软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2011,22(10):2358−2371 [doi: 10.3724/SP.J.1001.2011.03929]

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

基于时隙质心流水印的匿名通信追踪技术*

张 璐[1,2+], 罗军舟[1], 杨 明[1], 何高峰[1]

[1](东南大学 计算机科学与工程学院,江苏 南京 210096)

[2](上海市信息安全综合管理技术研究重点实验室,上海 200240)

Interval Centroid Based Flow Watermarking Technique for Anonymous Communication Traceback

ZHANG Lu[1,2+], LUO Jun-Zhou[1], YANG Ming[1], HE Gao-Feng[1]

[1](School of Computer Science and Engineering, Southeast University, Nanjing 210096, China)

[2](Shanghai Key Laboratory of Integrate Administration Technologies for Information Security, Shanghai 200240, China)

+ Corresponding author: E-mail: luzhang@seu.edu.cn, http://www.seu.edu.cn

Zhang L, Luo JZ, Yang M, He GF. Interval centroid based flow watermarking technique for anonymous communication traceback. *Journal of Software*, 2011,22(10):2358−2371. http://www.jos.org.cn/1000-9825/3929.htm

Abstract: The spread spectrum based flow watermarking, which can be used to trace anonymity abuses effectively, applies spread spectrum technique to encode watermark signals and embeds them into suspect flows. This serves to confirm the communication relationship among network users. The implementation of watermarking can be divided into four phases: Signal encoding, flow modulation, flow demodulation and signal decoding. It is important to choose the right watermark carrier that determines the robustness and invisibility of watermarking techniques. Since most applications using anonymous communication, such as Web browsing, instant message and remote login generate interactive traffic with unstable traffic rate, existing spread spectrum based flow watermarking adopting traffic rate as its carrier has big limitations. Furthermore, there exist some attacks against the invisibility of this watermarking technique, destroying the traceback effect. Based on the spread spectrum flow marking model, this paper proposes a novel flow watermarking technique that adopts interval centroid as its watermark carrier, which is insensitive to different types of flows. The theoretical analysis and experimental results show that this flow watermarking technique is appropriate for both interactive and non-interactive traffic, and can resist most existing attacks against flow watermarking.

Key words: anonymous communication; flow watermarking; interactive traffic; spread spectrum; interval centroid

* 基金项目: 国家自然科学基金(60903161, 60903162, 61003257, 61070161, 61070158); 国家重点基础研究发展计划(973)(2010CB328104); 国家科技支撑计划(2010BAI88B03); 高等学校博士点专项科研基金(200802860031); 江苏省自然科学基金(BK2008030); 江苏省"网络与信息安全"重点实验室资助项目(BM2003201); "计算机网络与信息集成"教育部重点实验室资助项目(93K-9-2010-28); "信息安全"国家重点实验室(中国科学院研究生院)

收稿时间: 2009-12-05; 定稿时间: 2010-07-28

摘 要: 基于扩频的流水印通过扩频技术对水印信号进行编码,将其嵌入特定通信流中以确认网络主体间的通信关系,可以有效地对匿名滥用进行追踪.流水印的实施分为编码、调制、解调、解码等步骤.其中,水印载体的选择尤为重要,关系到水印的健壮性和隐秘性.已有扩频流水印方案选用流速率作为水印载体,由于大部分匿名通信应用,如 Web 浏览、即时通信、远程登录等均产生交互式流量,其速率是非稳定的,因而以流速率作为水印载体具有很大的局限性.此外,目前已存在多种针对此类水印隐秘性的攻击技术,降低了追踪的效果.在扩频流水印模型的基础上,引入与特定流无关的基于时隙质心的水印载体,提出一种新型流水印技术.理论分析与实验结果表明,这种新型流水印能够适用于对交互式与非交互式流量的追踪,有着更为广泛的适用性.此外,新型流水印能够有效抵抗现有攻击,保证追踪的隐秘性.

关键词: 匿名通信;流水印;交互式流量;扩频;时隙质心

中图法分类号: TP393 **文献标识码**: A

匿名通信技术在保护用户身份隐私的同时,也给网络犯罪的调查与追踪带来严峻的挑战.本文在扩频流水印模型的基础上,提出了一种基于时隙质心的流水印技术,能够对不同特征的匿名通信流量进行有效追踪并抵御多种针对流水印技术的攻击.

本文第 1 节介绍研究工作的背景与意义.第 2 节简要介绍匿名通信及其追踪方面的相关工作.第 3 节描述流水印追踪技术的基本原理和基于扩频技术的流水印.第 4 节给出基于时隙质心的新型流水印技术的详细设计.第 5 节对新技术的健壮性、适应性和隐秘性进行详细的理论分析.第 6 节在实用匿名通信系统下对新技术进行验证并给出实验结果.最后总结时隙质心流水印的技术特点及其在匿名通信追踪方面的优势并对下一步工作进行展望.

1 研究背景

随着 Internet 的迅猛发展和广泛应用,网络上的隐私问题受到越来越多的关注.在很多在线服务如电子商务、网上医疗中,用户身份的私密性是网络安全所关注的一个新的焦点.传统的网络安全技术注重对信息内容的保护,并不隐藏通信双方的身份信息和通信模式,攻击者通过 IP 报文的源地址、目的地址等信息能够轻而易举地获知用户的身份.

为保证用户身份的隐私性,研究人员设计了多种匿名通信系统[1],如 Crowds[2],Tor[3],Anonymizer[4]等.这些系统大多采用重路由技术,在发送者和接收者的通信路径上插入一个或多个中间节点,在对数据包进行转发的同时改写其中的 IP 地址等相关信息,隐藏数据包的来源、目的及出入关系.攻击者从数据包中获得的 IP 地址并非属于真正的发送者或接收者,从而无法推断准确的通信关系.结合内容层的加密技术,能够为用户提供全方位、多层次的身份隐私保护.

然而,匿名通信技术在保护用户身份隐私的同时,也可能为不法分子所利用而进行犯罪活动,身份的隐藏给网络犯罪的调查与追踪带来了严峻的挑战.针对这一问题,提出了多种匿名通信追踪方案.从实施对象和层次上,大致可将其分为两类:通信流层追踪技术和匿名协议层追踪技术.通信流层追踪技术利用通信流的特征或在流中加入标记,将匿名通信系统的输入流和输出流进行匹配,进而识别网络主体间的通信关系;匿名协议层追踪技术以追踪者控制一部分匿名通信服务节点为前提,通过参与匿名通信协议的执行从系统内部对网络主体间的通信关系加以关联.两类技术各有所长,总体而言,由于在通用性和资源需求方面具有优势,通信流层追踪技术的应用更为广泛.

