doi:10.3969/j.issn.1000-436x.2014.07.022

主动网络流水印技术研究进展

郭晓军[1,2,3]，程光[1,3]，朱琛刚[1,3]，TRUONG Dinh-Tu[1,3]，周爱平[1,3]

(1. 东南大学 计算机科学与工程学院，江苏 南京 210096；
2. 西藏民族学院 信息工程学院，陕西 咸阳 712082；
3. 东南大学 计算机网络和信息集成教育部重点实验室，江苏 南京 210096)

摘 要：在匿名网络环境下通信双方关系确认、僵尸网络控制者追踪、中间跳板主机发现等方面，以被动网络流量分析（passive traffic analysis）为核心的传统入侵检测与流关联技术存在空间开销大、实时性差、识别率低、灵活性欠佳、难以应对加密流量等明显缺点。而将主动网络流量分析与数字水印思想相融合的主动网络流水印（ANFW, active network flow watermark）技术能有效克服传统被动网络流量分析方法的不足，已引起了国内外学者的广泛关注。首先阐述了 ANFW 机制的通用模型，总结了 ANFW 技术的分类及所涉及的角色关系；其次，详细综述了近年来提出的多种典型的基于不同网络流特征的 ANFW 技术，并进行对比性总结；最后，概述了当前 ANFW 技术自身安全威胁及应对措施现状，展望了其未来的研究方向。

关键词：网络安全；主动流量分析；网络流水印；流特征；匿名通信；跳板节点；僵尸网络

中图分类号：TP393 **文献标识码**：A **文章编号**：1000-436X(2014)07-0178-15

Progress in research on active network flow watermark

GUO Xiao-jun[1,2,3], CHENG Guang[1,3], ZHU Chen-gang[1,3], TRUONG Dinh-Tu[1,3], ZHOU Ai-ping[1,3]

(1. School of Computer Science and Engineering, Southeast University, Nanjing 210096, China;
2. School of Information Engineering, Tibet Nationalities Institute, Xianyang 712082, China;
3. Ministry of Education Key Laboratory of Computer Network and Information Integration, Southeast University, Nanjing 210096, China)

Abstract: In face of confirming user communication relationship in anonymous network, tracing botmaster and detecting stepping stones, traditional intrusion detection and flow correlation methods which mainly rely on passive traffic analysis have shown many drawbacks obviously, such as high space costs, poor real-time, low accuracy, poor flexibility, fail in dealing with encrypted traffic and so on. However, the active network flow watermark(ANFW) which combined the idea of digital watermarking and active traffic analysis can overcome the drawbacks above effectively. ANFW has aroused extensive attention of scholars at home and abroad. Firstly, the general model of ANFW is presented, and the classification of existing proposals and roles involved in ANFW are summarized. Then, several representative ANFW approaches using distinct network flow characteristics are presented and compared in detail. Finally, threats against existing ANFW technology and their corresponding countermeasures are overviewed, also some future research directions about ANFW are discussed.

Key words: network security; active traffic analysis; network flow watermark; network flow characteristics; anonymous communication; stepping stones; botnet

收稿日期：2013-10-07；**修回日期**：2013-12-11

基金项目：江苏省科技支撑计划（工业）基金资助项目（BE2011173）；江苏省未来网络前瞻性基金资助项目（BY2013095-5-03）；江苏省六大人才高峰基金资助项目（2011-DZ024）；国家重点基础研究发展计划（“973”计划）基金资助项目（2009CB320505）；国家自然科学基金资助项目（60973123）

Foundation Items: Jiangsu Provincial Science and Technology Support Program—Industrial Part (BE2011173); The Future Network Proactive Program of Jiangsu Province (BY2013095-5-03); The Six Talent Peak Project of Jiangsu Province(2011-DZ024); The National Basic Research Program (973 Program) of China (2009CB320505); The National Natural Science Foundation of China (60973123)

