[64]取代 PIR, 相比 PIR 需要多个副本, cPIR 只需检索单一副本. 用户被分组, 保证每组中

只有一个用户实际参与通信, 以组为单位进行通信, 使那些未参与通信的用户不必生成额外的虚拟流量. 通信双方在通信时共用同一位置交换消息. 通信时, 发送者将待发送消息 P 和上一个收到的消息 Q 的异或值 $P\oplus Q$ 存储到相应位置上, 接收者使用 cPIR 从服务器中相应位置获取消息 $P\oplus Q$, 再与自己的消息 Q 异或得到 P.

DP5[65]基于一种改进的 PIR 方案[66]设计一种应用于即时通信的匿名好友系统, 用于匿名更新好友密钥和在线状态. 在长周期进行用户密钥更新, 用户为每个好友都生成一份新公钥并发布到服务器上, 然后使用 PIR 从服务器检索好友的新公钥; 短周期进行用户状态更新, 用户生成自身的状态签名并发布到服务器上, 并使用 PIR 从服务器上检索好友的当前状态.

Riposte[67]是 PIR 思想的逆向应用, 提供发送者不可观测性. 用户生成 n (服务器数量) 个异或结果为明文 M 的随机字符串 M_i, 向每个服务器发送一个. 客户端从各服务器下载字符串 M_i 并异或得到明文 M. 另外, 引入审计服务器对用户消息写入位置进行验证来防止恶意用户破坏服务器上的消息.

Riffle[68]结合 Mix 网与 PIR, 服务器同时扮演中间节点和 PIR 副本两种角色. 客户端选取一个服务器作为主服务器. 在每个周期, 发送者将 Mix 加密后的密文提交到主服务器, 在 K 个服务器间以 Mix 网方式传递, 出口服务器得到明文后广播给所有服务器, 因此其延迟为 $\theta(K)$. 使用 PIR 从服务器下载数据时, 使用两种策略降低带宽开销: (1) 引入伪随机数生成器让所有非主服务器自动更新掩码, 避免每次检索都需要向服务器发送掩码; (2) 接收者使用主服务器代替自己进行 PIR 检索, 再将结果返回给自己, 并通过预先向所有非主服务器分配一套额外掩码防止主服务器识别接收者.

基于 PIR 的匿名网络设计主要针对两方面优化: 一是将对 PIR 技术本身的改进应用于匿名网络, 如 pMIX 的 cPIR 和 DP5 的 PIR 改进方案; 二是为发送者提供匿名性或不可观测性, 通常将 PIR 与其他匿名思想结合, 如 the Pynchon Gate 和 Riffle 结合 PIR 和 Mix 网. 鉴于 PIR 本身的特点, 基于 PIR 的匿名网络设计均为 C/S 结构和同步网络. 除 DP5 外, 均采用匀速混淆策略生成虚拟 PIR 请求, 实现接收者不可观测性, 带宽开销为 $\theta(N/N)$. 另外, the Pynchon Gate 和 Riffle 采用的 Mix 网路由策略分别为随机和固定. 表 4 对此类工作进行比较分析.

表 4 基于 PIR 的匿名网络分析

匿名网络	匿名性	网络结构	时间假设	路由策略	流量混淆	延迟	带宽开销
The Pynchon Gate[61]	发送者匿名性接收者不可观测性	C/S	同步	随机	匀速	$\theta(1)$	$\theta(N/N)$
pMIX[62,63]	接收者不可观测性	C/S	同步	无	匀速	$\theta(1)$	$\theta(N/N)$
DP5[65]	接收者匿名性	C/S	同步	无	无	$\theta(1)$	$\theta(1/N)$
Riposte[67]	发送者不可观测性	C/S	同步	无	匀速	$\theta(1)$	$\theta(N/N)$
Riffle[68]	不可观测性	C/S	同步	固定	匀速	$\theta(K)$	$\theta(N/N)$

6 其他匿名网络

本节介绍的匿名网络均不基于 Mix 网、DC 网和 PIR 这 3 种基础匿名网络中的任意一种, 表 5 对各工作进行比较分析.

