ISSN 1673-9418 CODEN JKYTA8
Journal of Frontiers of Computer Science and Technology
1673-9418/2009/03(01)-0001-17
DOI:10.3778/j.issn.1673-9418.2009.01.001

E-mail:fcst@public2.bta.net.cn
http://www.ceaj.org
Tel:+86-10-51616056

基于互联网的匿名技术研究 *

陆天波[1+],时金桥[2],程学旗[2]
1. 国家计算机网络应急技术处理协调中心,北京 100029
2. 中国科学院 计算技术研究所,北京 100190

A Survey of Anonymity on the Internet*

LU Tianbo[1+], SHI Jinqiao[2], CHENG Xueqi[2]
1. National Computer Network Emergency Response Technical Team/Coordination Center of China, Beijing 100029, China
2. Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100190, China
+ Corresponding author: E-mail: lutianbo@software.ict.ac.cn

LU Tianbo, SHI Jinqiao, CHENG Xueqi. A survey of anonymity on the Internet. Journal of Frontiers of Computer Science and Technology, 2009,3(1):1-17.

Abstract: With the world-wide fast developing of Internet, it has come true to share information on the network. And information security and privacy has gained more and more attention. Anonymity is the privacy of user identification, which has been the basis requirement of many network applications. Firstly, an overview of existing and proposed techniques that can provide anonymity on the Internet is given, the current trends and developments in this area are analyzed. Then a research agenda for anonymity is proposed.

Key words: anonymity; MIX; DC-Net; traffic analysis

摘 要:随着互联网在世界范围内的迅猛发展,通过网络已逐步实现了全社会的信息共享,由此带来的信息安全与隐私问题也逐步受到人们的广泛关注。匿名是指用户身份信息的隐私,已经成为许多网络应用的基本需求。总结了匿名技术二十多年来的研究进展情况,提出了该领域面临的挑战及发展趋势。

* The National Grand Fundamental Research 973 Program of China under Grant No.2004CB318109,2007CB311100 (国家重点基础研究发展计划(973)); the National High-Tech Research and Development Plan of China under Grant No.2006AA01Z452 (国家高技术研究发展计划(863)).
Received 2008-07, Accepted 2008-09.

关键词:匿名;MIX 机制;DC-Net 协议;流量分析
文献标识码:A **中图分类号**:TP393

1 引言

随着互联网在世界范围内的迅猛发展,通过网络已逐步实现了全社会的信息共享,由此带来的信息安全与隐私问题也逐渐受到人们的广泛关注。匿名是指保护用户身份信息的隐私,已经成为很多网络应用的基本需求。在电子商务、电子选举、电子拍卖、Web 浏览、电子邮件、即时通信、在线医疗咨询以及军事通信、情报通信等各种网络应用中,都需要保护用户身份以及通信关系等隐私信息不被泄漏。然而,当前的互联网协议并不支持匿名性保护,网络管理人员、网络服务提供商甚至非法监听者都可以通过各种手段来获取网络使用者的身份信息、行为习惯等,来危害个人隐私。尽管加密协议(如 SSL、TSL、IPSec 等)可以防止对通信过程中传递的信息内容进行窃听和分析,但是通过对网络数据报文的分析仍能解析出通信的源地址、目的地址、报文长度、通信时间以及通信频率等,从而获知通信者的身份信息、网络行为特征或通信者之间的对应关系,危害个人隐私。在这种情况下,网络匿名通信技术作为一种保护网络用户隐私的基本手段,已经成为学术界、企业界甚至国家安全部门普遍关注的重要技术。

网络匿名通信技术的基本目的是保护通信参与者的身份信息不被泄漏。图 1 以非常通用的术语给出了网络匿名通信技术的研究框架,它由消息的发送者 S、接收者 R、消息 M,匿名系统接口 I、匿名通信信道 T 和攻击者 A 构成。框架中信息的发送者、接收者为参与通信的双方,通过匿名系统接口与匿名通信信道传递消息 M。匿名通信系统由一组互连的匿名通信构件 C 组成,它们是匿名通信的基础设施,目标是为其上的匿名消息传递提供保障。匿名通信构件相互协作,对发送者的消息进行变换、延迟等操作(如消息编码、插入掩护流量等),并将变换后的消息 M' 传递给接收方处的匿名通信接口。接收方的匿名通信接口将接收到的消息 M' 还原成初始消息 M 传递给接收者 R。匿名通信的攻击者通过对通信基础设施甚至接收者进行流量分析、数据分析等方法破坏系统的匿名服务,目的是获取匿名通信参与者的身份信息或通信关系等信息。网络匿名通信技术的研究框架给出了两个研究要点:

(1)匿名机制与匿名协议的设计:设计安全、可靠、高效、实用的匿名通信协议,保障匿名通信参与者的身份不被泄漏;

(2)匿名系统的攻击分析:分析匿名通信协议所有可能受到的攻击,并研究相应对策;分析匿名通信系统的匿名性能。

匿名技术的研究始于 1981 年,Chaum 提出消息混合(MIX)[1]的思想并将其应用到不可追踪的电子邮件系统中,成为此领域的开创性技术。最初十年中,由

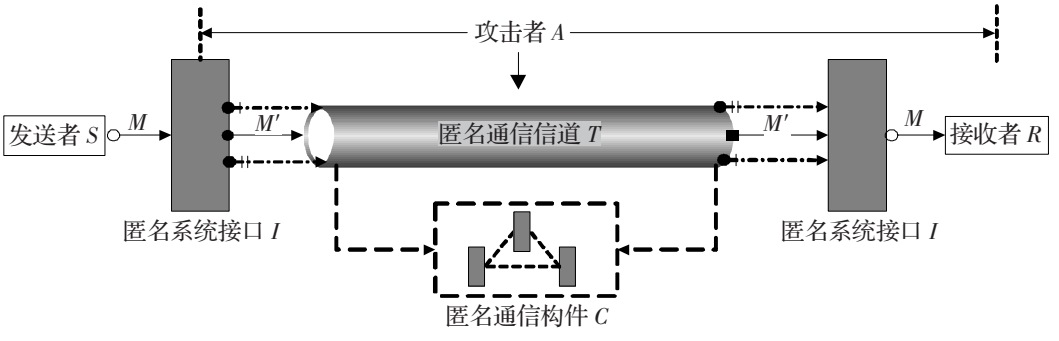

Fig.1 Research framework of anonymous communication techniques

图 1 网络匿名通信技术的研究框架

于互联网尚未普及,针对网络匿名技术的研究并不多见，但是，在此阶段提出的一些基本匿名机制如MIX、DC-Net[2]等为匿名技术的研究奠定了非常坚实的基础,这些匿名机制至今仍广为应用。进入20世纪90年代，伴随着通信网络尤其是互联网的飞速发展以及新的网络应用的不断产生与普及,匿名技术得到了长足地发展。本文针对互联网上匿名技术进行研究,从匿名的定义与衡量方法、匿名实现机制以及匿名系统的攻击技术分析等方面总结匿名技术的研究进展与现状,并探讨匿名技术未来的研究方向。

2 匿名的定义及度量

2.1 匿名的基本概念与分类

所谓匿名,是指“在一组对象的集合(即匿名集合,anonymity set)中不可识别的状态”[3]。匿名集合中的成员以及每个成员的概率大小依赖于攻击者的知识,匿名集合的大小可以用来评价匿名性的强弱,匿名集合的变化可以用来衡量攻击者对匿名系统的攻击效果。

根据通信过程中受保护角色的不同,通信系统中的匿名保护通常可以分为如下3种形式[3]:发送者匿名、接收者匿名和通信关系匿名。发送者匿名或接收者匿名的情况下一定是通信关系匿名的,但是通信关系匿名的前提下发送者或接收者不一定是匿名的。例如在某些情况下虽然发送者与接收者之间的通信关系是匿名的,但是通信双方却知道对方的身份。根据匿名保护实现机制的不同,通信系统中的匿名保护可以分为两类:计算匿名和信息理论匿名。其中计算匿名的基本假设是攻击者拥有的计算能力不足以破解匿名通信协议,而基于信息理论的匿名则依赖于无限计算能力都不可破解的问题。从匿名保护的层面来看,匿名可以分为数据匿名和连接匿名。数据匿名指的是在数据通信过程中过滤掉可能泄漏个人身份信息的数据,如cookie等,而连接匿名指的是在通信过程中网络连接本身不泄漏身份信息,攻击者不会通过流量分析来破坏匿名保护。

2.2 匿名性的度量方法

2.2.1 匿名性的定性描述

文献[4]给出了匿名等级的概念,最早对网络计算机系统中的匿名进行分级描述，匿名性被分为从“无用户标识”到“超级标识”6个等级。这是第一个对匿名性进行评价的尝试，但是评价方法是定性的,并且不是基于匿名集合概念的。