1　引言

近年来，随着 Internet 爆炸式的发展，网络安全问题日益严重，尤其在经济利益的驱使下，各种网络攻击手段层出不穷，给用户带来巨大经济损失。一方面，为了逃避检测和追踪，攻击者往往并不直接对目标主机发起攻击，而是使用 SSH[1]，IPsec 协议[2]登录跳板节点（stepping stone）主机[3~6]、借助匿名通信系统[7~9]、僵尸网络 [10~12]等手段来隐藏自己的真实身份，给攻击流追踪、真实攻击源定位、网络监控与管理等方面造成了巨大困难；另一方面，由于经济、政治利益等因素，犯罪分子可利用匿名通信系统（如 Tor、Mixmaster 等）传播赌博、色情、暴力、反动等不良信息，这些违法通信行为严重污染了合法用户的网络环境，也使对这些行为的犯罪取证及网络审查面临严峻挑战。

针对上述问题，传统的入侵检测系统 IDS（intrusion detection systems）与流关联（flow correlation）技术主要采用被动网络流量分析方法[3~5,13,14]。该类方法通过布置在网络关键位置的节点来收集网络流量，借助于分析和比较各网络流量中数据分组数量[5]、大小[13]、时序等特征[15,16]，来确认各网络流之间的关联匹配关系。但此类方法要捕获和检查所有网络流量，会明显增加网络设备的时空开销，其离线分析方式也导致识别滞后性，实时性较差，可扩展性不强，难以应用在大规模、高带宽网络环境，尤其面对加密流量及匿名通信环境更显得力不从心。为了改善传统被动式方法的不足，应对加密流量及匿名通信环境中流追踪和定位问题，主动网络流水印（ANFW）技术应运而生。

ANFW 技术主要借鉴数字水印(digital watermarking)[17]的思想，通过主动改变可疑发送端（sender）所产生流[18]的某些特征，使之隐蔽地携带一些特殊标记信息，即水印（watermark），在经过通信网络传输后，若从可疑接收端（receiver）所嗅探的网络流中能检测出相应的水印，则认为 sender 和 receiver 之间存在网络流关联，从而可认定它们之间存在明确的通信关系，是一种主动网络流量整形与分析技术。与传统被动网络流量分析相比，ANFW 方法显著优势在于能够较好地适用于存在加密流量、跳板节点、匿名通信等多种网络环境，其过程对于可疑收发双方无法察觉，即具备透明性，且可用较少的时空开销确认 sender 和 receiver 通信关系，具有较高的识别率，此外，还可同时面向多数据流的追踪和定位等。因此，该技术近年来也逐渐成为网络安全研究领域的热点。

目前，国内外学者已在主动网络流水印系统模型、流水印载体选择及流水印调制解调技术等方面开展了较多研究工作。本文试图以 TCP/IP 网络体系结构为核心，从层次的视角对现有主动网络流水印技术研究进行归纳和总结，并对未来主动网络流水印技术发展趋势及可能的研究方向进行了展望。

2　主动网络流水印概述

2.1　通用模型

一些学者已从不同的角度给出了 ANFW 模型[19,20]。为了更好理解主动网络流水印本质和描述方便，本文在借鉴已有研究工作的基础上给出了 ANFW 的通用模型。

定义 1　ANFW 可描述为一个六元组<*OF*, *W*, *AP*, *EM*, *DE*, *CM*>。其中，

1) *OF*(original flows)为原始网络流集合，本文中，$OF=\{f_1, f_2, \cdots, f_n\}$，$f_i$（$i$=1, 2, …, n）为 sender 产生的流。

2) *W* 为嵌入的水印信息，$W=\{w_1, w_2, \cdots, w_l\}$，$|W|=l(l>0)$，$w_i$ 为水印信息位，且 $w_i\in\{0,1\}$，l 称为水印容量。

3) *AP*(assist parameters)是在流 f_i 中嵌入水印 *W* 时所需的辅助参数集合，$AP=\{ap_1, ap_2, \cdots, ap_m\}$，其中，$ap_i$ 为辅助参数，如 f_i 中各数据分组之间的时间间隔、PN(pseudo-noise)码[21]等。不同 ANFW 方法具有多个不同的辅助参数。