表 5 其他匿名网络分析

匿名网络	设计思路	匿名性	网络结构	时间假设	流量混淆	延迟	带宽开销
Anonymizer[69]	消息中转	发送者匿名性	C/S	异步	无	$\theta(1)$	$\theta(1/N)$
LPWA[70]	消息中转	发送者匿名性	C/S	异步	无	$\theta(1)$	$\theta(1/N)$
Crowd[71]	消息中转	发送者匿名性	P2P	异步	无	$\theta(1)$	$\theta(1/N)$
Freenet[72]	消息中转	发送者匿名性	P2P	异步	无	$\theta(1)$	$\theta(1/N)$
P^5[73]	逻辑广播	不可观测性	P2P	异步	匀速	$\theta(\log N)$	$\theta(N/N)$
Buses[74]	逻辑广播	不可观测性	P2P	同步	匀速	$\theta(N)$	$\theta(N/N)$
MIPNets[75]	逻辑广播	不可观测性	C/S	同步	匀速	$\theta(N)$	$\theta(N/N)$

6.1 基于消息中转的匿名网络

Anonymizer[69]和 LPWA[70]是两个早期匿名 Web 浏览工具. 核心思想是通过单代理提供匿名, 即用户将 Web 请求发送到代理服务器, 再由代理服务器转发到目标网站. Anonymizer 过滤掉网页中可能暴露用户隐私的内容, 并将内嵌的网页链接改写成需经过代理访问的形式. LPWA 根据用户的用户名、密码和网站 IP 地址为用户生成一个网站别名, 用户使用别名访问网站.

Crowd[71]是基于多代理的 P2P 匿名 Web 浏览工具. 任意两节点间消息传递均采用共享密钥加密. 当用户访问某网站时, 由本地 jondo 代理发起请求, 随机选取下一跳 jondo 节点. 当 jondo 收到请求时, 以概率 p>1/2 选择将请求转发给随机 jondo 节点, 以概率 1–p 转发给接收者. 经过的每个 jondo 节点记录上一跳和下一跳, 由同一 jondo 代理发起的请求均按相同路径转发, 接收者回复时按原路径返回.

Freenet[72]是 P2P 匿名文件存储与检索系统. 网络中的每个节点同时扮演文件缓存节点和路由节点, 并根据 key 对网络中存储的所有文件进行索引. 文件发布者计算待存储文件的 key, 并将文件上传到若干缓存节点. 检索数据时, 用户采用回溯法根据 key 生成检索请求, 对相邻节点不断检索, 直到缓存命中, 缓存节点将文件按原路返回给用户. 用户扮演匿名网络的发送者角色, 且在回溯检索过程中中间节点仅能知道其邻居节点检索某文件, 无法得知真实的发送者身份, 因此 Freenet 具有发送者匿名性.

此类匿名网络均通过消息中转实现匿名, 具有发送者匿名性, 运行在异步网络上且不采用任何流量混淆策略, 其延迟和带宽开销分别为 $\theta(1)$ 和 $\theta(1/N)$. Anonymizer 和 LPWA 的匿名性以单台代理服务器可信为前提, 其网络结构为 C/S 结构. Crowd 通过多个随机中间节点转发消息, 类似 Mix 网, 但相比之下是一种更轻量级的协议. 而 Freenet 则是通过文件缓存使得发送者不必将文件直接发给接收者, 来间接提供匿名.

6.2 基于逻辑广播的匿名网络

P^5[73]中所有用户被组织成二叉树, 树上每个节点代表一个用户组, 用户依其公钥被映射到一个组中. 发送者将消息广播给组内用户、祖先节点和子孙节点, 其他节点收到消息时也进行相同操作, 直到广播给所有节点. 其通信类似于遍历二叉树操作, 因此延迟为 $\theta(\log N)$.