Reiter和Rubin在分析Crowds系统[5]时提出匿名度的概念,用来描述和衡量匿名性能。匿名度被描述为从无匿名到完全匿名的连续区间,其间含有若干个关键点(如图1所示),并给出了各个关键点的非形式化定义。其中,probable innocence关键点定义为真实发送者，被攻击者判定为发起者的概率应该小于0.5。Crowds系统就是基于这种定义对系统进行匿名性分析的。

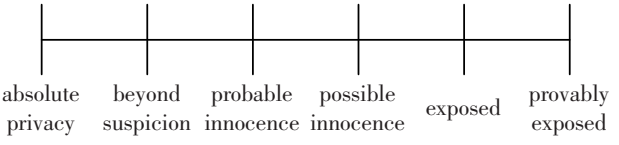

Fig.2 Degree of anonymity[5]

图2 匿名度[5]

2.2.2 匿名性的定量描述

Berthod等人给出了一种基于匿名集合大小的匿名度定义[6]。匿名度$A=\mathrm{lb}(N)$,其中N是可能的消息发送者的个数,也就是发送者匿名集合的大小。这种方法没有考虑到攻击者可能通过一定的攻击手段获得相关信息后,对匿名集合中对象判定概率的不一致性。因此,这种匿名度的定义方法无法表示攻击者进行攻击获得部分信息后匿名性的变化。

文献[7]提出了一种基于概率论的匿名度定义。Shields等强调在系统中的不同对象的匿名度并不是全部相同的。这种匿名度定义考虑了不同对象攻击者赋予的概率不同,因此更适合于描述单个对象的匿名度,但是在描述总匿名度时采用的是单个对象匿名度的最小值,无法精确反映整个系统的匿名保护程度。

基于信息论的匿名性描述方法是目前研究领域

广泛接受的方法。文献[8-9]分别独立给出了基于信息熵的匿名度定义方法。定义匿名集合为 $S=\{s_1,s_2,\cdots,s_N\}$,其中 $N=|S|$。定义 X 为离散随机变量,其概率密度函数为 $p_i=Pr(x=i)$。其实际意义为攻击者赋予匿名集合中的成员 s_i 的概率为 p_i,$\sum_{i=1}^{n}p_i=1$。则随机变量 X 的熵为:$H(X)=-\sum_{i=1}^{n}p_i\mathrm{lb}(p_i)$。定义 H_M 为最大熵,有 $H_M=\mathrm{lb}(N)$,则攻击者获得的信息可以表示为 $H_M-H(X)$。由此,可以定义匿名系统的匿名度为:

$$d=1-\frac{H_M-H(X)}{H_M}=\frac{H(X)}{H_M}$$

当匿名集合只有 1 个元素时,定义系统的匿名度为 0。$0\leqslant d\leqslant 1$,当匿名集合中的 1 个成员被认定是消息发送者的概率为 1 时,系统的匿名度最小,$d=0$;当匿名集合中所有的成员被认定为消息发送者的概率均相等时($p_i=1/N$),系统的匿名度最大,$d=1$。

这种定义方法不光考虑了匿名集合的大小,还考虑了匿名集合中不同成员的概率分布,因此能够更好地反映攻击者获取部分信息后匿名集合中成员概率分布的不均匀性。文献[10-13]也分别对基于信息论进行匿名性度量进行了研究。

3 匿名的实现机制与应用

3.1 匿名的实现机制

3.1.1 代理机制

代理通过修改消息的源地址向消息的接收者隐藏发送者的身份信息(这里指 IP 地址)。目前互联网上有大量的主机提供免费的 CGI 代理、HTTP 代理、Socks4 代理、Socks5 代理、加密代理等服务。三角男孩(triangle boy)是 SafeWeb 公司开发的一种分布式加密代理技术,它采用数据折射、地址伪装的技术,在隐匿数据请求者的地址信息的同时,还隐匿了数据回应者的地址信息。朗讯个性化 Web 助手(Lucent personalized Web assistant,LPWA)[14]也是一种基于代理的匿名通信技术,它的基本思想是作为本地代理转发用户的浏览请求,在用户访问网站时生成与个人信息无关的别名,从而隐藏用户的真实身份信息。

基于代理的匿名通信技术虽然能够对接收者隐匿发送者的身份信息,但是由于中间的代理服务器会知道用户的真实身份,因此代理服务器被攻占时,匿名保护就遭到破坏。

3.1.2 MIX

MIX 是目前应用最广泛的源重写类匿名实现机制。MIX 的基本思想非常简单:MIX 节点接收一定数量的消息,通过加密或填充(padding)等手段修改消息的外观(appearance),通过延迟(delaying)或重排序(reordering)等手段来修改消息的顺序(flow),从而以一种隐藏输入输出对应关系的方式输出消息,保证攻击者无法准确推断通信参与者的通信关系。多台 MIX 服务器可以以级联(MIX cascade)或网络(MIX network)的形式进行连接,在消息报文通过的一组 MIX 服务器中,只要有一台服务器正常工作,就可以保证系统的匿名性。

MIX 的消息刷新策略指的是 MIX 在存储转发过程中为了改变消息的顺序所采取的措施的统称,关系到 MIX 的匿名性以及消息延迟等特性,是 MIX 的设计与研究中最重要的内容之一。图 3 总结了 MIX 消息刷新策略的发展过程与分类,消息刷新策略主要可以分为批处理型策略(batching strategies)和连续型策略(continuous strategies)两大类,而批处理型刷新策略则经历了从简单策略到消息池策略到二项式策略的发展历程。消息刷新时机主要包括阈值策略、定时策略以及两者的不同方式结合。MIX 消息刷新策略在发展过程中,不断地在 MIX 消息存储转发过程中引入新的不确定性,目标是提高攻击者推断输入消息、输出消息对应关系的难度。此外,文献[15]给出了消息刷新策略的统一描述框架;国内的时金桥等人[16]对此框架进行扩展,提出了一种两阶段消息刷新策略通用描述框架,并在此框架下提出结合批处理策略和连续策略优点的混合型消息刷新策略。

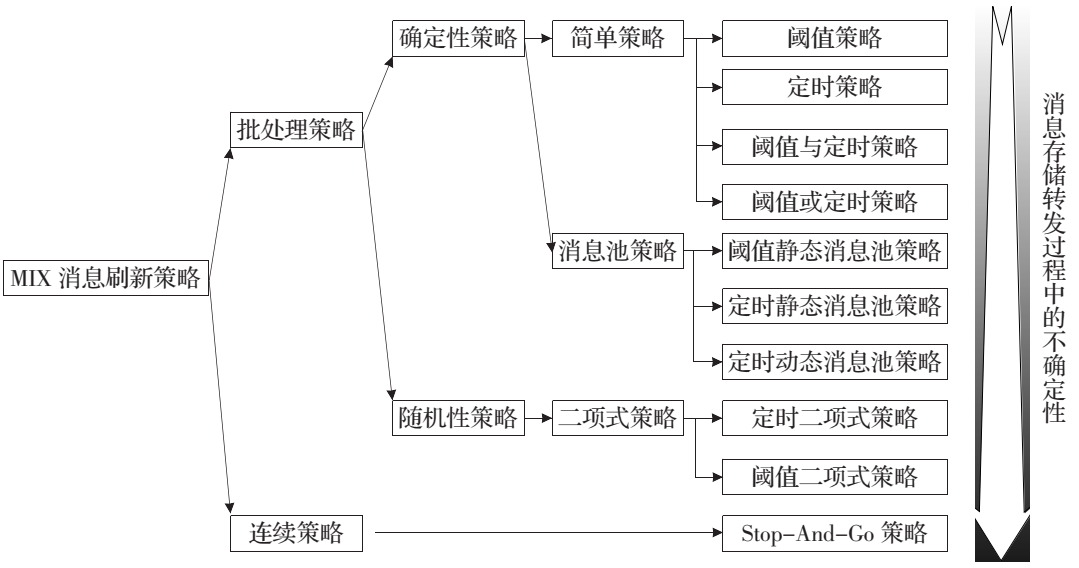

Fig.3 Messages flushing strategies of MIX

图 3 MIX 消息刷新策略

MIX 的报文组织格式主要可以分为分层加密和重加密两种方法。Chaum 提出的原始 MIX 采用的是分层加密的报文组织格式,文献[17]指出这种方法的缺点是消息报文的大小随 MIX 节点数的增加而增加,并提出了基于 ElGamal 加密方案的重加密 MIX。每台中间 MIX 服务器不再像传统的 MIX 服务器那样对消息进行解密,而是对消息进行重新加密后发送,其密文长度始终是明文长度的 2 倍,因此消息长度不会随着路径的增长而变大。Golle 等人在 2004 年提出了通用重加密 MIX 方案[18],对上述方案进行了巧妙地扩展,使得 MIX 在对消息进行重加密时不需要知道公钥信息。ElGamal 重加密 MIX 协议的弱点是不能像分层加密的 MIX 协议那样在消息报文中包含路由信息,因此就很难应用于自由路由拓扑结构的 MIX 网络中。文献[19-20]对此弱点进行了改进,提出 URE-Onion 的基于重加密的洋葱路由机制,可以将路由信息携带在消息报文中。但是文献[21]却发现这种方法的安全漏洞,指出通用重加密的密文可扩展特性和重加密语义容易带来安全隐患,必须小心使用。时金桥等人提出了一种改进的通用重加密报文结构以解决其安全隐患[16]。