流水印是一种比较准确和高效的通信流层追踪技术.这种技术在特定发送方的通信流中嵌入水印信号,该信号随通信流传播到接收方后被提取出来,两端信号进行对比以确定双方通信关系.基于扩频的流水印[5]是近年来出现的一类新型流水印技术,其将流水印的实施过程分为编码、调制、解调、解码等步骤,构建了一种全新的流水印模型,具有检测率高、误报率低等优点.然而,最初的扩频流水印技术(以下简称原始扩频流水印)采用流速率作为水印载体,而事实上,很多典型的匿名通信系统应用,如 Web 浏览、即时通信、远程登录等,所产生的

流量属于交互式流量(interactive traffic),这种流量一般速率较低且在其持续时间内波动很大,因此针对此类流量,以流速率作为水印载体存在一定的局限性.此外,很多针对此类流水印的攻击技术[6,7]能够发现并清除流中的水印信号,导致追踪失败.本文在扩频流水印模型的基础上引入与特定流无关的基于时隙质心[8]的水印载体,通过对时隙质心的调制嵌入水印信号,提出了一种新型流水印技术,避免了流速率的波动对信号提取的影响,解决了对交互式流量的追踪问题,有着更为广泛的适用性.此外,新型流水印能够有效抵抗现有攻击,保证追踪的隐秘性.

2 相关工作

1981 年,Chaum 开创性地提出了匿名通信的概念[1],阐述了匿名通信的基本思想——MIX 技术,即通过一系列 MIX 节点对消息进行重路由以掩盖用户的真实 IP 地址,并以加密、混淆、包填充、掩饰流等手段将通信流中的通信关系加以隐藏.此后的实用系统大都基于此技术而设计,如 Mixmaster[9],Mixminion[10],Tor[3],Anonymizer[4]等.其中,Mixmaster 和 Mixminion 属于基于消息的(高延时)匿名通信系统,Tor,Anonymizer 属于基于流的(低延时)匿名通信系统.高延时系统主要针对延时不敏感的应用,如电子邮件等,此类系统相对易于设计,发展比较成熟.低延时系统主要针对延时敏感的应用,如 Web 浏览、即时通信等,此类系统在设计上较为复杂,目前研究主要集中于此,本文的追踪技术也是针对此类系统.

匿名通信在保护用户身份隐私的同时也会为不法分子所滥用.针对匿名滥用的追踪技术本质上是对匿名通信系统的攻击,现有追踪技术从实施对象和层次上大致可分为两类:通信流层追踪技术和匿名协议层追踪技术.通信流层追踪技术将匿名通信系统作为“黑盒”处理,利用流的特征或在流中加入标记,将进出这个“黑盒”的输入流和输出流加以关联,从而识别出网络主体间的通信关系.早期的通信流层追踪技术主要采用被动关联的方法,通过观察通信流提取其相关特征,使用特定算法计算其相似性以确定通信关系[11,12].近年来,流关联技术有了进一步的发展,出现了主动流水印技术,极大地提高了追踪的效率,如:Wang 等人[13]提出用于 VoIP 匿名流识别的主动水印技术;Fu 等人[14]针对无线匿名通信网络提出了流标记追踪技术;Wang 等人[8]针对低延时匿名系统在转发数据时无法完全消除流中数据包时间特征的缺陷,提出了基于包抵达时间的流水印技术;Yu 等人[5]使用直序扩频技术,将水印信号扩频后通过调制流速率的方式嵌入通信流中,有效地提高了流水印的检测率;Houmansadr 等人[15]提出了一种非盲检测流水印,减小了对流的调制幅度,大大提高了流水印的隐秘性.匿名协议层追踪技术以追踪者控制一部分匿名通信服务节点为前提,通过参与匿名通信协议的执行,从系统内部对网络主体间的通信关系加以关联.这方面的典型工作包括:Wu 等人[16]提出一种在洋葱包的 GMT 域插入标记的方法,追踪针对洋葱路由 OR 节点的 DoS/DDoS 攻击源;Baucer 等人[17]针对 Tor 系统的路由协议提出了一种低消耗的路由攻击技术,通过这种攻击,追踪者可以占据通信链路的首尾节点,进而确定网络主体间的通信关系;Pries 等人[18]利用 Tor 的加密机制,提出了一种针对 Tor 的重放攻击,对比入口节点重放消息的时间和出口节点检测到错误的时间,确定这次通信的源和目的地址;Ling 等人[19]利用 Tor 中信元(cell)大小相等的特点,通过调制 Tor 节点一次发送信元数量的方法,在 Tor 的协议层嵌入水印以确认发送者和接收者之间的通信关系.

相比而言,匿名协议层追踪技术在准确性和效率上具有一定的优势,但依赖的资源较多,并且针对不同的系统需要设计不同的追踪方案,通用性较差.通信流层追踪技术依赖的资源较少,并且不关心匿名通信系统的具体设计细节,具有较好的通用性,但其追踪效果容易受网络噪声和具体流量特征的影响.本文提出的时隙质心流水印属于通信流层追踪技术,采用扩频技术对水印信号进行编码,具有较强的抗干扰能力,以不依赖于特定流的时隙质心作为水印载体,能够适应对不同特征流量的追踪要求.此外,这种技术能够抵御多种针对流水印的攻击,具有很高的隐秘性.

3 基于扩频流水印的追踪方案

3.1 流水印技术基本原理

流水印技术的基本思想如图 1 所示[5],为证实 Alice 和 Bob 之间的通信关系,位于 Alice 处的干涉者

(interferer)将水印嵌入需追踪的通信流中,当通信流经过匿名系统后,位于 Bob 处的嗅探者(sniffer)从流中提取水印,若两端的水印信号相匹配,则可确认 Alice 和 Bob 之间存在通信关系.

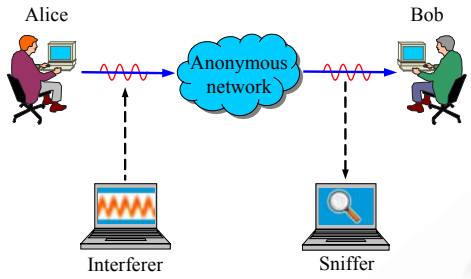

Fig.1 Principle of flow watermarking

图 1 流水印技术原理

3.2 扩频技术

扩频是无线通信中常用的一种传输技术,利用伪噪声码(pseudo-noise,简称 PN 码)将信号所占频带宽度扩展至远大于其所需的最小宽度进行传输,在接收方使用相同的 PN 码对扩频后的信号解扩以恢复出原始信号,该技术的主要优点是抗干扰性强,隐秘性高.

在各种扩频技术中,直序扩频(direct sequence spread spectrum,简称 DSSS)[5]以其简单易用的特点得到了广泛的应用,基于扩频的流水印一般也采用该技术.其基本原理如图 2 所示,原始信号 D_s 与 PN 码 P_s 相乘得到扩频信号 T_s(即 $T_s=D_s\cdot P_s$),T_s 通过信道进行传输,假设在传输过程中没有遭受干扰,接收方得到信号 $T_r=T_s=D_s\cdot P_s$,使用 PN 码 P_r 对其解扩以恢复出原始信号,具体方法如下:

$$D_r=\frac{\sum(T_r\cdot P_r)}{N}=D_s\frac{\sum(P_s\cdot P_r)}{N} \tag{1}$$

这里,·表示向量之间的内积,∑表示对一个向量中的所有元素求和,N 表示 PN 码长度.解扩时存在两种情况:

(1) $P_r=P_s$:若发送方和接收方的 PN 码相同,则 $P_r\cdot P_s=\mathbf{1}$.这里,$\mathbf{1}$ 表示长度为 N 且所有元素都为 1 的向量,因此,$D_r=D_s\frac{\sum(P_s\cdot P_r)}{N}=D_s\frac{N}{N}=D_s$,信号恢复成功;

(2) $P_r\neq P_s$:若发送方和接收方的 PN 码不同,则 $\sum(P_s\cdot P_r)/N\neq 1$,即 $D_r\neq D_s$,信号恢复失败.