Buses[74]的设计思想源于公交运输系统, 将所有消息组织为一个二维数组消息, 该二维数组消息类似一辆公交车, 在由所有节点组成的欧拉环上进行单向传输. 当公交车经过某节点时, 该节点读取接收地址为自己的消息, 并写入待发送消息或虚拟消息. 为降低延迟, 可在网络中相邻节点间设置双向、多辆公交车通信, 令消息经过最短路径传输.

MIPNets[75]以不知情代理 (oblivious proxy, OP) 为中心, 客户端组织成环状拓扑. OP 存储所有消息, 并依次与每个客户端交互. 为保证 OP 对客户端间的通信完全不知情, 客户端和 OP 间使用安全函数计算 (secure function evaluation)[76]进行交互. 当客户端发送消息时, 根据发送者和接收者编号确定位置并写入从 OP 获得的长消息, 然后用自己与下一个客户端间共享密钥加密长消息并发送给 OP; 下一个客户端从 OP 接收长消息并用与前一个客户端间共享密钥解密后读取消息, 接着执行上述发送过程. 通过这种客户端与 OP 间依次交互的方式间接实现客户端间的逻辑广播.

P^5、Busus 和 MIPNets 的本质均是通过逻辑广播来实现匿名, 均具有不可观测性, 采用匀速流量混淆策略, 带宽开销为 $\theta(1/N)$. 但三者的实现方式有所不同: P^5 将节点组织成二叉树结构, 通过遍历二叉树来实现逻辑广播, 进而降低通信延迟; Busus 则通过遍历由所有节点组成的欧拉环来实现逻辑广播; MIPNets 采用以代理服务器为中心的星型结构, 由代理服务器依次与各用户交互来实现逻辑广播.

7 展 望

匿名网络经过近 40 年的发展, 如今已支持绝大多数常见网络应用. 但受延迟、可扩展性及网络审查的制约, 匿名网络尚未在互联网上普及. 未来匿名网络研究可从以下方向展开: (1) 针对特定应用场景设计专用性强的高性能匿名网络, 如针对非延迟敏感型应用可采用同步假设及更复杂的路由策略、转发混合和流量混淆来实现不可观

测性, 针对用户规模较大的应用采用带宽开销较低的消息中转匿名思想, 针对接收者身份敏感型应用采用能提供接收者匿名性或接收者不可观测性的匿名思想; (2) 将新型隐私保护技术应用在匿名网络中来进一步提高匿名网络性能, 如可验证的洗牌[54]可用于在消息被重新排列并加密后验证其正确性, 差分隐私[53]通过加入噪音来最大限度地减少在服务器暂存消息时对手可观察到的服务器变化信息; (3) 在未来网络架构下的匿名研究, 当前匿名网络的研究均基于主机到主机的通信模型, 而未来互联网架构可能不采用该模型, 这可能会推翻现有匿名网络概念、匿名思想及方法等, 如 NDN[77]中以数据获取为通信模型, 消费者 (接收者) 的消息来源可能是节点缓存而非生产者 (发送者), 依据现有的匿名性定义, NDN 本身就具有发送者匿名性, 在此类新型互联网架构下进行匿名研究将面临新挑战.

References:

[1] Chaum DL. Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM, 1981, 24(2): 84–90. [doi: 10.1145/358549.358563]

[2] Dingledine R, Mathewson N, Syverson P. Tor: The second-generation onion router. Journal of the Franklin Institute, 2004, 239(2): 135–139.

[3] Chaum D. The dining cryptographers problem: Unconditional sender and recipient untraceability. Journal of Cryptology, 1988, 1(1): 65–75. [doi: 10.1007/BF00206326]

[4] Kesdogan D, Borning M, Schmeink M. Unobservable surfing on the World Wide Web: Is private information retrieval an alternative to the Mix based approach? In: Proc. of the 2nd Int'l Workshop on Privacy Enhancing Technologies. San Francisco: Springer, 2002. 224–238. [doi: 10.1007/3-540-36467-6_17]