4) *EM* 为调制或嵌入水印函数

$$EM(f_i, W, AP)=f_i^w \tag{1}$$

5) *DE* 为解调或提取水印函数

$$DE(f_r, AP)=W' \tag{2}$$

其中，f_r 为 receiver 处捕获的网络流。

6) *CM* 为比较函数，*Th* 为预先设置的阈值。

$$CM(W, W')\leqslant Th \tag{3}$$

图 1 给出了主动网络流水印机制的通用模型。水印嵌入器（watermark embedder）首先收集 Bob 产生的流 f_i，选取流 f_i 某个特征（如速率、分组间隔等）作为承载水印 *W* 的载体，然后在式(1)的控制下，主动改变该特征并使之呈现不同状态，用以

表示水印信息位 w_i，从而完成水印 W 在流 f_i 中的嵌入过程。水印检测器（watermark decoder）捕获到达 Alice 的流 f_r，应用式(2)提取出 f_r 所携带的水印 W'，若 W' 与 W 满足式(3)，则说明 f_r 是 f_i 在经过通信网络传输后叠加网络噪声（如网络拥塞、抖动等）所形成的流，从而确认 Bob 与 Alice 之间存在通信行为，否则，则认为 f_r 与 f_i 无关，即 Bob 与 Alice 不存在通信行为。

2.2 应用场景示例

ANFW 技术可通过调整网络中流特征来确定可疑发送端与可疑接收端之间是否存在明确的通信关系，尤其适用于加密流量、跳板节点、匿名通信等多种网络环境。为更好地理解 ANFW 机制及其应用，此处给出一个 ANFW 在匿名通信网络 Tor[7] 中的应用示例，如图 2 所示。

Tor 是一个开源项目，借助洋葱头路由器 OR（onion router）来隐藏原始 TCP 流量的真实信息，为 TCP 应用提供匿名通信服务，可看成基于 Internet 的覆盖网。在 Tor 匿名网络中，OR 与 OR 之间构成匿名信道或者加密信道，使用 TLS（transport layer security）协议加密原始 TCP 流量，且并将其转变为大小相同的数据分组。这样，原始 TCP 流量中的一些敏感信息（如源宿 IP 地址、端口号等）就变成了密文，即使数据分组被捕获也无法识别，达到了匿名原始 TCP 流量的目的。

攻击者可利用 Tor 网络的匿名性特点，在隐藏自己真实主机信息的情况下对网络中的主机进行入侵或攻击。很显然，若采用被动流量为分析方法是难以对攻击源头进行准确追踪和定位的。在此情况下，ANFW 技术提供了一种可行的解决途径。首先可在被侵害主机 Victim 所在网络关键位置（如网关）启用 ANFW 嵌入器，主动调制 Victim 所产生