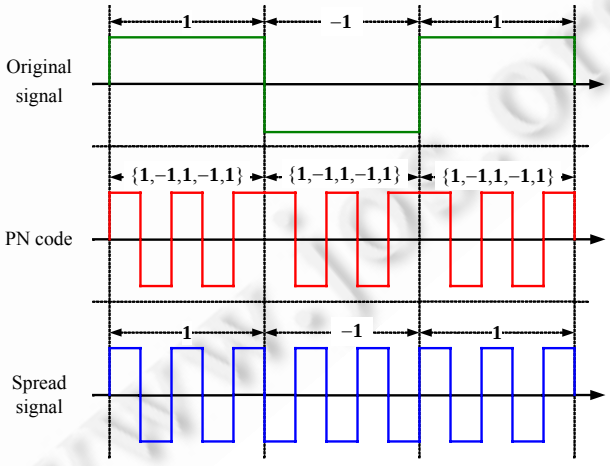

Fig.2 Principle of DSSS

图 2 直序扩频原理

3.3 基于扩频的流水印

基于扩频的流水印是近年来出现的一类新型流水印技术,它将流水印的实施过程分为编码、调制、解调、解码等步骤,构建了一种全新的流水印模型.具体实施时,位于发送方 Alice 处的干涉者使用扩频技术对水印信号进行编码,选取特定的水印载体,调制通信流以嵌入编码后的信号.位于接收方 Bob 处的嗅探者解调流并结合判断规则恢复出水印信号,将两端的水印信号进行比对,以确定 Alice 和 Bob 的通信关系.在最初的方案中,对水印信号的编码采用直序扩频技术,水印载体选用流速率,若编码信号为 1,则进行弱干涉,使通信流在该信号持续时间内保持较高的速率;若编码信号为–1,则进行强干涉,使通信流在该信号持续时间内保持较低的速率.这种变化的流速率可视为一组模拟信号,在经过匿名通信系统到达接收方后,分别使用高通滤波器和低通滤波器滤去信号中的直流分量(即平均速率)和网络噪声,利用共享的 PN 码和判断规则恢复出水印信号.具体实施流程如图 3 所示,详细的追踪方案可参考文献[5].

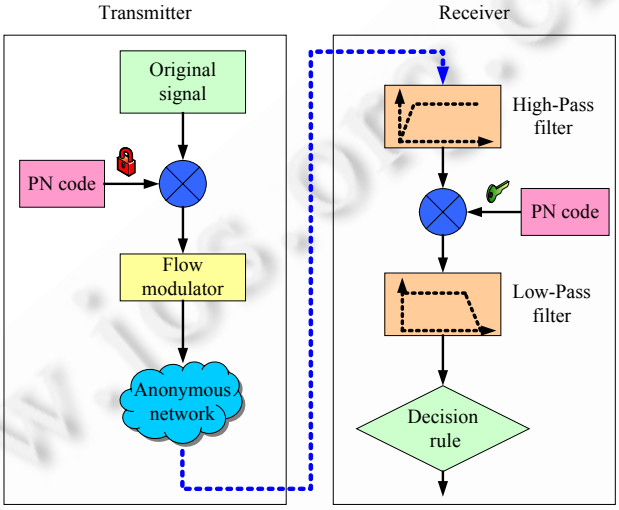

Fig.3 Spread spectrum based watermarking

图 3 基于扩频的流水印技术

4 基于时隙质心流水印的追踪方案

在原始扩频流水印中,使用流速率作为水印的载体.然而,若流速率波动较大,则会发生如下情况:对慢速流施加弱干涉,其速率仍然相对较慢;对快速流施加强干涉,其速率仍然相对较快.由于对水印载体的调制并未产生预期的效果,在滤去直流分量后将无法准确识别出对流施加的是何种干涉,从而无法提取出正确的水印信号,导致追踪时产生漏报或误报.因此,要保证追踪的准确性,稳定的水印载体至关重要.本节从提高稳定性入手,引入新的水印载体,提出一种基于时隙质心的新型流水印技术.

4.1 水印载体

流在本质上是一组源地址和目的地址都相同的包的集合,若从一个流中取偏移量 $o>0$ 起以 T 为单位将随后的流分成 n 个时隙:$I_0,I_1,\ldots,I_{n-1}$,假设其中共有 m 个包:$P_1,P_2,\ldots,P_m$,$t_i(i=1,2,\ldots,m)$表示每个包所对应的时间戳,t_0 为第 1 个时隙 I_0 的开始时间,$t_i'=t_i-t_0$ 表示包 P_i 相对于时隙 I_0 开始时间的偏移量,那么 $\Delta t_i=t_i' \bmod T$ 即为包 P_i 相对于其所属时隙开始时间的偏移量.

在文献[8]中,Wang 等人通过实验证明,以 X 作为除数对一个远大于它的随机变量 Y 进行取模运算,其结果近似服从[0,X]上的均匀分布.即对于 $t_1',t_2',\ldots,t_m'$,若 $T<<t_m'-t_1'$,那么Δt_i 服从[0,T]上的均匀分布,Δt_i 的期望为

$$E(\Delta t_i)=\frac{T}{2} \tag{2}$$

假设时隙 I_i 中共有 $k>0$ 个包 $P_{i,1},P_{i,2},\ldots,P_{i,k}$,定义 I_i 的质心为

$$C(I_i)=\frac{1}{k}\sum_{j=1}^{k}\Delta t_{i,j} \tag{3}$$

特别地,如果 I_i 为空,则定义 $C(I_i)$ 为 $T/2$.