[5] Chor B, Goldreich O, Kushilevitz E, Sudan M. Private information retrieval. In: Proc. of the 36th IEEE Annual Foundations of Computer Science. Milwaukee: IEEE, 1995. 41–50. [doi: 10.1109/SFCS.1995.492461]

[6] Edman M, Yener B. On anonymity in an electronic society: A survey of anonymous communication systems. ACM Computing Surveys, 2009, 42(1): 5. [doi: 10.1145/1592451.1592456]

[7] Ren J, Wu J. Survey on anonymous communications in computer networks. Computer Communications, 2010, 33(4): 420–431. [doi: 10.1016/j.comcom.2009.11.009]

[8] Shirazi F, Simeonovski M, Asghar MR, Backes M, Diaz C. A survey on routing in anonymous communication protocols. ACM Computing Surveys, 2019, 51(3): 51. [doi: 10.1145/3182658]

[9] Unger N, Dechand S, Bonneau J, Fahl S, Perl H, Goldberg I, Smith M. SoK: Secure messaging. In: Proc. of the 2015 IEEE Symp. on Security and Privacy. San Jose: IEEE, 2015. 232–249. [doi: 10.1109/SP.2015.22]

[10] Sampigethaya K, Poovendran R. A survey on mix networks and their secure applications. Proc. of the IEEE, 2006, 94(12): 2142–2181. [doi: 10.1109/JPROC.2006.889687]

[11] Wu YH, Wang WP, Chen JE. Anonymous communication: A survey. Journal of Chinese Computer Systems, 2007, 28(4): 583–588 (in Chinese with English abstract). [doi: 10.3969/j.issn.1000-1220.2007.04.002]

[12] Luo JZ, Yang M, Ling Z, Wu WJ, Gu XD. Anonymous communication and Darknet: A survey. Journal of Computer Research and Development, 2019, 56(1): 103–130 (in Chinese with English abstract). [doi: 10.7544/issn1000-1239.2019.20180769]

[13] Zhao H, Wang LM, Shen TH, Huang L, Ni XL. Survey on anonymity metrics in communication network. Ruan Jian Xue Bao/Journal of Software, 2021, 32(1): 218–245 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/6103.htm [doi: 10.13328/j.cnki.jos.006103]

[14] Hevia A, Micciancio D. An indistinguishability-based characterization of anonymous channels. In: Proc. of the 8th Int'l Symp. on Privacy Enhancing Technologies Symp. Leuven: Springer, 2008. 24–43. [doi: 10.1007/978-3-540-70630-4_3]

[15] Das D, Meiser S, Mohammadi E, Kate A. Anonymity trilemma: Strong anonymity, low bandwidth overhead, low latency-choose two. In: Proc. of the 2018 IEEE Symp. on Security and Privacy. San Francisco: IEEE, 2018. 108–126. [doi: 10.1109/SP.2018.00011]

[16] Erdin E, Zachor C, Gunes MH. How to find hidden users: A survey of attacks on anonymity networks. IEEE Communications Surveys & Tutorials, 2015, 17(4): 2296–2316. [doi: 10.1109/COMST.2015.2453434]

[17] Pfitzmann A, Hansen M. A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management. 2010.

[18] Wright M, Adler M, Levine BN, Shields C. Defending anonymous communications against passive logging attacks. In: Proc. of the 2003 Symp. on Security and Privacy. Berkeley: IEEE, 2003. 28–41. [doi: 10.1109/SECPRI.2003.1199325]

[19] Bauer K, McCoy D, Grunwald D, Kohno T, Sicker D. Low-resource routing attacks against tor. In: Proc. of the 2007 ACM Workshop on Privacy in Electronic Society. Alexandria: ACM, 2007. 11–20. [doi: 10.1145/1314333.1314336]

[20] Pries R, Yu W, Fu XW, Zhao W. A new replay attack against anonymous communication networks. In: Proc. of the 2008 IEEE Int'l Conf. on Communications. Beijing: IEEE, 2008. 1578–1582. [doi: 10.1109/ICC.2008.305]