可证明行为正确(verifiability)的健壮 MIX 方案也是 MIX 研究中的大热点,这类方案主要用于匿名投票。文献[22]提出了一个称为 receipt-free 的投票方案,这种方案具有通用可证明性(universal verifiability),即发送者能够证明所有的投票都被计数了,而不仅仅是自己的投票被计数。文献[23]提出对该协议的一种攻击方法。文献[24]提出了两个健壮的可证明的匿名通道方案,一个基于 r 轮剩余类问题,另一个基于 ElGamal 方案,并对前者进行了零知识证明。Abe 和 Jakobsson 于 1998 年分别提出了两个高效实用的可证明 MIX 协议[25-26],其中后者被 Desmedt 和 Kurosawa 证明是不安全的[27]。为了减少[26]方案中乱序的代价,Jakobsson 在 1999 年提出了 Flash MIX[28]。Mitomo 和 Kurosawa 后来发现了针对 Flash MIX 的一种攻击并对其进行了完善[29]。Furukawa 等人[30]和 Neff[31]在 2001 年分别提出了对 ElGamal 密文置乱的正确性进行有效证明的方案。文献[32]提出了一种优化的 MIX 方案。如果没有检测到攻击,则该方案的效率很高,但是一旦有错误发生,则该方案不输出任何结果。国内的研究者[33-35]也分别提出了安全匿名投票方案。

3.1.3 DC-Net 机制

DC-Net 是 Chaum 于 1984 年提出的一种基于信息理论的基本匿名通信机制,其实现基础是不可破解

的数学难题“密码员晚餐(dining cryptographer,DC)问题”[2]。DC-Net是一种基于消息广播的协议,提供发送者匿名服务,在存在可靠的广播隧道的前提下,保证接收者匿名。DC-Net协议简单而又安全地提供了匿名通信服务,但它却有着严重的缺陷:(1)匿名信息传输依赖于一个安全可靠的广播信道,即每个诚实参与者所广播的消息都被其他参与者未经修改地接收到。Waidner指出,可靠的广播是一种不现实的假设,它不可能通过密码学的手段来获得[36];(2)每次只能发送一条消息,否则会发生信道冲突;(3)消息数量巨大,每匿名发送一条消息都需要所有参与者广播一条消息,这在实际情况中是不可能的;(4)共享密钥数量巨大,在实际环境中,每次发送新消息时都需要协商生成新的密钥,这也是不现实的。

Cornell大学的CliqueNet系统[37]采用分治的思想对DC-Net协议进行了改进,目的是解决DC-Net协议效率低及可扩展性差的弱点。CliqueNet虽然在一定程度上缓解了广播通信流量大的问题,但它的路由层却带来了不必要的网络延迟。当网络规模比较大时,路由转发节点对包的转发量将急剧增加,成为网络的瓶颈。并且,它同样需要可靠的广播。Herbivior[38]是Cornell大学开发的另一个基于DC-Net协议构建的匿名通信系统,目标是保护发送者和接收者匿名,系统可扩展性好,提供高带宽低延迟的高效消息传输。CMU大学提出的k-anonymity协议[39]的思想与CliqueNet类似。它同样把整个网络分成许多小的类似于DC-Nets的单元。每个单元至少有k个诚实的用户,这样攻击者最多知道消息的发送者(或接收者)在这k个用户中,但并不知道是哪一个。该协议匿名传递一个消息需要传递$O(k^2)$个额外的消息,当k较大时,其通信流量还是很大,并且它同样需要可靠的广播。

3.1.4 Crowds

Crowds系统是AT&T实验室的Reiter和Rubin开发的系统[5],目的是保护用户Web浏览的匿名性,是最早的基于对等网络思想构建的匿名通信系统。Crowds的基本思想是消息在不同的转发服务器(称为jondo)之间随机转发,最终发送给目的节点。这样,发送者就被隐藏在一系列转发节点之中。

Purdue大学提出的Hordes协议[7]对Crowds进行扩充和改进。Hordes在Crowds的回路阶段采用组播发送应答消息,一方面降低了延迟,但另一方面又降低了带宽利用率。与Crowds相比,Hordes通过组播提高了抵抗回溯攻击(traceback attack)的能力。不过组播在互联网上不是一种被广泛支持的技术,要在今天的互联网环境中实现Hordes将是一件非常困难的事情。中南大学的学者针对Crowds系统进行了研究,改进了路由方法[40-42]并进行了负载分析[43]。时金桥等人则对Crowds系统中存在的自私成员对系统的影响以及对抗策略进行了研究[44-45],提出了一种基于区分服务思想的自私行为惩罚机制。

3.1.5 广播或多播机制

互联网上的广播或多播可以实现一对多之间的通信,多播或广播地址代表一组主机,而不是某一个特定的主机。利用广播或多播技术发送消息时,可以使通信者隐藏在组播或广播成员中,由此实现匿名。典型的系统包括Maryland大学开发的P5系统[46]及前面提到的Purdue大学提出Hordes系统[7]等。

Maryland大学提出的P2P匿名通信协议P5采用分级广播的思想建立匿名通信网络,实现发送者匿名、接收者匿名与通信关系匿名,并且提供用户自己在匿名性与效率之间进行权衡的功能,这是它优于Xor-Tree[47]协议的地方。P5声称可以扩展到一个支持数千个活动用户同时通信的大规模匿名通信系统,然而,它的可扩展性并没有所声称的那样好,当用户数很大(大约达到一万)时,该协议效率很低,但它的攻击模型却是比较强的。

可以看出,基于广播/多播的匿名协议的匿名性较好,但通信开销很大,而且由于目前的互联网并不广泛支持广播和多播,因此这类协议并不实用。到目前为止,还没有一个实用的基于这类协议的匿名系统。Shields在文献[48]中进一步详细探讨了多播的匿

名性。

3.1.6 其他匿名机制

PipeNet 是 Dai 于 1998 提出的一种匿名机制[49],它由一系列的转发节点构成,消息在节点之间加密传输且所有链路中的消息流都需要保持恒定。当出现指定时间片内没有消息到达时,则认为可能发生攻击。这种匿名机制在理论上能够提供很好的匿名保护,但是在实际网络中并不适用。

Beimel 等人受日常公交系统的启发而设计了几个具有不同时间和通信复杂度的 Buses 协议[50]。它们都依赖于所有用户的协同工作,而且还假定存在一个全局的时钟,因而不太可能产生实际应用。其基本思想为:假定有一辆公共汽车,它会在每个用户前面停下来,用户在该公共汽车停下来时检查哪些消息是发给他的,并改变为这些消息所分配的位置。

Al-Muhtadi 等人[51]对位置隐私(location privacy)进行了讨论。其目的在于使攻击者不能确定出用户的位置,但他们的系统架构很苛刻,每个数据包都必须沿着树进行上传或下传,其攻击模型也比较弱,而且基本上没有分析系统的匿名性。Martin 在文献[52]中提出了位置匿名,主要讨论在一个域中如何通过否认(deniability)来获得匿名保护。文献[53]展示了如何发现 Tor[54]的隐匿服务器的位置,并提出了改进方法。

3.2 匿名系统

3.2.1 匿名邮件系统

电子邮件系统是匿名技术的主要应用之一。从 1993 年开始,历经十余年的发展,匿名邮件系统已经由最初的 0 型系统发展为如今的 III 型系统。

0 型匿名邮件系统 Anony.penet.fi 是最早广泛应用的匿名邮件系统。每天发送的邮件个数超过 7 000,其别名数据库最多保存超过 500 000 条记录。Anony.penet.fi 最终由于法律诉讼以及用户滥用而于 1996 年 8 月关闭。I 型匿名邮件系统 Cypherpunk[55]于 1994 年投入使用,主要解决了 0 型邮件系统的单点失效以及在匿名服务器存储大量用户信息的弱点。II 型匿名邮件系统 MixMaster 于 1995 年开始研究[56],主要目标是解决 I 型邮件系统在流量分析攻击下消息顺序和长度可能暴露邮件去向的弱点。截止到 2003 年 11 月,网络上大约运行着四十余台 MixMaster 邮件服务器,并且大多数同时支持 I 型与 II 型匿名邮件协议。MixMinion 匿名邮件系统[57]是目前最新的匿名邮件系统,它也称为 III 型匿名邮件系统,同前面的匿名系统相比,增加了匿名回复、前向匿名、抵御重放攻击、增加掩护流量等特性,安全性有所提高。除了上述 0 型到 III 型匿名邮件系统外,IBM 瑞士苏黎世研究实验室开发的匿名邮件系统 Babel 也是一个非常典型的系统[58]。Babel 基于 MIX 思想,采用洋葱消息结构与报文填充技术,并同时支持匿名发送与匿名回复。