为提高流水印的健壮性,本文选择一组时隙共同承载水印信号,其分配方式如图 4 所示.假设追踪时使用的水印信号共有 L 比特,PN 码的长度为 N.根据文献[8]对时隙质心的定义,对于所有 n 个时隙 $I_0,I_1,\ldots,I_{n-1}$,将其随机分为 L 组,每组包含 n/L 个时隙,对应于 1 比特水印信号,记对应于水印信号第 i 比特的时隙组为 G^i.每一比特水印信号扩频后对应的编码信号有 N 个码片(chip),将 G^i 随机分为 N 组,每组包含 $r=n/LN$ 个时隙,称 r 为冗余度,记对应于第 j 个码片的时隙组为 G^i_j,其所包含的时隙记为 $I^i_{j,l}$ (l=0,…,r−1),定义 $I^i_{j,0},\ldots,I^i_{j,r-1}$ 的共同质心为

$$C(G^i_j)=\frac{\sum_{l=0}^{r-1}[N^i_{j,l}C(I^i_{j,l})]}{\sum_{l=0}^{r-1}N^i_{j,l}}=\frac{\sum_{l=0}^{r-1}\sum_{k=1}^{N^i_{j,l}}\Delta t^i_{j,l,k}}{N^i_j} \tag{4}$$

这里,$\Delta t^i_{j,l,k}$ 表示时隙 $I^i_{j,l}$ 中第 k 个包相对于该时隙开始处的偏移,$N^i_{j,l}$ 表示时隙 $I^i_{j,l}$ 中包的数量,N^i_j 表示时隙组 G^i_j 中包的数量.由于 $E(\Delta t^i_{j,l,k})=T/2$,因此,

$$E(C(G^i_j))=\frac{T}{2} \tag{5}$$

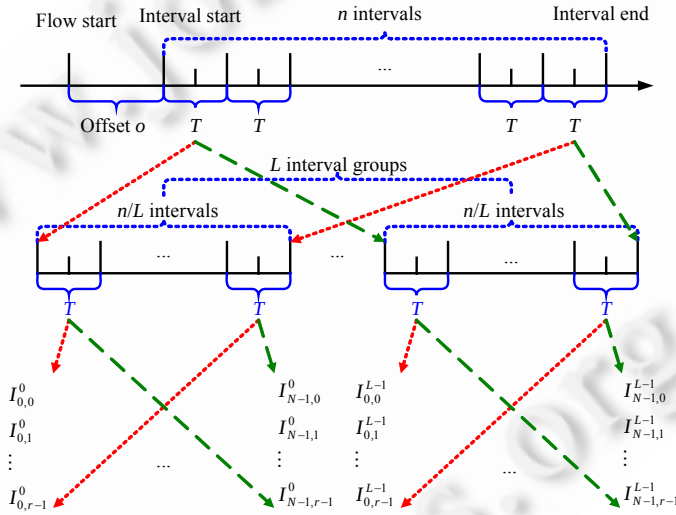

Fig.4 Assignment of interval groups

图 4 时隙组分配方式

根据大数定律,如果时隙组 G^i_j 中包的数量足够多,那么其质心 $C(G^i_j)$ 将稳定在 $T/2$ 附近.由公式(5)可知,基于时隙质心的水印载体只依赖于选定的时隙长度 T,而与具体的流无关.这种与特定流无关的特性对流水印的适应能力有着至关重要的作用,第 5.2 节将对此加以详细阐述.

要嵌入编码信号,只需调制其每个码片所对应的时隙组质心,若码片为 1,则增大 $\Delta t^i_{j,l,k}$,使

$$(\Delta t^i_{j,l,k})'=a+\frac{(T-a)\Delta t^i_{j,l,k}}{T} \tag{6}$$

这里,a 为调制幅度.由于 $\Delta t^i_{j,l,k}$ 服从[0,T)上的均匀分布,因此 $(\Delta t^i_{j,l,k})'\in[a,T)$ 且服从[a,T)上的均匀分布($a>0$).此时,$C(G^i_j)$ 的期望由 $T/2$ 增大为$(T+a)/2$.同理,若码片为−1,则减小 $\Delta t^i_{j,l,k}$,使

$$(\Delta t_{j,l,k}^{i})'=\frac{(T-a)\Delta t_{j,l,k}^{i}}{T} \tag{7}$$

因此, $C(G_j^i)$ 的期望由 $T/2$ 减小为$(T–a)/2$.由于包只能被延迟而不能被提前,因此在调制时隙组质心时,首先对所有的时隙施加一个较大的延时 b,若要嵌入的码片为 1,则对相应时隙组中的每个包施加一个大于 b 的延时,其结果相当于每个包在 b 的基础上进一步延迟,进而增大时隙组的质心;反之,若要嵌入的码片为–1,则对相应时隙组中的每个包施加一个小于 b 的延时,其结果相当于每个包在 b 的基础上被提前,进而减小时隙组的质心.

4.2 追踪流程

类似于原始扩频流水印[5],基于时隙质心流水印的匿名通信追踪技术同样包含编码、调制、解调、解码等步骤,其详细流程如下所述:

第 1 步:利用 PN 码 P_s 对水印信号 D_s 进行扩频,得到编码信号 T_s,即

$$T_s=D_s\cdot P_s \tag{8}$$

第 2 步:为编码信号的每一码片分配相应的时隙组,可使用随机数发生器(SNG)和特定的种子从 n 个时隙中随机挑选;

第 3 步:根据编码信号 T_s 对流进行调制,若码片为 1,增大其所对应的时隙组质心;若码片为–1,减小其所对应的时隙组质心,假设调制前的时隙组质心为 D,则其增大后为 $D+A$,减小后为 $D–A$.这里,A 表示质心的偏移幅度,与调制幅度 a 成正比关系.调制后流所承载的信号为

$$s=AD_sP_s+D \tag{9}$$

第 4 步:信号 s 经过匿名通信系统传输到接收方时,位于此处的嗅探者根据时隙组的分配情况提取信号:

$$r=AD_sP_s+D+w \tag{10}$$

这里,w 表示传输时受到的网络噪声干扰.

第 5 步:利用高通滤波器滤去直流分量 D,得到信号:

$$r'\approx AD_sP_s+w \tag{11}$$

第 6 步:利用相同的 PN 码 P_r 对信号 r'进行解扩,即

$$T_r=AD_sP_s\cdot P_r+w\cdot P_r \tag{12}$$

第 7 步:利用低通滤波器滤去网络噪声,结合下一节给出的判断规则恢复出水印信号 D_r.

4.3 判断规则

在得到信号 T_r 后,利用类似文献[5]中的判断规则恢复水印信号.为便于分析,暂不考虑网络上的噪声干扰.此时,嗅探者得到的编码信号可表示为

$$r=AD_sP_s+D \tag{13}$$

令 $t=AD_sP_s$,对信号 r 进行离散傅里叶变换(DFT):

$$R(k)=\sum_{n=0}^{N-1}(t(n)+D)W_N^{kn}=T(k)+\sum_{n=0}^{N-1}DW_N^{kn} \tag{14}$$

$$r(n)=\frac{1}{N}\sum_{k=0}^{N-1}R(k)W_N^{-kn} \tag{15}$$

其中,$W_N=e^{-j(2\pi/N)}$,N 为 PN 码的长度.