[21] Ling Z, Luo JZ, Yu W, Fu XW, Xuan D, Jia WJ. A new cell counter based attack against tor. In: Proc. of the 16th ACM Conf. on Computer and Communications Security. Chicago: ACM, 2009. 578–589. [doi: 10.1145/1653662.1653732]

[22] Serjantov A, Dingledine R, Syverson P. From a trickle to a flood: Active attacks on several mix types. In: Proc. of the 5th Int'l Workshop on Information Hiding. Noordwijkerhout: Springer, 2002. 36–52. [doi: 10.1007/3-540-36415-3_3]

[23] Cypherpunk anonymous remailer. https://en.wikipedia.org/wiki/Cypherpunk_anonymous_remailer.

[24] Möller U, Cottrell L, Palfrader P, Sassaman L. Mixmaster protocol—Version 2. IETF Internet Draft, 2003.

[25] Díaz C, Sassaman L, Dewitte E. Comparison between two practical mix designs. In: Proc. of the 9th European Symp. on Research in Computer Security. Sophia Antipolis: Springer, 2004. 141–159. [doi: 10.1007/978-3-540-30108-0_9]

[26] Danezis G, Dingledine R, Mathewson N. Mixminion: Design of a type III anonymous remailer protocol. In: Proc. of the 2003 Symp. on Security and Privacy. Berkeley: IEEE, 2003. 2–15. [doi: 10.1109/SECPRI.2003.1199323]

[27] Gulcu C, Tsudik G. Mixing E-mail with babel. In: Proc. of Internet Society Symp. on Network and Distributed Systems Security. San Diego: IEEE, 1996. 2–16. [doi: 10.1109/NDSS.1996.492350]

[28] Gelernter N, Herzberg A, Leibowitz H. Two cents for strong anonymity: The anonymous post-office protocol. In: Proc. of the 16th Int'l Conf. on Cryptology and Network Security. Hong Kong: Springer, 2018. 390–412. [doi: 10.1007/978-3-030-02641-7_18]

[29] Goldschlag DM, Reed MG, Syverson PF. Hiding routing information. In: Anderson R, ed. Information Hiding. Berlin, Heidelberg: Springer, 1996. 137–150. [doi: 10.1007/3-540-61996-8_37]

[30] Kate A, Zaverucha GM, Goldberg I. Pairing-based onion routing with improved forward secrecy. ACM Trans. on Information and System Security, 2010, 13(4): 29. [doi: 10.1145/1880022.1880023]

[31] Catalano D, Fiore D, Gennaro R. Certificateless onion routing. In: Proc. of the 16th ACM Conf. on Computer and Communications Security. Chicago: ACM, 2009. 151–160. [doi: 10.1145/1653662.1653682]

[32] Doshi N, Jinwala D. AB-OR: Improving the efficiency in onion routing using attribute based cryptography. In: Chaki N, Meghanathan N, Nagamalai D, eds. Computer Networks & Communications (NetCom). New York: Springer, 2013. 425–432. [doi: 10.1007/978-1-4614-6154-8_42]

[33] Chen C, Asoni DE, Barrera D, Danezis G, Perrig A. HORNET: High-speed onion routing at the network layer. In: Proc. of the 22nd ACM SIGSAC Conf. on Computer and Communications Security. Denver: ACM, 2015. 1441–1454. [doi: 10.1145/2810103.2813628]

[34] Mokhtar SB, Berthou G, Diarra A, Quéma V, Shoker A. RAC: A freerider—Resilient, scalable, anonymous communication protocol. In: Proc. of the 33rd Int'l Conf. on Distributed Computing Systems. Philadelphia: IEEE, 2013. 520–529. [doi: 10.1109/ICDCS.2013.52]

[35] The invisible internet project. https://geti2p.net/

[36] Heydt-Benjamin TS, Serjantov A, Defend B. Nonesuch: A mix network with sender unobservability. In: Proc. of the 5th ACM Workshop on Privacy in Electronic Society. Alexandria: ACM, 2006. 1–8. [doi: 10.1145/1179601.1179603]