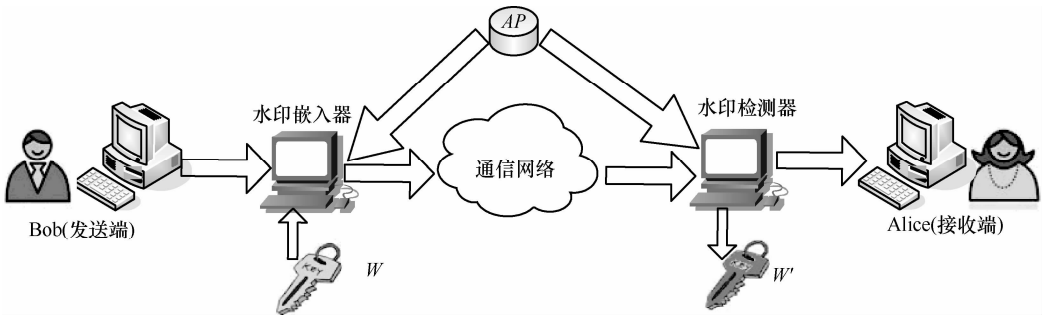


图 1 ANFW 技术通用模型

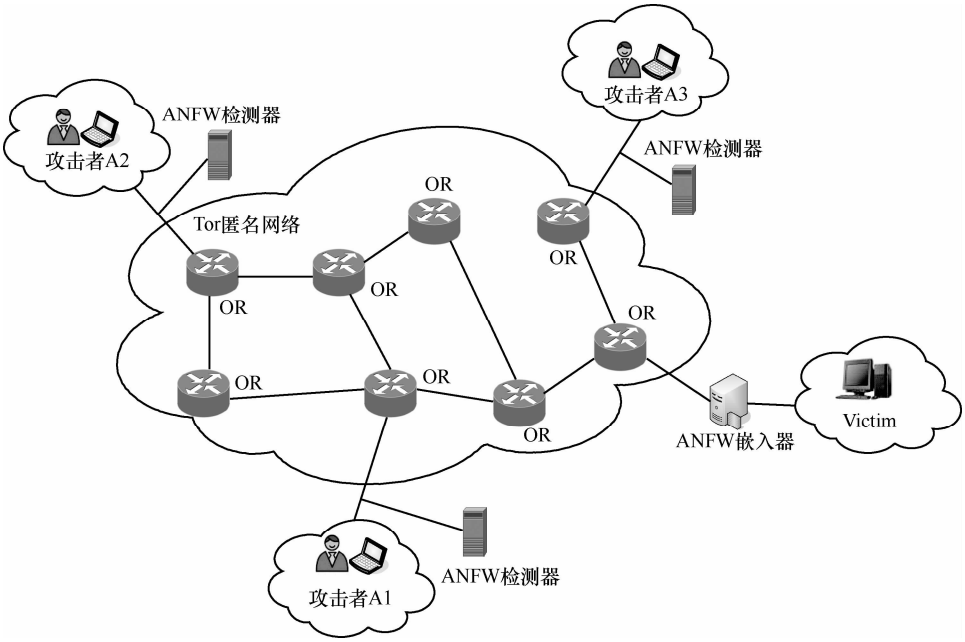


图 2 ANFW 在匿名网络 Tor 中应用示例

的向外的流的特征，以使流携带水印信息 W，该流经过 Tor 匿名通信网络传输后可能会到达网络 A1、A2 或 A3，此时部署在网络 A1、A2 及 A3 关键位置的 ANFW 检测器会对进入本网的流进行水印信息检测和提取，若检测得到的水印信息为 W，则可确定攻击者位置存在于本网络中，为下一步准确找出攻击者精确位置提供依据，以达到对攻击源的定位与追踪。此外，也可将 ANFW 嵌入器、ANFW 检测器作为功能模块嵌入在 OR 中，方便部署与应用。

2.3　面向的主要角色

ANFW 面向的主要角色是指 ANFW 技术在实际应用中所涉及的主要人员，如图 3 所示。本文根据已有研究文献的描述、ANFW 原理及应用领域，从网络安全的角度将 ANFW 面向的主要角色总结为 4 类，分别为：攻击者、普通用户、网络管理员及网络执法者。

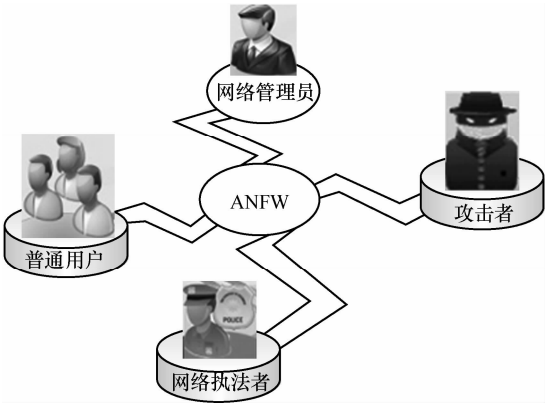


图 3　涉及 ANFW 的主要角色

攻击者可分为 2 类，一类是指恶意和非法使用 ANFW 技术检测、跟踪通信网络中正常用户间通信行为的人员，如在匿名通信系统中，此类攻击者就可以利用 ANFW 技术在收发双方未觉察的情况下，确认和跟踪收发双方的关系，从而破坏匿名通信系统的匿名性，为后续实施其他网络攻击提供可靠信息；另一类是指以故意移除或破坏 ANFW 为目标的人员，如一些违法人员会操纵匿名系统中主机传播色情、谣言等不良信息，甚至进行其他犯罪（赌博、倒卖个人隐私信息等），当网络监管人员利用 ANFW 技术对这些违法主机进行跟踪时，违法人员很可能会利用一些技术手段[22]对潜在的 ANFW 进行移除，以逃避检测和追踪。