由公式(14)可得:

$$R(0)=\sum_{n=0}^{N-1}(t(n)+D)W_N^{0n}=\sum_{n=0}^{N-1}AD_sP_s(n)+ND=AD_s\sum_{n=0}^{N-1}P_s(n)+ND \tag{16}$$

假设 $\sum_{n=0}^{N-1}P_r(n)=\sum_{n=0}^{N-1}P_s(n)=x$,那么,

$$R(0)=AD_sx+ND \tag{17}$$

利用高通滤波器滤去直流分量 $R(0)$,得到:

$$\begin{aligned} r'(n)&=\frac{1}{N}\left[\sum_{k=0}^{N-1}R(k)W_N^{-kn}-R(0)\right]=\frac{1}{N}\left[\sum_{k=0}^{N-1}\left(T(k)+\sum_{m=0}^{N-1}DW_N^{km}\right)W_N^{-kn}-R(0)\right]\\ &=\frac{1}{N}\left[\sum_{k=0}^{N-1}T(k)W_N^{-kn}+ND-AD_sx-ND\right]=\frac{1}{N}\left[\sum_{k=0}^{N-1}T(k)W_N^{-kn}-AD_sx\right]=t(n)-\frac{AD_sx}{N}\end{aligned} \tag{18}$$

因此,

$$\begin{aligned}\sum T_r/N&=\frac{\sum(r'\cdot P_r)}{N}=\frac{\sum\left[\left(t-\frac{AD_sx}{N}\right)\cdot P_r\right]}{N}=\frac{\sum\left[\left(AD_sP_s-\frac{AD_sx}{N}\right)\cdot P_r\right]}{N}\\ &=\frac{AD_sN-\frac{AD_sx}{N}\sum P_r}{N}=AD_s-\frac{AD_sx^2}{N^2}=AD_s\left(1-\frac{x^2}{N^2}\right)\end{aligned} \tag{19}$$

这里,$\sum$表示对向量中所有元素求和.由于 PN 码一般由 m 序列发生器产生,因此,$|x|<|N|$,$1-x^2/N^2>0$.当 $D_s=1$ 时,$\sum T_r/N>0$;当 $D_s=-1$ 时,$\sum T_r/N<0$.因此,可得出判断规则:

$$D_r=\begin{cases}+1, & \sum T_r/N>0\\ -1, & \sum T_r/N<0\end{cases} \tag{20}$$

5 理论分析

5.1 健壮性分析

水印的健壮性是指水印在传输中遭受网络噪声干扰后仍然存活并且可被正确识别,具体表现为存在干扰时水印的检测率和误报率.

假设网络上的噪声 w 为高斯白噪声,其幅度服从正态分布 $N(0,\sigma)$,其经过 PN 码 P_r 扩频后仍为高斯白噪声.令 $w_p=\sum(w\cdot P_r)/N>0$,则

$$E(w_p)=E\left(\sum(w\cdot P_r)/N\right)=\sum[E(w_i)\cdot E(P_r)]/N \tag{21}$$

由于 $E(w_i)=0$,因此 $E(w_p)=0$.

$$var(w_p)=E(w_p-E(w_p))^2=E\left(\sum(w\cdot P_r)/N\right)^2=\sum(Ew_i^2\cdot EP_{r,i}^2)/N^2 \tag{22}$$

由于 $Ew_i^2=\sigma^2$,$EP_{r,i}^2=1$,因此 $var(w_p)=\sigma^2/N$,即高斯白噪声 w_p 的幅度服从正态分布 $N(0,\sigma/\sqrt{N})$.

在 PN 码唯一确定后,$A(1-x^2/N^2)$为常数.

那么,当 $D_s=1$ 时,$D_{+1}=A(1-x^2/N^2)+w_p$ 服从正态分布 $N(A(1-x^2/N^2),\sigma/\sqrt{N})$;当 $D_s=-1$ 时,$D_{-1}=-A(1-x^2/N^2)+w_p$ 服从正态分布 $N(-A(1-x^2/N^2),\sigma/\sqrt{N})$.假设水印信号为 1 和−1 的概率相同,那么对于水印信号的一个比特,误报率为

$$P_e=\frac{1}{2}P(D_{+1}<0)+\frac{1}{2}P(D_{-1}>0) \tag{23}$$

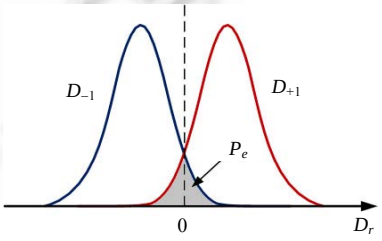

Fig.5 Distributions of signal value

图 5 信号取值的分布

由于 D_{+1} 与 D_{-1} 是对称的,如图 5 所示,因此 $P(D_{+1}<0)=P(D_{-1}>0)$,那么,

$$\begin{aligned}P_e=P(D_{-1}>0)&=\int_0^{\infty}\frac{1}{\sqrt{2\pi}\sigma/\sqrt{N}}\exp\left\{-\frac{[t+A(1-x^2/N^2)]^2}{2\sigma^2/N}\right\}\mathrm{d}t\\ &=\int_{\frac{A(1-x^2/N^2)}{\sigma/\sqrt{N}}}^{\infty}\frac{1}{\sqrt{2\pi}}\mathrm{e}^{-\frac{t^2}{2}}\mathrm{d}t\end{aligned} \tag{24}$$

对于水印信号的一个比特,其检测率 $P_c=1-P_e$.对于 n 比特的水印信号,

检测率:

$$P_d = P_c^n \tag{25}$$

误报率:

$$P_f = P_e^n \tag{26}$$

由此可见,提高检测率和降低误报率的关键在于减小 P_e 的值.

根据公式(24),减小 P_e 必须增大 $A(1-x^2/N^2)/(\sigma/\sqrt{N})$,达到此目的有两条途径:增加质心偏移幅度 A(也即增加调制幅度 a)或增大 PN 码长度 N.增加调制幅度会使嵌入水印的流与原始流之间存在较大的差异,容易被发现,降低了追踪的隐秘性.因此,提高检测率、降低误报率的最好方法是增加 PN 码的长度 N.

5.2 适应性分析

水印的适应性即指流水印技术对不同特点的流的适应能力.本质上,流水印技术是将选定的水印载体视为一组信号,调制信号的值以嵌入水印,通信流传输到接收方后,对目标流进行解调,将流中的信号滤去直流分量以还原出对信号的调制方式,进而提取出水印.水印载体作为直流分量存在于信号中,若水印载体的稳定性较差,滤去直流分量后所还原出的调制方式将产生偏差,进而提取出错误的水印,导致追踪的失败.