[37] Le Blond S, Choffnes D, Zhou WX, Druschel P, Ballani H, Francis P. Towards efficient traffic-analysis resistant anonymity networks. ACM SIGCOMM Computer Communication Review, 2013, 43(4): 303–314. [doi: 10.1145/2534169.2486002]

[38] Le Blond S, Choffnes D, Caldwell W, Druschel P, Merritt N. Herd: A scalable, traffic analysis resistant anonymity network for VoIP systems. In: Proc. of the 2015 ACM Conf. on Special Interest Group on Data Communication. London: ACM, 2015. 639–652. [doi: 10.1145/2785956.2787491]

[39] Golle P, Juels A. Parallel mixing. In: Proc. of the 11th ACM Conf. on Computer and Communications Security. Washington: ACM, 2004. 220–226. [doi: 10.1145/1030083.1030113]

[40] van den Hooff J, Lazar D, Zaharia M, Zeldovich N. Vuvuzela: Scalable private messaging resistant to traffic analysis. In: Proc. of the 25th Symp. on Operating Systems Principles. Monterey: ACM, 2015. 137–152. [doi: 10.1145/2815400.2815417]

[41] Lazar D, Zeldovich N. Alpenhorn: Bootstrapping secure communication without leaking metadata. In: Proc. of the 12th USENIX Conf. on Operating Systems Design and Implementation. Savannah: USENIX Association, 2016. 571–586.

[42] Tyagi N, Gilad Y, Leung D, Zaharia M, Zeldovich N. Stadium: A distributed metadata-private messaging system. In: Proc. of the 26th Symp. on Operating Systems Principles. Shanghai: ACM, 2017. 423–440. [doi: 10.1145/3132747.3132783]

[43] Chaum D, Das D, Javani F, Kate A, Krasnova A, Ruiter J, Sherman A. cMix: Mixing with minimal real-time asymmetric cryptographic operations. In: Proc. of the Int'l Conf. on Applied Cryptography and Network Security. Cham: Springer, 2017. 557–578.

[44] Kwon A, Corrigan-Gibbs H, Devadas S, Ford B. Atom: Horizontally scaling strong anonymity. In: Proc. of the 26th Symp. on Operating

Systems Principles. Shanghai: ACM, 2017. 406–422. [doi: 10.1145/3132747.3132755]

[45] Piotrowska AM, Hayes J, Elahi T, Meiser S, Danezis G. The loopix anonymity system. In: Proc. of the 26th USENIX Conf. on Security Symp. Vancouver: USENIX Association, 2017. 1199–1216.

[46] Mazières D, Kaashoek MF. The design, implementation and operation of an email pseudonym server. In: Proc. of the 5th ACM Conf. on Computer and Communications Security. San Francisco: ACM, 1998. 27–36. [doi: 10.1145/288090.288098]

[47] Okamoto E, Okamoto T. Cryptosystems based on elliptic curve pairing. In: Proc. of the 2nd Int'l Conf. on Modeling Decisions for Artificial Intelligence. Tsukuba: Springer, 2005. 13–23. [doi: 10.1007/11526018_3]

[48] Boneh D, Franklin M. Identity-based encryption from the weil pairing. In: Proc. of the 21st Annual Int'l Cryptology Conf. Santa Barbara: Springer, 2001. 213–229. [doi: 10.1007/3-540-44647-8_13]

[49] Al-Riyami SS, Paterson KG. Certificateless public key cryptography. In: Proc. of the 9th Int'l Conf. on the Theory and Application of Cryptology and Information Security. Taipei: Springer, 2003. 452–473. [doi: 10.1007/978-3-540-40061-5_29]

[50] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption. In: Proc. of the 2007 IEEE Symp. on Security and Privacy. Berkeley: IEEE, 2007. 321–334. [doi: 10.1109/SP.2007.11]