3.2.2 匿名连接系统

WebMixes 系统[59]是由德国德累斯顿科技大学系统结构研究所主持开发的一个开放源码项目,目的是提供互联网上匿名的、不可监察的通讯服务,保护使用者的个人隐私。WebMixes 系统由 4 部分组成:本地客户端软件(JAP 软件)、InfoService、MIX 服务器链以及远端缓存代理。本地客户端软件作为浏览器的本地代理,将本地浏览器的请求多路复用并将数据请求报文重组加密发送给 MIX 服务器,MIX 服务器链通过加密传输将数据请求发送给缓存代理,并由缓存代理通过 MIX 服务器链重新将数据回应加密传输给本地 JAP 代理,并最终返回用户信息。InfoService 统计各个 MIX 服务器的流量,分析整个系统的匿名程度并通知用户。目前,WebMixes 原型系统已经吸引了大量的用户使用。

Onion-Routing 系统[60]是由美国海军研究实验室(Naval Research Library,NRL)主持开发的匿名网络。同基于消息的匿名通信系统不同,Onion-Routing 系统是采用通道方式构建匿名路径,即消息传输前需要先发送控制消息建立通道,此后的消息传输均按照同一路径传输,在消息传输结束后拆除通道。Onion-Routing 系统于 2000 年 1 月关闭。Tor[54]又称为新一代 Onion-Routing 系统,支持延迟敏感的 Web 浏览、即时通信、IRC、SSH 等应用。目前,Tor 网络的用户已增

长至数十万，成为目前应用最为广泛的匿名通信系统。国内的大学也对洋葱路由系统进行了研究，提出了可靠洋葱路由方案[61]、可追踪的洋葱路由方案[62]以及引入 MPLS 的洋葱路由隐蔽通信模型[63]等方案。

Freedom 系统是由零知识系统(Zero-Knowledge System)公司开发的用于匿名网络连接的商用系统[64-65]。Freedom 提供 IP 层的支持，利用报文封装支持HTTP、SMTP、POP3、SSL、IRC、NNTP 和 Telnet 等协议。Freedom 没有采用传统 MIX 消息混合机制，而是采用简单的 FIFO 机制以保证消息的传输效率。Freedom 系统于 2001 年 10 月由于经济原因而关闭。

MorphMix 系统[66]大致可以看作一个基于点对点思想的 Tor 系统，它同样是采用通道方式建立匿名网络，支持延迟敏感的网络应用。MorphMix 系统中采用共谋检测(conclusion detection)机制来防止攻击者控制的节点之间相互合作，破坏发送者匿名。Tarzan 系统[67]是由 MIT 开发的一个基于 IP 层的匿名协议，节点之间采用 UDP 进行通信，并采用掩护流量提高系统的安全性。

WonGoo 协议是中国科学院计算技术研究所开发的 P2P 匿名通信平台[68-74]，主要为信息安全、网格计算提供支撑技术和实验环境。WonGoo 主要包括两方面功能：具有强匿名性的 P2P 通讯(WonGoo-Link)以及基于内容查找的 P2P 资源共享(WonGoo-Search)，可以在这两个功能的基础上搭建各种特色化的 P2P 应用。WonGoo-Link 与 WonGoo-Search 可以分别独立构造并搭建各自的应用。同时，WonGoo-Search 底层通讯也可以采用 WonGoo-Link 协议来实现更安全地应用。WonGoo 的底层首先是一个在 Internet 开放环境中的可扩展的实用点对点匿名通信协议(WonGoo-Link)，主要是通过分层加密和随机转发实现强匿名性和高效率的通讯。WonGoo-Link 提供 3 种形式的匿名保护来实现强匿名机制，包括发送者匿名、接收者匿名和关系匿名。从匿名通讯层次来看，WonGoo 理论上可以支持上百万节点的通讯网络。在任意两点进行通讯时采用定向与随机选择两种方式选择中间节点，以此来保证通讯的强匿名和高效率。WonGoo-Link 匿名通讯的过程如图 4 所示。图中 A 与 B 通讯时，节点 C、D、E 表示确定的中间节点，节点 F、G、H 是根据实际通讯情况随机选择的中间节点。

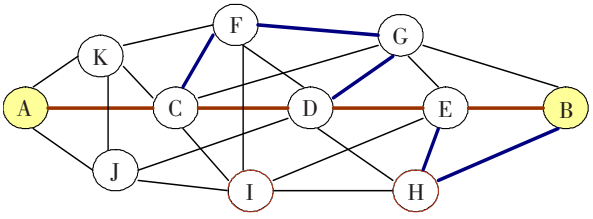

Fig.4 Communication representation of WonGoo-Link

图 4 WonGoo-Link 通讯示意图

3.2.3 匿名存储与发布

剑桥大学的 Anderson 于 1996 年提出 Eternity Service[75]系统，目标是抗审查的发布，即任何人想删除他所发布的信息都是很困难的。发布者把自己想发布的信息提交给 Eternity Service，Eternity Service 再把该信息拷贝到随机选定的 Eternity Service 服务器上。这样发布者就不知道自己的东西是在哪一个服务器上，因而也就无法删除。

由 Waldman、Rubin 和 Cranor 设计的匿名发布系统 Publius[76]采用了秘密共享的方法。发布者对要发布的东西进行加密，然后采用 Shamir 的秘密共享方案[77]把该加密密钥分割成 n 份。重建该密钥时只需要其中的任意 k 份秘密就可以。之后，发布者挑选 n 个 Publius 服务器并把加密的文档及一份秘密发给其中的每一个服务器。系统再把该文档的名字及相应的 n 个服务器的地址一起发布，形成一个 URL。用户根据该 URL 就可以取回加密的文档及每一份秘密，然后重建密钥并解密文档。对文档进行加密并分割加密密钥的目的是使得 Publius 服务器不能轻易地根据自己的喜好读出和删掉文档。Publius 的一个缺点是一个服务器可以通过搜索包含其地址的 URL 知道自己存储了哪些文档(但并不知道文档内容)。

Berkeley 大学的 Rewebber Network 发布系统[78]，MIT 的 Free Haven 项目[79]以及由 Purdue 大学设计开

发的匿名发布系统 GNUnet[80-81]都采用了 MIX 的思想。而 New York 大学设计开发的 Tangler 发布系统[82]则采用了文档混合(document entanglements)的思想。它把文档进行分块,一个块可以用来构建好几个不同的文档,新发布的文档的块必须与已有的块进行合并,这样就把新发布的文档与已经发布的文档关联起来了。

Freenet 是点对点思想与匿名应用的经典结合[83]。Freenet 的设计目标是建立一个保护用户隐私的分布式信息存储系统,能够确保信息的匿名发布与匿名使用,保证信息存储者的可否认性,防止第三者的 DoS 攻击,提供高效的信息动态存储及路由。Freenet 是一种自适应的对等网络应用,它允许匿名的作者和阅读者发表文章,复制数据和读取数据。Freenet 中的节点是自适应的对等节点,通过向邻节点查询和请求来检索和获取数据文件,文件以与位置无关的密钥命名,查找和请求文件是用密钥标识和定位的。Freenet 系统是相互协作的分布式文件系统,文件定位与位置无关并且被透明地复制。Freenet 在文件存储以及文件传输方面都采用了缜密的加密手段,是文件共享型匿名对等应用的代表。

4 匿名的分析与攻击

4.1 威胁模型

在现实生活中,网络匿名通信面临着包括技术、法律、政策、道德等多方面的攻击,本文主要讨论匿名通信所面临的技术性攻击。为了更好地分析匿名通信所面临的攻击,首先要确定对攻击者能力的假设。在匿名通信的研究领域中,通常假定攻击者的属性如下:

(1)内部-外部攻击者:内部攻击者控制匿名通信系统的部分组成部件,如发送者、接收者或者中间路由节点等。外部攻击者则控制匿名通信系统底层的通信介质,例如可以对通信链路进行报文监听等。