假设理论上稳定的水印载体为 D,实际调制时不断波动的水印载体为 D',令 $y=D'-D$,那么 $r=t+D'-D+D=t+y+D$,对其进行离散傅里叶变换:

$$R(k)=\sum_{n=0}^{N-1}[t(n)+y(n)+D(n)]W_N^{kn}=T(k)+Y(k)+\sum_{n=0}^{N-1}DW_N^{kn} \tag{27}$$

$$r(n)=\frac{1}{N}\sum_{k=0}^{N-1}R(k)W_N^{-kn} \tag{28}$$

其中,$W_N=e^{-j(2\pi/N)}$.

$$R(0)=\sum_{n=0}^{N-1}[t(n)+y(n)+D(n)]W_N^{0n}=\sum_{n=0}^{N-1}[t(n)+y(n)]+ND \tag{29}$$

$$\begin{aligned} r'(n)&=\frac{1}{N}\left[\sum_{k=0}^{N-1}R(k)W_N^{-kn}-R(0)\right]=\frac{1}{N}\left[\sum_{k=0}^{N-1}\left(T(k)+Y(k)+\sum_{m=0}^{N-1}DW_N^{km}\right)W_N^{-kn}-R(0)\right]\\ &=\frac{1}{N}\left[\sum_{k=0}^{N-1}T(k)W_N^{-kn}+\sum_{k=0}^{N-1}Y(k)W_N^{-kn}+ND-\sum_{n=0}^{N-1}(t(n)+y(n))-ND\right]\\ &=t(n)+y(n)-\frac{1}{N}\sum_{n=0}^{N-1}[t(n)+y(n)] \end{aligned} \tag{30}$$

由于 D'围绕 D 上下波动,且 D_s 为+1 和−1 的概率相同,因此,$\frac{1}{N}\sum_{n=0}^{N-1}[t(n)+y(n)]$ 相对于 $t(n)+y(n)$是一个非常小的值,可近似得出 $r'\approx t+y$,那么,

当 D_s=1 时,

$$\frac{\sum(r'\cdot P_r)}{N}=\frac{\sum[(AP_s(n)+y(n))\cdot P_r]}{N}=A+\frac{\sum[y(n)\cdot P_r]}{N} \tag{31}$$

当 D_s=−1 时,

$$\frac{\sum(r'\cdot P_r)}{N}=\frac{\sum[(-AP_s(n)+y(n))\cdot P_r]}{N}=-A+\frac{\sum[y(n)\cdot P_r]}{N} \tag{32}$$

由于 $y(n)$与 P_r 没有对应关系,不能保证 $\sum[y(n)\cdot P_r]$ 必然为正或为负.

因此,要确保任何情况下 D_s=1 时 $\sum(r\cdot P_r)/N>0$,D_s=−1 时 $\sum(r\cdot P_r)/N<0$,则必须满足:

$$A>\left|\frac{\sum[y(n)\cdot P_r]}{N}\right| \tag{33}$$

若要满足公式(33),可通过 3 种途径实现:增大质心偏移幅度 A、增加 PN 码长度 N 及减小$|y(n)|$.类似上一节,

增加 A 必然导致对流的改变过于明显,降低水印的隐秘性;减小$|y(n)|$,也就是尽量使作为直流分量的水印载体在调制前保持稳定.在时隙质心流水印中,水印载体为时隙组质心,根据大数定律,只要取足够多的包,那么Δt_i 的平均值,即质心将逼近并稳定在 $T/2$ 处.这种不依赖于特定流的特性,使水印载体在面对任何特征流量(包括交互式与非交互式流量)时都具有非常高的稳定性.相比而言,原始扩频流水印虽然可以通过增大 PN 码长度的方式尽量满足公式(33),但其水印载体的稳定性依赖于特定的流,若流速率的波动非常大,即$|y(n)|$非常大,则达到同样的效果需要大幅增加 N 的值,这将大大增加完成追踪所需花费的时间,甚至在流的持续时间内都难以完成.而时隙质心流水印却不存在这样的问题,在包的数量满足水印对载体稳定性的要求后,水印载体的值将保持稳定,无需增加包的数量或 PN 码的长度以应付速率波动较大的流,从而保证了追踪时间和计算规模的可控性.

5.3 隐秘性分析

扩频技术的使用将嵌入通信流中的水印隐蔽于网络噪声之中,具有较强的隐秘性[5].然而很多具有针对性的攻击技术,如多流攻击[6]、自相关性攻击[7]等,仍然能够发现水印的存在,破坏追踪的隐秘性.

在多流攻击中,首先建立通信流的理论模型,通过将多条嵌入水印的流叠加后与理论模型进行对比,放大水印对流特征的改变,进而发现流水印.为抵御这种攻击,可对不同的流使用不同的时隙组分配方式,即建立一个随机种子集合,对不同的流随机地从集合中选取一个种子进行时隙组分配.提取水印时,逐一测试集合中的种子,对于追踪的实施者,由于该集合是已知的,相对于单一的时隙组分配方式,计算复杂度呈线性增长;而对于攻击者,由于该集合是未知的,逐一测试时隙组的分配方式将使其计算复杂度呈指数级增长,当冗余度达到一定规模后,计算复杂度将会超越攻击者的计算能力.而攻击者一旦无法获知准确的时隙组分配方式,也就难以准确定位承载特定信号的水印载体在流中的具体位置,从而无法简单地通过叠加多条嵌入水印的流放大流特征的改变,进而发现流水印的存在.在自相关性中,攻击者利用 PN 码在流调制时被反复使用从而导致流在短时间内出现自相似性这一特点,通过计算自相关性期望平方(mean-square autocorrelation,简称 MSAC)来检测水印的存在.在基于时隙质心的流水印技术中,由于时隙组是随机分配的,攻击者在不确定时隙组具体分配方式的情况下难以得到相应码片所具体对应的时隙质心,进而无法判断流是否在短时间内出现了自相似性,也就无法计算出 MSAC.因此,基于时隙质心的流水印对这类攻击具有天然的免疫力.

6 实 验

对时隙质心流水印的性能验证通过实用匿名通信系统 Tor[3]进行.实验网络环境设置如图 6 所示,发送者与接收者通过 Tor 网络进行通信.干涉者位于发送者与 Tor 之间,向途经它的通信流中嵌入水印;嗅探者位于接收者处,从接收到的通信流中提取水印.干涉者与嗅探者间进行水印信号的比对,以计算追踪的检测率和误报率.

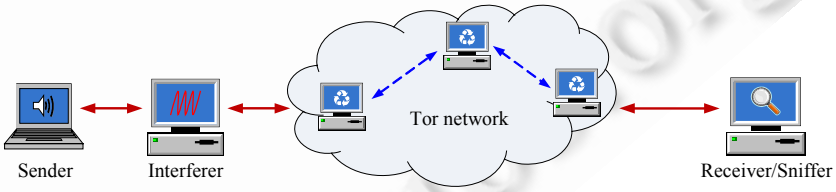

Fig.6 Experimental network setup

图 6 实验环境设置

6.1 时隙质心流水印的检测率

在时隙质心流水印的检测率实验中,干涉者向通信流中嵌入 32 比特水印信号.检测时,允许提取出的水印信号与嵌入的水印信号之间存在一定程度的误差,即有部分比特不一致,不一致的比特数称为水印间的海明距离(Hamming distance,简称 HD).确定一个阈值,若两个信号间的海明距离低于这个阈值,则认为这两个信号是相匹配的.第 5 节的理论分析表明,影响水印检测率的主要因素包括调制幅度、PN 码长度以及所使用的数据包数量.其中,数据包的数量与时隙长度及冗余度直接相关,本文将逐一对其进行测试.