[51] Danezis G, Goldberg I. Sphinx: A compact and provably secure mix format. In: Proc. of the 30th IEEE Symp. on Security and Privacy. Oakland: IEEE, 2009. 269–282. [doi: 10.1109/SP.2009.15]

[52] Danezis G, Laurie B. Minx: A simple and efficient anonymous packet format. In: Proc. of the 2004 ACM Workshop on Privacy in the Electronic Society. Washington: ACM, 2004. 59–65. [doi: 10.1145/1029179.1029198]

[53] Dwork C, Roth A. The algorithmic foundations of differential privacy. Foundations and Trends® in Theoretical Computer Science, 2014, 9(3–4): 211–407. [doi: 10.1561/0400000042]

[54] Bayer S, Groth J. Efficient zero-knowledge argument for correctness of a shuffle. In: Proc. of the 31st Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Cambridge: Springer, 2012. 263–280. [doi: 10.1007/978-3-642-29011-4_17]

[55] Benaloh J. Simple verifiable elections. In: Proc. of the USENIX/ACCURATE Electronic Voting Technology Workshop 2006 on Electronic Voting Technology Workshop. Vancouver: USENIX Association, 2006. 5.

[56] Khazaei S, Moran T, Wikström D. A Mix-net from any CCA2 secure cryptosystem. In: Proc. of the 18th Int'l Conf. on the Theory and Application of Cryptology and Information Security. Beijing: Springer, 2012. 607–625. [doi: 10.1007/978-3-642-34961-4_37]

[57] Goel S, Robson M, Polte M, Sirer E. Herbivore: A scalable and efficient protocol for anonymous communication. Technical Report, Cornell University Computing and Information Science, 2003.

[58] Wolinsky DI, Corrigan-Gibbs H, Ford B, Johnson A. Dissent in numbers: Making strong anonymity scale. In: Proc. of the 10th USENIX Symp. on Operating Systems Design and Implementation. Hollywood: USENIX Association, 2012. 179–182.

[59] Corrigan-Gibbs H, Wolinsky DI, Ford B. Proactively accountable anonymous messaging in verdict. In: Proc. of the 22nd USENIX Security Symp. Washington: USENIX Association, 2013. 147–162.

[60] Ruffing T, Moreno-Sanchez P, Kate A. P2P mixing and unlinkable bitcoin transactions. In: Proc. of the 24th Annual Network and Distributed System Security Symp. San Diego: The Internet Society, 2017. 824.

[61] Sassaman L, Cohen B, Mathewson N. The Pynchon Gate: A secure method of pseudonymous mail retrieval. In: Proc. of the 2005 ACM Workshop on Privacy in the Electronic Society. Alexandria: ACM, 2005. 1–9. [doi: 10.1145/1102199.1102201]

[62] Melchor CA, Deswarte Y. pMIX: Untraceability for small hiding groups. In: Proc. of the 4th IEEE Int'l Symp. on Network Computing and Applications. Cambridge: IEEE, 2005. 29–40. [doi: 10.1109/NCA.2005.40]

[63] Melchor CA, Deswarte Y. From DC-nets to pMIXes: Multiple variants for anonymous communications. In: Proc. of the 5th IEEE Int'l Symp. on Network Computing and Applications. Cambridge: IEEE, 2006. 163–172. [doi: 10.1109/NCA.2006.32]

[64] Kushilevitz E, Ostrovsky R. Replication is not needed: Single database, computationally-private information retrieval. In: Proc. of the 38th Annual Symp. on Foundations of Computer Science. Miami Beach: IEEE, 1997. 364–373. [doi: 10.1109/SFCS.1997.646125]

[65] Borisov N, Danezis G, Goldberg I. DP5: A private presence service. Proc. on Privacy Enhancing Technologies, 2015, 2015(2): 4–24. [doi: 10.1515/popets-2015-0008]

[66] Devet C, Goldberg I, Heninger N. Optimally robust private information retrieval. In: Proc. of the 21st USENIX Security Symp. Bellevue: USENIX Association, 2012. 269–283.