(2)被动-主动攻击者:被动攻击者只能监听网络流量,而主动攻击者除此之外还具有插入、更改、删除消息的能力。

(3)静态-自适应攻击者:静态攻击者在攻击过程中占有的通信系统资源是不变的,而自适应攻击者在攻击时可能不断改变占有的资源,例如他们可以"跟踪"消息的传送。

(4)局部-全局攻击者:局部攻击者控制着通信系统的一部分资源而全局攻击者控制着整个通信系统。

对于匿名通信系统的攻击者来说,可能同时拥有其中的几种属性,例如既是主动攻击者又是内部攻击者。

4.2 攻击方法

时间攻击(timing attack)的基本思想是攻击者利用消息进入离开服务器的时间信息来关联消息。文献[84]针对 Web 浏览器访问 Cache 所引发的时间攻击进行讨论。文献[85]对低延迟 MIX 系统中的时间攻击进行探讨,并提出了一种称为"防御性丢失"(defensive dropping)的掩护消息来抵御时间攻击。解决时间攻击问题的一个可能的方法是每个中间路由节点采用随机长度的延迟时间。此外,在文献[59]中提出使用掩护消息来防止时间攻击。

编码攻击(coding attack)是指如果消息在传输过程中存在没有改变的编码,则攻击者可以将系统输入输出消息联系起来。编码攻击又称为标记攻击(tagging attack)。文献[86-87]探讨了如何利用标记攻击破坏 MIX 系统,文献[21]探讨了如何利用标记攻击破坏 URE-Onion 机制[19-20]。标记攻击的一种抵御方法是对消息进行完整性校验,MixMaster 系统[56]和 MixMinion 系统[57]中都提出了相应的解决方案。此外,Danezis 还提出了一种称为 Minx[88]的报文格式。Minx 采用 AES 加密算法的 IGE 模式,攻击者改变消息中的某几位会导致整个消息不可读,由此可以防止攻击者在消息中添加标记。

流量形状攻击(traffic shape attack)[89]主要包括通信模式攻击(communication pattern attack)、消息频度攻击(message frequency attack)及报文计数攻击(packet counting attack)。通信模式攻击主要是针

对实时交互式的应用。在这种应用中,通常只有一个用户发送消息而另外一个用户沉默接收消息。长时间对报文发送与接收的时间进行分析,有可能发现通信双方的对应关系。消息频度与计数的攻击则是建立在对发送接收数据报文的比较上,如果二者频度或数量相同,则有可能将其对应起来。解决流量形状攻击的方法主要有报文填充、掩护消息流量以及报文分片等等。文献[90]提出利用消息分片的方法抵御局部攻击者的计数攻击。

交集攻击(intersection attack)[6]基于长时间对用户网络行为的观察。对于一个特定的网络用户来说,通常登陆时间、交互对象等具有一定的规律,因此,通过对不同时间、不同活动的网络用户进行交集分析,有可能确定对应关系。文献[91]指出 Tarzan 和 Crowds 系统对于这种攻击都是脆弱的,但其攻击代价会随着网络规模的增大而增大。文献[92-93]对交集攻击作了进一步地讨论,称之为暴露攻击(disclosure attack),并指出实施这样的攻击等价于求解 CSP 问题(constrain satisfaction problem),这是一个 NP 难问题。文献[94]则给出了一个更有效的 HS 攻击(hitting set attack),并对攻击方法进行了优化。文献[95]提出了一种称为概率暴露攻击(statistical disclosure attack)的攻击方法。目前,如何抵御交集攻击及其衍生出的攻击仍是匿名通信领域的开放型问题。

Chuam 在其经典 MIX 论文中提到了重放攻击(repetitive attack)。所谓重放攻击,指的是攻击者首先记录下待追踪的消息,然后再重新将此消息发送进入 MIX 网络以追踪特定消息传输路径的一种攻击。由于 MIX 节点会对同样的消息进行相同的操作,因此两条相同的输入消息必然会引起在 MIX 的输出端出现两条相同的消息,攻击者可以确定待追踪的消息并由此确定消息传输路径,最终发现消息接收者,破坏 MIX 系统的匿名保护。重放攻击是一种针对 MIX 的十分有效的主动攻击[1,19,57,96]。时金桥等人在文献[16]中提出了一种改进的通用重加密洋葱路由机制以抵御重放攻击。

(n-1)攻击是针对 MIX 的主动攻击中最为有效的一种攻击。攻击者通过消息延迟或发送虚假消息等方法将待攻击 MIX 的内部缓冲区清空,然后将待追踪消息与其他攻击者的虚假消息一起发送给 MIX 服务器。当 MIX 服务器输出消息时,只有一条消息对于攻击者是未知的,则攻击者可以确认这条消息就是待追踪消息。(n-1)攻击在不同环境下有时也称为涓流攻击(trickle attack)、洪泛攻击(flooding attack)、混合攻击(blending attack)、隔离攻击(isolating attack)、刷新攻击(flushing attack)及 Spam 攻击等。在此前的研究中,研究者提出链路加密[57]、消息时间戳[96]、掩饰消息[97]以及绕路传输[58]等方法抵御重放攻击,然而这些方法却由于实际应用的限制等原因无法完全防止重放攻击。文献[98]中总结了(n-1)成功攻击的前提,并提出了一种称为 Regroup-And-Go MIX(RG MIX)的抵御攻击方法。这种攻击方法可以使攻击者成功进行(n-1)攻击的概率降到很低。

前驱攻击(predecessor attack)是 Reiter 和 Rubin 在分析 Crowds 系统[5]的安全性时首先提出的,他们称之为共谋攻击(collusion attack)。多个节点共享其得

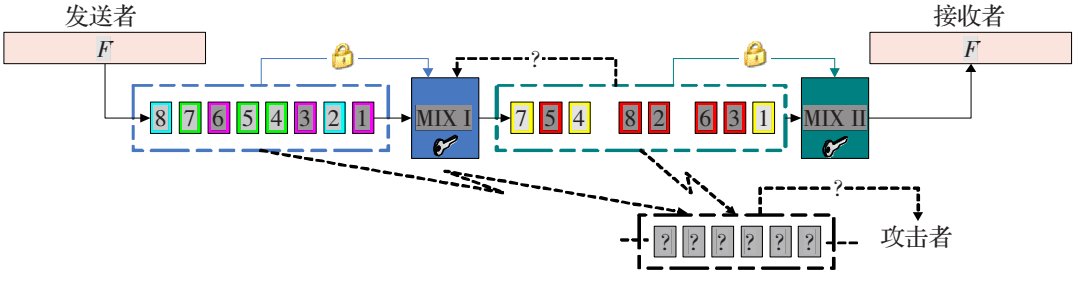

Fig.5 Illustration of Regroup-And-Go MIX

图 5 Regroup-And-Go MIX 示意图

到的路径信息,从而共同推断消息发送者的身份。Wright 等人[91,99-100]对包括 Crowd、Onion-Routing 和 DC-Net 协议在内的前驱攻击进行了分析。

拒绝服务攻击(denial-of-service attack)是指攻击者通过种种手段使匿名通信系统的服务能力降低。文献[101]针对攻击者阻断访问匿名通信系统进行分析,并提出了对抗手段。

女巫攻击(sybil attack)[102]是指攻击者首先向网络中植入恶意节点(自己的节点或者控制部分网络节点),然后恶意节点把知道的系统信息泄漏给攻击者,攻击者再从这些信息推断出通信关系或者发动其他的攻击(如前驱攻击等)。在参与者充当转发代理的系统中尤其要防范女巫攻击,防止攻击者控制多个主机作为参与者加入系统,从而使得系统中相当比例成员成为恶意节点,破坏系统匿名性能。在 Crowds 系统中证明了恶意节点比例必须控制在一定的范围内才能达到它所声称的匿名性。当系统对用户加入没有身份限制时,实力强大的攻击者是很容易发动女巫攻击的。抵抗的办法是采取适当的加入控制策略,MorphMix 系统[66]中就提到一种共谋检测机制,防止受控节点选择其他共谋节点组成匿名路径,进行女巫攻击。

5 结束语

匿名技术除了用于保护互联网上用户的隐私之外,还在军事机构、执法机关、情报机构等安全性要求很高的环境中有着很重要的用途。在军事上,军事指挥中心和各个部门之间的通信,甚至其通信模式的变化本身已经暗含了很多有用的信息。而一封加密之后的电子邮件,如果它在毒贩和其他尚未被怀疑的人之间,或者国防建设的雇员与敌方大使馆官员之间传递,显然,它包含某种深意。

匿名技术发展到今天,虽然取得了一定的成就,但还有很多问题有待解决。虽然基于消息的延迟不敏感系统在理论上已逐渐趋于完善,但在实践中还存在一些问题,而基于通道的延迟敏感系统无论在理论上还是实践上都还存在很多问题,需要进一步研究。首先,对于延迟敏感系统来说,需要研究如何抵抗一些常见的攻击,如重放攻击和泄漏攻击等;第二是如何发现一些新的攻击手段,以进一步验证现有的匿名协议的安全性;第三是如何形式化地描述攻击者。对攻击者能力的描述将直接影响到协议的安全性。现有的形式化方法并不能很好地描述针对匿名协议的攻击者;第四是如何评估匿名系统的匿名性。至今为止,还没有一种合适、统一地评估匿名系统的方法,因此,现有的对匿名系统的比较都有很大的局限性;第五是如何对掩饰流的作用进行评价。目前最关键的问题就是不能从理论上说明掩饰流到底能不能提高系统的安全性;第六是匿名系统的可控性问题。匿名技术的出现带来了滥用问题,如利用匿名系统进行攻击,事后无法进行追查;利用匿名系统登陆网上银行,让电子货币不可追踪,给不法分子提供了洗钱的机会等。为了避免匿名的滥用,有必要研究可控匿名技术。但是匿名系统的可控性实际上是与匿名性相冲突的一种概念,因此要在保证匿名性的情况下提供可控的能力是一个难题。最后是研究匿名的经济学问题,即如何激励用户自愿地为别人提供匿名保护。匿名技术需要依赖通信过程中所有参与人员的共同努力,匿名系统的参与人数越多,发送消息越积极,则系统提供的匿名保护水平就越高。匿名技术中的经济学问题也已经成为匿名技术未来发展过程中所必须解决的问题。

Refereence:

[1] Chaum D. Untraceable electronic mail, return addresses, and digital pseudonyms[J]. Communications of the ACM, 1981,4(2):84-88.