6.1.1 调制幅度对检测率的影响

为测试调制幅度对检测率的影响,设定时隙长度 T=800ms,冗余度 r=5,PN 码长度 N=9,分别测试调制幅度 a 从 50ms 增大到 450ms 时的检测率.实验结果如图 7 所示,检测率随调制幅度 a 的增大而增大;并且允许的海明距离越大,得到的检测率越高.整体上,海明距离为 4、调制幅度为 300ms 后可达到近 100%的检测率.实验结果与第 5.1 节和第 5.2 节的理论分析结论相一致.

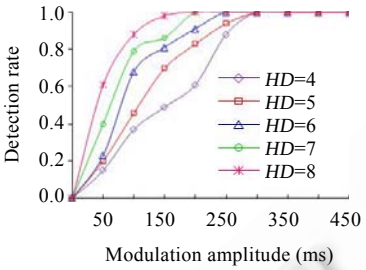

Fig.7 Detection rate changing with modulation amplitude

图 7 调制幅度对检测率的影响

6.1.2 PN 码长度对检测率的影响

为测试 PN 码长度对检测率的影响,设定时隙长度 T=800ms,冗余度 r=5,调制幅度 a=250ms,分别测试 PN 码长度从 3 增加到 17 时的检测率.实验结果如图 8 所示,检测率随 PN 码长度 N 的增大而增大;并且允许的海明距离越大,得到的检测率越高.整体上,海明距离为 4、PN 码长度为 13 后可达到近 100%的检测率.实验结果与第 5.1 节和第 5.2 节的理论分析结论相一致.

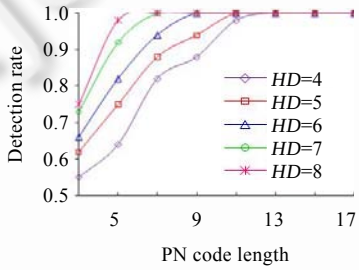

Fig.8 Detection rate changing with PN length

图 8 PN 码长度对检测率的影响

6.1.3 时隙长度对检测率的影响

为测试时隙长度对检测率的影响,设定调制幅度 a=150ms,冗余度 r=5,PN 码长度 N=9,分别测试时隙长度 T 从 400ms 增大到 1 300ms 时的检测率.实验结果如图 9 所示,检测率随时隙长度 T 的增大而增大;并且允许的海明距离越大,得到的检测率越高.整体上,海明距离为 4、时隙长度为 1 200ms 后可达到近 100%的检测率.实验结果与第 5.2 节的理论分析结论相一致.

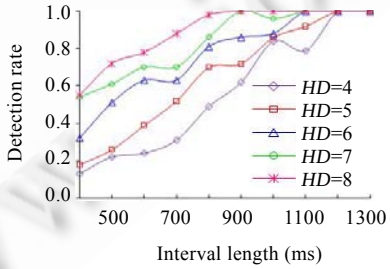

Fig.9 Detection rate changing with interval length

图 9 时隙长度对检测率的影响

6.1.4 冗余度对检测率的影响

为测试冗余度对检测率的影响,设定调制幅度 a=150ms,时隙长度 T=1000ms,PN 码长度 N=9,分别测试冗余度 r 从 1 增大到 10 时的检测率.实验结果如图 10 所示,检测率随冗余度 r 的增大而增大;并且允许的海明距离越大,得到的检测率越高.整体上,海明距离为 4、冗余度为 7 后可达到近 100%的检测率.实验结果与第 5.2 节的理论分析结论相一致.

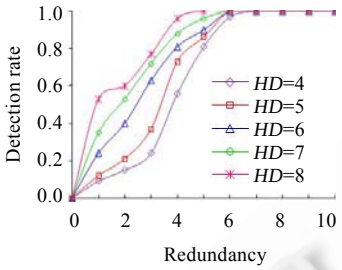

Fig.10 Detection rate changing with redundancy

图 10 冗余度对检测率的影响

6.2 时隙质心流水印的误报率

在对一条未嵌入任何水印的流使用判断规则时可能产生错误,从中提取出与某条流相匹配的水印,从而造成误判.这种情况发生的概率要高于对嵌入水印的流使用判断规则时造成误判的概率.因此,本文在时隙质心流水印的误报率实验中,测试对未嵌入水印的流使用判断规则时的误报率.一条流未嵌入水印,即对它的调制幅度为 0,由公式(24)可得,这种情况下,P_e=0.5,误报率 P_f=0.5^n,其中 n 为水印长度.因此,理论上误报率随着水印长度的递增以指数速度递减.本文测试水印长度从 1 到 8 时误报率的变化.干涉者对流不进行任何调制,嗅探者对每一固定的水印长度随机生成一个具体的水印信号,设定时隙长度 T=800ms,冗余度 r=5.分别测试 PN 码长度 N 从 3~11 时,从接收到的流中提取出该水印信号的检测率,取其平均值作为该水印长度下追踪的误报率.这里不考虑水印间的海明距离,两个水印相匹配当且仅当它们完全相同.实验结果如图 11 所示,误报率随水印长度的增加迅速减小;在水印长度大于 7 之后,保持低于 0.1%的误报率.

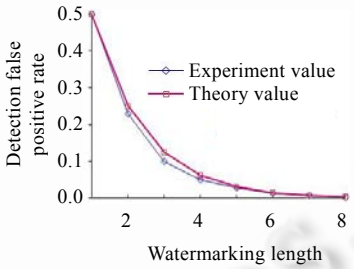

Fig.11 Detection false positive rate changing with watermark length

图 11 水印长度对误报率的影响

6.3 时隙质心流水印与原始扩频流水印的比较

为比较时隙质心流水印与原始扩频流水印在应对交互式流量时的适应能力,发送者周期性地改变流的速率,流速率的波动程度由其持续时间内的最高速率与最低速率比值来描述(值为 1,表明这是一条匀速的流).分别以时隙质心流水印和原始扩频流水印方法嵌入水印信号,两种方法所使用的 PN 码长度都为 9,时隙质心流水印中时隙长度 T=800ms,冗余度 r=5,调制幅度 a=300ms.在原始扩频流水印中,每个码片对应的时间长度为 4 000ms,调制幅度为平均速率的 3/8.实验结果如图 12 所示,原始扩频流水印在面对匀速流量时可保证较高的检测率;但是随着流速率波动性地增加,性能下降得较为明显,而时隙质心流水印则基本不受速率波动的影响,始

终保持较高的检测率.