[67] Corrigan-Gibbs H, Boneh D, Mazières D. Riposte: An anonymous messaging system handling millions of users. In: Proc. of the 2015 IEEE Symp. on Security and Privacy. San Jose: IEEE, 2015. 321–338. [doi: 10.1109/SP.2015.27]

[68] Kwon AH, Lazar D, Devadas S, Ford B. Riffle: An efficient communication system with strong anonymity. Proc. on Privacy Enhancing Technologies, 2016, 2016(2): 115–134. [doi: 10.1515/popets-2016-0008]

[69] Boyan J. The anonymizer: Protecting user privacy on the Web. Computer-mediated Communication Magazine, 1997, 4(9).

[70] Kristol DM, Gabber E, Gibbons PB, Matias Y, Mayer A. Design and implementation of the Lucent Personalized Web Assistant (LPWA). Information Sciences Research Center, Bell Laboratories, Lucent Technologies, 1998.

[71] Reiter MK, Rubin AD. Anonymous Web transactions with crowds. Communications of the ACM, 1999, 42(2): 32–48. [doi: 10.1145/293411.293778]

[72] Clarke I, Sandberg O, Wiley B, Hong TW. Freenet: A distributed anonymous information storage and retrieval system. In: Federrath H, ed. Designing Privacy Enhancing Technologies. Berlin, Heidelberg: Springer, 2001. 46–66. [doi: 10.1007/3-540-44702-4_4]

[73] Sherwood R, Bhattacharjee B, Srinivasan A. P^5: A protocol for scalable anonymous communication. Journal of Computer Security, 2005, 13(6): 839–876. [doi: 10.3233/JCS-2005-13602]

[74] Beimel A, Dolev S. Buses for anonymous message delivery. Journal of Cryptology, 2003, 16(1): 25–39. [doi: 10.1007/s00145-002-0128-6]

[75] Nipane N, Dacosta I, Traynor P. “Mix-in-place” anonymous networking using secure function evaluation. In: Proc. of the 27th Annual Computer Security Applications Conf. Orlando: ACM, 2011: 63–72. [doi: 10.1145/2076732.2076742]

[76] Malkhi D, Nisan N, Pinkas B, Sella Y. Fairplay—A secure two-party computation system. In: Proc. of the 13th Conf. on Usenix Security Symp. San Diego: USENIX Association, 2004. 20.

[77] Zhang LX, Afanasyev A, Burke J, Jacobson V, Claffy KC, Crowley P, Papadopoulos C, Wang L, Zhang BC. Named data networking. ACM SIGCOMM Computer Communication Review, 2014, 44(3): 66–73. [doi: 10.1145/2656877.2656887]

附中文参考文献:

[11] 吴艳辉, 王伟平, 陈建二. 匿名通信研究综述. 小型微型计算机系统, 2007, 28(4): 583–588. [doi: 10.3969/j.issn.1000-1220.2007.04.002]

[12] 罗军舟, 杨明, 凌振, 吴文甲, 顾晓丹. 匿名通信与暗网研究综述. 计算机研究与发展, 2019, 56(1): 103–130. [doi: 10.7544/issn1000-1239.2019.20180769]

[13] 赵蕙, 王良民, 申屠浩, 黄磊, 倪晓铃. 网络匿名度量研究综述. 软件学报, 2021, 32(1): 218–245. http://www.jos.org.cn/1000-9825/6103.htm [doi: 10.13328/j.cnki.jos.006103]

马传旺(1992－), 男, 博士生, CCF 学生会员, 主要研究领域为匿名网络, 拜占庭容错共识.

方滨兴(1960－), 男, 博士, 教授, 博士生导师, 主要研究领域为网络与信息安全的理论与技术.

张宇(1979－), 男, 博士, 副教授, 主要研究领域为互联网关键资源安全, 网络拓扑测量, 未来网络体系系统.

张宏莉(1973－), 女, 博士, 教授, 博士生导师, 主要研究领域为网络安全, 网络测量, 网络计算.