[2] Chaum D. The dining cryptographers problem: Unconditional sender and recipient untraceability[J]. Journal of Cryptology, 1988,1(1):65-75.

[3] Pfitzmann A, Khntopp M. Anonymity, unobservability, and pseudonymity: A proposal for terminology[C]//LNCS 2009: Proceedings of Workshop on Design Issues in Anonymity and Unobservability, Berkeley, California, USA, 2000:10-29.

[4] Flinn B, Maurer H. Levels of anonymity[J]. Journal of Universal

Computer Science, 1995,1(1):35-47.

[5] Reiter M, Rubin A. Crowds: Anonymity for Web transactions[J]. ACM Transactions on Information and System Security, 1998,1(1):66-92.

[6] Berthold O, Pfitzmann A, Standtke R. The disadvantages of free MIX routes and how to overcome them[C]//LNCS 2009: Proceedings of Workshop on Design Issues in Anonymity and Unobservability, Berkeley, California, USA, 2000:30-45.

[7] Shields C, Levine B N. A protocol for anonymous communication over the Internet[C]//Proceedings of the 7th ACM Conference on Computer and Communications Security (CCS'00). Athens, Greece: ACM Press, 2000:33-42.

[8] Díaz C, Seys S, Claessens J, et al. Towards measuring anonymity[C]//LNCS 2482: Proceedings of Privacy Enhancing Technologies Workshop(PET'02), San Francisco, CA, USA, 2002:54-68.

[9] Serjantov A, Danezis G. Towards an information theoretic metric for anonymity[C]//LNCS 2482: Proceedings of Privacy Enhancing Technologies Workshop (PET'02), San Francisco, CA, USA, 2002:41-53.

[10] Guan Y, Fu X, Bettati R, et al. An optimal strategy for anonymous communication protocols[C]//IEEE Computer Society: Proceedings of the 22nd International Conference on Distributed Computing Systems (ICDCS'02), Vienna, Austria, 2002:257-266.

[11] Zhu Y, Bettati R. Anonymity vs. information leakage in anonymity systems[C]//Proceedings of the 25th IEEE International Conference on Distributed Computing Systems (ICDCS'05), Washington DC, USA, 2005:514-524.

[12] Clauβ S, Schiffner S. Structuring anonymity metrics[C]//Proceedings of the Second ACM Workshop on Digital Identity Management (DIM'06). Alexandria, Virginia, USA: ACM Press, 2006:55-62.

[13] Deng Y, Pang J, Wu P. Measuring anonymity with relative entropy[C]//LNCS 4691: Proceedings of the 4th International Workshop on Formal Aspects in Security and Trust (FAST'06), Hamilton, Ontario, Canada, 2006:59-77.

[14] Gabber E, Gibbons P B, Matias Y, et al. How to make personalized Web browsing simple, secure, and anonymous[C]//LNCS 1318: Proceedings of Financial Cryptography (FC'97), Anguilla, British West Indies, 1997:17-31.

[15] Díaz C, Serjantov A. Generalising mixes[C]//LNCS 2760: Proceedings of Privacy Enhancing Technologies Workshop (PET'03), Germany, 2003:18-31.

[16] Shi Jinqiao. Anonymous communication technologies on the Internet[D]. Harbin: Harbin Institute of Technology, 2007.

[17] Park C, Itoh K, Kurosawa K. Efficient anonymous channel and all/nothing election scheme[C]//LNCS 765: Proceedings of Eurocrypt'93, Lofthus, Norway, 1994:248-259.

[18] Golle P, Jakobsson M, Juels A, et al. Universal re-encryption for mixnets[C]//LNCS 2964: Proceedings of RSA-Conference, Cryptographers' Track, San Francisco, CA, USA, 2004:163-178.

[19] Gomulkiewicz M, Klonowski M, Kutylowski M. Onions based on universal re-encryption-anonymous communication immune against repetitive attack[C]//LNCS 3325: Proceedings of the International Workshop on Information Security Applications (WISA'04), Jeju Island, Korea, 2004:400-410.

[20] Klonowski M, Kutylowski M, Zagrski F. Anonymous communication with on-line and off-line onion encoding[C]//LNCS 3381: Proceedings of SOFSEM 2005: Theory and Practice of Computer Science, 31st Conference on Current Trends in Theory and Practice of Computer Science, Slovakia, 2005:229-238.

[21] Danezis G. Breaking four mix-related schemes based on universal re-encryption[C]//LNCS 4176: Proceedings of 9th Information Security Conference(ISC'06), Samos Island, Greece, 2006:46-59.

[22] Sako K, Kilian J. Receipt-free mix-type voting scheme a practical solution to the implementation of a voting booth[C]//LNCS 921: Proceedings of Advances in Cryptology-Eurocrypt'95, France, 1995:393-403.

[23] Michels M, Horster P. Some remarks on a receipt-free and universally verifiable mix-type voting scheme[C]//LNCS 1163: Proceedings of Advances in Cryptology(Asiacrypt'96), Kyongju, Korea, 1996:125-132.

[24] Ogata W, Kurosawa K, Sako K, et al. Fault tolerant anonymous channel[C]//LNCS 1334: Proceedings of Inter-

national Conference on Information and Communication Security (ICICS'97), Beijing, China, 1997:440-444.

[25] Abe M.Universally verifiable MIX with verification work independent of the number of MIX servers[C]//LNCS 1403: Proceedings Advances in Cryptology (Eurocrypt'98), Helsinki, Finland, 1998:437-447.

[26] Jakobsson M. A practical mix[C]//LNCS 1403: Proceedings of Advances in Cryptology (Eurocrypt'98), Helsinki, Finland, 1998:448-461.

[27] Desmedt Y, Kurosawa K. How to break a practical mix and design a new one[C]//LNCS 1807: Proceedings of Advances in Cryptology (Eurocrypt'00), Bruges, Belgium, 2000:557-572.

[28] Jakobsson M. Flash mixing[C]//Proceedings of 8th ACM Symposium on Principles of Distributed Computing (PODC'99), Atlanta, GA, USA, 1999:83-89.

[29] Mitomo M, Kurosawa K. Attack for flash MIX[C]//LNCS 1976: Proceedings of Advances in Cryptology(Asiacrypt'00), Kyoto, Japan, 2000:192-204.

[30] Furukawa J, Sako K. An efficient scheme for proving a shuffle[C]//LNCS 2139: Proceedings of Crypto'01, Santa Barbara, California, USA, 2001:368-387.

[31] Neff A. A verifiable secret shuffle and its application to e-voting[C]//Proceedings of 8th ACM Conference on Computer and Communications Security(CCS'01), Philadelphia, USA, 2001:116-125.

[32] Golle P,Zhong S,Boneh D,et al.Optimistic mixing for exit-polls[C]//LNCS 2501: Proceedings of Advances in Cryptology (Asiacrypt'02), Queenstown, New Zealand, 2002:451-465.

[33] Chen Xiaofeng, Wang Yuming. A secure electronic voting scheme based on anonymous communication channel[J]. Acta Electronica Sinica, 2003,31(3):390-393.

[34] Gao Huming, Wang Jilin, Wang Yuming. An electronic voting scheme based on a new MIX net[J]. Acta Electronica Sinica, 2004,32(6):1047-1049.

[35] Li Yanjiang, Ma Chungui, Huang Liusheng. An electronic voting scheme[J]. Journal of Software, 2005,16(10):1805-1810.

[36] Waidner M. Unconditional sender and recipient untraceability in spite of active attacks[C]//LNCS 434: Proceedings of Eurocrypt'89, Houthalen, Belgium, 1990:302-319.

[37] Sirer E G, Polte M, Robson M. CliqueNet: A self-organizing, scalable, Peer-to-Peer anonymous communication substrate[EB/OL]. [2002]. http://www.cs.cornell.edu/People/egs/cliquenet/papers.html.