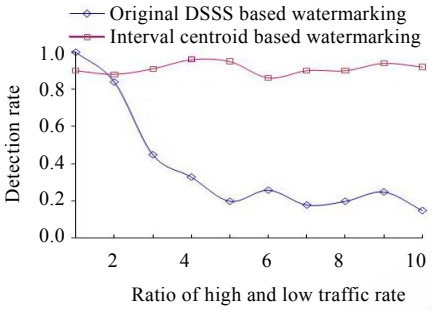

Fig.12 Detection rate comparison between the two watermarks

图 12 两种水印的检测率对比

7 结束语

流水印技术是一种准确、高效的匿名滥用追踪技术,很多匿名通信系统的典型应用产生交互式流量,速率较低且波动性较大.针对这一问题,本文引入一种与特定流无关的基于时隙质心的水印载体,提出了一种新型流水印技术.在水印嵌入时,以直序扩频方式对水印信号进行编码,将流分成若干时隙,对编码信号每一码片,随机选择一组时隙构成与其相对应的时隙组,通过增大或减小相应的时隙组质心嵌入编码信号.信号通过匿名通信系统后,滤去其中的直流分量和网络噪声,解调时隙组质心并结合判断规则提取水印,将两端的水印信号进行比对以确定双方的通信关系.基于时隙质心的水印载体不依赖于特定的流,具有良好的稳定性,因而这种新型流水印技术能够同时用于对交互式与非交互式流量的追踪,具有更为广泛的适用性.此外,时隙组的随机选取与多种分配方式的结合,能够迅速增加攻击者的计算复杂度,可以有效抵抗多流攻击、自相关性攻击等针对流水印的攻击技术,保证追踪的隐秘性.

下一步的研究工作包括:引入其他扩频技术,如,时跳扩频(time hopping spread spectrum,简称 THSS)、频跳扩频(frequency hopping spread spectrum,简称 FHSS)等,设计更为高效而精确的编解码算法,提高流水印的隐秘性;建立通用的追踪框架,提出适当的指标对各种追踪技术进行比较与评价.

References:

[1] Chaum DL. Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM, 1981,24(2): 84−88. [doi: 10.1145/358549.358563]

[2] Reiter MK, Rubin AD. Crowds: Anonymity for Web transactions. ACM Trans. on Information and System Security, 1998,1(1): 1−23. [doi: 10.1145/290163.290168]

[3] Dingledine R, Mathewson N, Syverson P. Tor: The second-generation onion router. In: Proc. of the 13th Conf. on USENIX Security Symp. San Diego: USENIX Association, 2004. http://dl.acm.org/citation.cfm?id=1251396

[4] Anonymizer. Inc., 2009. http://www.anonymizer.com

[5] Yu W, Fu XW, Graham S, Xuan D, Zhao W. DSSS-Based flow marking technique for invisible traceback. In: Proc. of the 2007 IEEE Symp. on Security and Privacy. Oakland: IEEE Computer Society, 2007. 18−32. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4223211 [doi: 10.1109/SP.2007.14]

[6] Kiyavash N, Houmansadr A, Borisov N. Multi-Flow attacks against network flow watermarking schemes. In: Proc. of the 17th Conf. on Security Symp. San Jose: USENIX Association, 2008. 307−320. http://dl.acm.org/citation.cfm?id=1496732

[7] Jia W, Tso FP, Ling Z, Fu X, Xuan D, Yu WX. Blind detection of spread spectrum flow watermarks. In: Proc. of the IEEE Conf. on Computer Communications. Rio de Janeiro: IEEE Computer Society, 2009. 2195−2203. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5062144 [doi: 10.1109/INFCOM.2009.5062144]

[8] Wang XY, Chen SP, Jajodia S. Network flow watermarking attack on low-latency anonymous communication systems. In: Proc. of the 2007 IEEE Symp. on Security and Privacy. Oakland: IEEE Computer Society, 2007. 116−130. http://www.computer.org/portal/web/csdl/doi/10.1109/SP.2007.30 [doi: 10.1109/SP.2007.30]

[9] Moller U, Cottrell L, Palfrader P, Sassaman L. Mixmaster Protocol-Version 2. IETF Internet Draft, 2003.

[10] Danezis G, Dingledine R, Mathewson N. Mixminion: Design of a type III anonymous remailer protocol. In: Proc. of the 2003 IEEE Symp. on Security and Privacy. Oakland: IEEE Computer Society, 2003. 2−15. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1199323 [doi: 10.1109/SECPRI.2003.1199323]

[11] Levine BN, Reiter MK, Wang CX, Wright M. Timing attacks in low-latency mix systems. In: Proc. of the Financial Cryptography. Key West: Springer-Verlag, 2004. 251−265. http://www.springerlink.com/content/n4khdtwk7dqvj0u0/

[12] Zhu Y, Fu XW, Graham B, Bettati R, Zhao W. On flow correlation attacks and countermeasures in mix networks. In: Proc. of the Workshop on Privacy Enhancing Technologies. Toronto: Springer-Verlag, 2004. 207−225. http://www.springerlink.com/content/kej7uwxee8h71p81/ [doi: 10.1007/11423409_13]

[13] Wang XY, Chen SP, Jajodia S. Tracking anonymous peer-to-peer VoIP calls on the Internet. In: Proc. of the 12th ACM Conf. on Computer and Communications Security. Alexandra: ACM Press, 2005. 81−91. http://dl.acm.org/citation.cfm?id=1102133 [doi: 10.1145/1102120.1102133]

[14] Fu XW, Zhu Y, Graham B, Bettati R, Zhao W. On flow marking attacks in wireless anonymous communication networks. In: Proc. of the IEEE Int'l Conf. on Distributed Computing Systems. Columbus: IEEE Press, 2005. 493−503. http://www.computer.org/portal/web/csdl/doi/10.1109/ICDCS.2005.55 [doi: 10.1109/ICDCS.2005.55]

[15] Houmansadr A, Kiyavash N, Borisov N. RAINBOW: A robust and invisible non-blind watermark for network flows. In: Proc. of the 16th Annual Network & Distributed System Security Symp. San Diego, 2009. https://netfiles.uiuc.edu/ahouman2/www/papers/NDSS09.pdf

[16] Wu ZQ, Yang B. An advanced marking scheme and realization for onion routing traceback. Journal of China Institute of Communications, 2002,23(5):96−102 (in Chinese with English abstract).

[17] Bauer K, McCoy D, Grunwald D, Kohno T, Sicker D. Low-Resource routing attacks against Tor. In: Proc. of the Workshop on Privacy in the Electronic Society. Alexandria: ACM Press, 2007. 11−20. http://dl.acm.org/citation.cfm?id=1314336 [doi: 10.1145/1314333.1314336]

[18] Pries R, Yu WW, Fu X, Zhao W. A new replay attack against anonymous communication networks. In: Proc. of the IEEE Int'l Conf. on Communications. Beijing: IEEE Press, 2008. 1578−1582. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4533341 [doi: 10.1109/ICC.2008.305]

[19] Ling Z, Luo JZ, Yu W, Fu XW, Xuan D, Jia W. A new cell counter based attack against Tor. In: Proc. of the 16th ACM Conf. on Computer and Communications Security. Chicago: ACM Press, 2009. 578−589. http://dl.acm.org/citation.cfm?id=1653732 [doi: 10.1145/1653662.1653732]

附中文参考文献:

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

张璐(1983－),男,江苏滨海人,博士生,主要研究领域为网络安全,匿名通信.

杨明(1979－),男,博士,讲师,主要研究领域为网络安全.

罗军舟(1960－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为下一代网络体系结构,网格与云计算,网络安全,服务计算.

何高峰(1984－),男,博士生,主要研究领域为网络安全.