[38] Goel S, Robson M, Polte M, et al. Herbivore: A scalable and efficient protocol for anonymous communication, Tech Rep 2003-1890[R]. Cornell University, 2003.

[39] Ahn L, Bortz A, Hopper N J. K-anonymous message transmission[C]//Proceedings of the 10th ACM Conference on Computer and Communication Security (CCS'03), Washington, DC, USA, 2003:122-130.

[40] Wang Weiping, Chen Jianer, Wang Jianxin, et al. An anonymous communication protocol based on groups with definite route length[J]. Journal of Computer Research and Development, 2004,41(4):609-614.

[41] Wang Weiping, Chen Jianer, Chen Songqiao, et al. Research on a short distance-prior rerouting scheme in anonymous communication[J]. Journal of Software, 2004,15(4):561-570.

[42] Sui Hongfei, Chen Jianer, Chen Songqiao, et al. Secret sharing-based rerouting in rerouting-based anonymous communication systems[J]. Journal of Computer Research and Development, 2005,42(10):1660-1666.

[43] Sui Hongfei, Chen Songqiao, Chen Jianer, et al. Payload analysis of rerouting-based anonymous communication systems[J]. Journal of Software, 2004,15(2):278-285.

[44] Shi Jinqiao, Fang Binxing, Li Bin. Towards an analysis of source-rewriting anonymous systems in a lossy environment[C]//LNCS 3320: Proceedings of the 5th International Conference on Parallel and Distribution Computing, Applications and Technologies (PDCAT'04), Singapore, 2004:613-618.

[45] Shi Jinqiao, Cheng Xiaoming. Research on penalty mechanism against selfish behaviors in anonymous communication system[J]. Journal on Communications, 2006,27(2):80-86.

[46] Sherwood R, Bhattacharjee B, Srinivasan A. P5: A protocol for scalable anonymous communication[C]//Proceedings of the 2002 IEEE Symposium on Security and Privacy, Berkeley, California, USA, 2002:58-72.

[47] Dolev S, Ostrovsky R. Xor-trees for efficient anonymous multicast and reception[J]. ACM Transactions on Information and

System Security, 2000,3(2):63-84.

[48] Shields C. Secure hierarchical multicast routing and multicast Internet anonymity[D]. University of California Santa Cruz, 1998.

[49] Dai W. PipeNet 1.1[EB/OL]. [1996-08]. http://www.eskimo.com/~weidai/pipenet.txt.

[50] Beimel A, Dolev S. Buses for anonymous message delivery[J]. Journal of Cryptology, 2003,16(1):25-39.

[51] Al-Muhtadi J, Campbell R, Kapadia A, et al. Routing through the mist: Privacy preserving communications in ubiquitous computing environments[C]//Proceedings of International Conference of Distributed Computing Systems(ICDCS'02), Vienna, Austria, 2002:74-83.

[52] Martin D. Local anonymity in the Internet[D]. Boston University, 1999.

[53] Overlier L, Syverson P. Locating hidden servers[C]//Proceedings of the 2006 IEEE Symposium on Security and Privacy, Berkeley, California, USA, 2006:100-114.

[54] Dingledine R, Mathewson N, Syverson P. Tor: The second-generation onion router[C]//Proceedings of the 13th USENIX Security Symposium, San Diego, CA, USA, 2004:303-320.

[55] Parekh S. Prospects for remailers: Where is anonymity heading on the Internet?[N/OL]. [1996-08-05]. http://www.firstmonday.dk/issues/issue2/remailers/index.html.

[56] Moeller U, Cottrell L, Palfrader P, et al. Mixmaster protocol version 2[EB/OL]. [2005-06]. http://www.ietf.org/internet-drafts/draft-sassaman-mixmaster-03.txt.

[57] Danezis G, Dingledine R, Mathewson N. Mixminion: Design of a type III anonymous remailer protocol[C]//Proceedings of the 2003 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 2003:2-15.

[58] Gülcü C, Tsudik G. Mixing E-mail with BABEL[C]//Proceedings of the Symposium on Network and Distributed System Security (NDSS'96), San Diego, California, USA, 1996:2-16.

[59] Berthold O, Federrath H, Köpsell S. Web MIXes: A system for anonymous and unobservable internet access[C]//LNCS 2009: Proceedings of International Workshop on Design Issues in Anonymity and Unobservability, Berkeley, California, USA, 2000:115-129.

[60] Goldschlag D, Reed M, Syverson P. Hiding routing information[C]//LNCS 1174: Proceedings of the First International Workshop on Information Hiding, Cambridge, UK, 1996:137-150.

[61] Zhao Fuxiang, Wang Yuming, Wang Changjie. An authenticated scheme of onion routing[J]. Chinese Journal of Computers, 2001,24(5):463-467.

[62] Wu Zhenqiang, Yang Bo. An advanced marking scheme and realization for onion routing trace back[J]. Journal on Communications, 2002,23(5):96-102.

[63] Wu Zhenqiang, Yang Bo. A model for anonymous communication based on onion routing and MPLS[J].Journal of Xidian University:Natural Science, 2002,29(4):513-517.

[64] Boucher P, Shostack A, Goldberg I. Freedom systems 2.0 architecture[N/OL]. White Paper, [2000]. http://www.freedom.net/info/whitepapers/.

[65] Shostack A, Back A, Goldberg I. Freedom 2.1 security issues and analysis[N/OL]. White Paper, [2001]. http://www.freedom.net/info/whitepapers/Freedom_Security2-1.pdf.

[66] Rennhard M, Plattner B. Introducing MorphMix: Peer-to-Peer based anonymous Internet usage with collusion detection[C]//Proceedings of the 2002 ACM Workshop on Privacy in the Electronic Society (WPES'02), Washington, DC, USA, 2002:91-102.

[67] Freedman M J, Morris R. Tarzan: A Peer-to-Peer anonymizing network layer[C]//Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS'02), Washington, DC, USA, 2002:193-206.

[68] Lu Tuanbo, Fang Binxing, Sun Yuzhong, et al. WonGoo: A Peer-to-Peer protocol for anonymous communication[C]//Proceedings of the 2004 International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA'04), Las Vegas, Nevada, USA, 2004:1102-1106.

[69] Lu Tianbo, Fang Binxing, Sun Yuzhong, et al. Building scale-free overlay MIX networks with small-world properties[C]//Proceedings of the Third International Conference on Information Technology and Applications(ICITA'05), Sydney, Australia, 2005,2:529-534.

[70] Lu Tianbo, Fang Binxing, Sun Yuzhong, et al. Performance analysis of WonGoo system[C]//Proceedings of the Fifth International Conference on Computer and Information Technology (CIT'05), Shanghai, China, 2005:716-722.

[71] Lu Tianbo, Fang Binxing, Sun Yuzhong, et al. Some remarks on universal re-encryption and a novel practical anonymous tunnel[C]//LNCS 3619: Proceedings of the Third International Conference on Computer Networks and Mobile Computing (ICCNMC'05), Zhangjiajie, China, 2005:853-862.

[72] Lu Tianbo, Fang Binxing, Cheng Xueqi, et al. Peer discovery in Peer-to-Peer anonymity networks[C]//Proceedings of 2006 IEEE International Conference on Networking, Sensing and Control (ICNSC'06), Ft Lauderdale, USA, 2006:131-136.

[73] Lu Tianbo, Fang Binxing, Sun Yuzhong, et al. Analysis of anonymity protocol WonGoo with probabilistic model checking[J]. Journal of Chinese Computer Systems, 2006,27(4): 646-650.

[74] Lu Tianbo. Research on WonGoo—A Peer-to-Peer anonymous communication protocol[D]. Institute of Computing Technology, Chinese Academy of Sciences, 2006-06.

[75] Anderson R. The eternity dervice[C/OL]//Proceedings of Pragocrypt'96. [1996]. http://www.cl.cam.ac.uk/~rja14/Papers/eternity.pdf.

[76] Waldman M, Rubin A, Cranor L. Publius: A robust, tamperevident, censorship-resistant and source-anonymous Web publishing system[C]//Proceedings of the 9th USENIX Security Symposium, Denver, Colorado, USA, 2000:59-72.

[77] Shamir A. How to share a secret[J]. Communications of the ACM, 1979,22(11):612-613.

[78] Goldberg I, Wagner D. TAZ servers and the rewebber network: Enabling anonymous publishing on the world wide web[N]. In First Monday 3(4), August 1998.

[79] Dingledine R, Freedman M J, Molnar D. The free haven project: Distributed anonymous storage service[C]//LNCS 2009: Proceedings of International Workshop on Design Issues in Anonymity and Unobservability, Berkeley, California, USA, 2000:67-95.

[80] Bennett K, Grothoff C. GAP Practical anonymous networking[C]//Proceedings of Privacy Enhancing Technologies workshop (PET'03), Dresden,Germany,2003:141-160.

[81] Kügler D. An analysis of GNUnet and the implications for anonymous, censorship-resistant networks[C]//Proceedings of Privacy Enhancing Technologies Workshop (PET'03), 2003: 161-176.

[82] Waldman M, Mazières D. Tangler: A censorship-resistant publishing system based on document entanglements[C]//Proceedings of the 8th ACM Conference on Computer and Communications Security(CCS'01), Philadelphia, Pennsylvania, USA, 2001:126-135.

[83] Clarke I, Sandberg O, Wiley B, et al. Freenet: A distributed anonymous information storage and retrieval system [C]//LNCS 2009: Proceedings of International Workshop Design Issues in Anonymity and Unobservability, Berkeley, California, USA, 2000:46-66.

[84] Felten E W, Schneider M A. Timing attacks on Web privacy[C]//Proceedings of the 7th ACM Conference on Computer and Communications Security, Athens, Greece, 2000:25-32.

[85] Levine B N, Reiter M K, Wang C, et al. Timing attacks in low-latency MIX-based systems[C]//Proceedings of Financial Cryptography (FC'04), Key West, FL, USA, 2004:251-265.

[86] Pfitzmann A, Pfitzmann B. How to break the direct RSA-implementation of MIXes[C]//LNCS 434: Proceedings of Eurocrypt'89, Houthalen, Belgium, 1990:373-381.

[87] Pfitzmann B. Breaking efficient anonymous channel [C]//LNCS 950: Proceedings of Advances in Cryptology (Eurocrypt'94), Perugia, Italy, 1994:332-340.

[88] Danezis G, Laurie B. Minx: A simple and efficient anonymous packet format[C]//Proceedings of the 2004 ACM workshop on Privacy in the electronic society (WPES'04), Washington, DC, USA, 2004:59-65.

[89] Raymond J F. Traffic analysis: Protocols, attacks, design issues, and open problems[C]//LNCS 2009: Proceedings of International Workshop on Design Issues in Anonymity and Unobservability, Berkeley, California, USA, 2000:10-29.

[90] Serjantov A, Murdoch S J. Message splitting against the partial adversary[C]//Proceedings of Privacy Enhancing Technologies Workshop (PET'05), Cavtat, Croatia, 2005:26-39.

[91] Wright M, Adler M, Levine B N, et al. Defending anonymous

communications against passive logging attacks[C]//Proceedings of the 2003 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 2003:28-42.

[92] Kesdogan D, Agrawal D, Penz S. Limits of anonymity in open environments[C]//LNCS 2578: Proceedings of Information Hiding Workshop (IH'02), Noordwijkerhout, The Netherlands, 2002:53-69.

[93] Agrawal D, Kesdogan D, Penz S. Probabilistic treatment of MIXes to hamper traffic analysis[C]//Proceedings of the 2003 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 2003:16-27.

[94] Kesdogan D, Pimenidis L. The hitting set attack on anonymity protocols[C]//LNCS 3200: Proceedings of the 6th Information Hiding Workshop, Toronto, 2004:326-339.

[95] Mathewson N, Dingledine R. Practical traffic analysis: Extending and resisting statistical disclosure[C]//LNCS 3424: Proceedings of Privacy Enhancing Technologies Workshop (PET'04), Toronto, Canada, 2004:17-34.

[96] Kesdogan D, Egner J, Büschkes R. Stop-and-Go MIXes: Providing probabilistic anonymity in an open system[C]//LNCS 1525: Proceedings of Information Hiding Workshop, Portland, Oregon, USA, 1998:83-98.

[97] Danezis G, Sassaman L. Heartbeat traffic to counter (n-1) attacks: red-green-black mixes[C]//Proceedings of the Workshop on Privacy in the Electronic Society (WPES'03), Washington,DC, USA, 2003:89-93.

[98] Shi Jinqiao, Fang Binxing, Shao L. Regroup-And-Go MIXes to counter the (n-1) attack[J].Internet Research, Special Issue on Privacy and Anonymity in the Digital Era: Theory, Technologies and Practice, 2006,16(2):213-223.

[99] Wright M K. Passive logging attacks against anonymous communications systems[D]. University of Massachusetts Amherst, 2005-05.

[100] Wright M, Adler M, Levine B N, et al. An analysis of the degradation of anonymous protocols[C]//Proceedings of Network and Distributed Security Symposium (NDSS'02), San Diego, California, USA, 2002.

[101] Kopsell S, Hillig U. How to achieve blocking resistance for existing systems enabling anonymous Web surfing[C]//Proceedings of the 2004 ACM Workshop on Privacy in the Electronic Society(WPES'04), Washington, DC, USA, 2004:47-58.

[102] Douceur J. The sybil attack[C]//LNCS 2429: Proceedings of the First International Peer-To-Peer Systems Workshop (IPTPS'02), Cambridge, MA, USA, 2002:251-260.

附中文参考文献:

[16] 时金桥.Internet 上匿名通信技术的研究[D].哈尔滨:哈尔滨工业大学,2007.

[33] 陈晓峰,王育民.基于匿名通讯信道的安全电子投票方案[J].电子学报,2003,31(3):390-393.

[34] 高虎明,王继林,王育民.一个基于 MIX net 的电子投票方案[J].电子学报,2004,32(6):1047-1049.

[35] 李彦江,马传贵,黄刘生.一种电子投票方案[J].软件学报,2005,16(10):1805-1810.

[40] 王伟平,陈建二,王建新,等.基于群组的有限路长匿名通信协议[J].计算机研究与发展,2004,41(4):609-614.

[41] 王伟平,陈建二,陈松乔,等.匿名通信中短距离优先分组重路由方法的研究[J].软件学报,2004,15(4):561-570.

[42] 睢鸿飞,陈建二,陈松乔,等.重路由匿名通信系统中基于秘密共享的重路由算法[J].计算机研究与发展,2005,42(10):1660-1666.

[43] 睢鸿飞,陈松乔,陈建二,等.基于重路由匿名通信系统的负载分析[J].软件学报,2004,15(2):278-285.

[45] 时金桥,程晓明.匿名通信系统中自私行为的惩罚机制研究[J].通信学报,2006,27(2):80-86.

[61] 赵福祥,王育民,王常杰.可靠洋葱路由方案的设计与实现[J].计算机学报,2001,24(5):463-467.

[62] 吴振强,杨波.追踪洋葱包的高级标记方案与实现[J].通信学报,2002,23(5):96-102.

[63] 吴振强,杨波.基于葱头路由技术和 MPLS 的隐匿通信模型[J].西安电子科技大学学报:自然科学版,2002,29(4):513-517.

[73] 陆天波,方滨兴,孙毓忠,等.匿名协议 WonGoo 的概率模型验证分析[J].小型微型计算机系统,2006,27(4):646-650.

[74] 陆天波.P2P 匿名通信协议 WonGoo 研究[D].北京:中国科学院计算技术研究所,2006.

LU Tianbo was born in 1977. He received the Ph.D. degree in Computer Science from Institute of Computing Technology, Chinese Academy of Sciences in 2006. He is a lecturer at National Computer Network Emergency Response Technical Team/Coordination Center of China(CNCERT/CC). His research interests include software assurance (SwA), information security, P2P computing, etc.

陆天波(1977–),男,贵州毕节人,2006 年于中国科学院计算技术研究所获计算机软件与理论专业工学博士学位,目前是国家计算机网络应急技术处理协调中心高级工程师,主要研究领域为软件确保,信息安全,对等网络等。

SHI Jinqiao was born in 1978. He received the Ph.D. degree in Computer Architecture from Harbin Institute of Technology in 2007. He is an assistant professor at Institute of Computing Technology, Chinese Academy of Sciences. His research interests include network and information security, privacy enhancing technologies, etc.

时金桥(1978–),男,黑龙江哈尔滨人,2007 年于哈尔滨工业大学获计算机系统结构专业工学博士学位,目前在中国科学院计算技术研究所任助理研究员,主要研究领域为网络与信息安全,隐私保护技术等。

CHENG Xueqi was born in 1971. He received the Ph.D. degree in Computer Architecture from Institute of Computing Technology, Chinese Academy of Sciences. He is a professor and doctoral supervisor at Institute of Computing Technology, Chinese Academy of Sciences. His research interests include network and information security, P2P computing, etc.

程学旗(1971–),男,安徽安庆人,于中国科学院计算技术研究所获计算机系统结构专业博士学位,目前任中国科学院计算技术研究所网络科学与技术部主任,研究员,博士生导师,主要研究领域为网络与信息安全,P2P 计算等。在 SIGIR,CIKM,PKDD 等国际学术会议和国内外重要学术刊物发表学术论文 50 余篇,申请或拥有十多项发明专利和软件著作权,先后主持了多项国家重点 863、973、科技攻关、中国科学院知识创新工程、自然科学基金等重大课题项目。