普通用户是指在网络中正常合法通信的主机。一方面，他们是 ANFW 技术的保护对象，ANFW 可作为判断这些普通用户是否已变为 stepping stone[19]、僵尸主机[23]等的一种重要技术手段；另一方面，普通用户也可主动利用 ANFW 技术来确定自身所访问网络信息来源的真实性和可靠性。

网络管理员可利用 ANFW 技术确定和追踪所辖子网或子域内存在的网络入侵事件和攻击行为，记录关键信息，形成证据日志，并联合 IPS（intrusion prevention system）、防火墙等系统遏制相关网络攻击行为。同时，也可在多个子网或子域展开合作，共享各自证据日志信息，以构建和还原完整的网络入侵路径[24]，追踪和定位网络攻击真实来源。

网络执法者从网络管理员处调取与网络犯罪行为相关的证据日志，并汇集其他安全系统（如 IPS/IDS、网络信息审计系统等）提供的信息及现实证据，形成完整的证据链，提高网络犯罪案件侦破效率，有效打击和遏制网络犯罪活动。

2.4　主动网络流水印技术分类

对已有 ANFW 方法可以从不同的角度得到不同的分类。如根据提取水印 W 时是否使用流 f_i 初始特征信息（流 f_i 被嵌入水印 W 前的特征信息），可分为非盲水印（NW, non-blind watermarking）和盲水印（BW, blind watermarking）。NW 类方法需要借助于流 f_i 初始特征信息（可由 watermark decoder 预先将 f_i 初始特征信息存放于 AP 中）才能完成水印信息提取，而 BW 类方法则不需要。

本文根据网络流的定义及承载水印 W 的流特征，依托 TCP/IP 网络层次模型，将现有 ANFW 方法分为基于流速率特征[21,28,29]、基于流内分组间隔特征[30~33]、基于流时间时隙分割特征[20,34~37]及基于分组载荷[25~27]等类别，如图 4 所示。

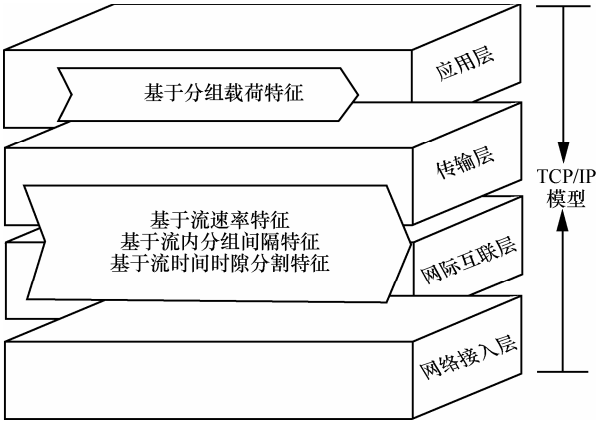


图 4　按 TCP/IP 网络层次模型分类 ANFW

从图 4 中可以看出，当前网络流水印技术的研究多数集中在网际互联层和传输层，这是由于一方面流定义及特征[18]主要涉及此两层，另一方面，在匿名通信和加密流量的环境下，难以在数据分组的应用层载荷中嵌入水印 W，使 ANFW 技术失效，而在网际互联网层和传输层应用 ANFW 技术则不受此限制。

3 典型的主动网络流水印技术

网际互联层和传输层的 ANFW 技术基本都是以网络流的某些与分组内容无关的特征为载体来完成水印 W 的嵌入，且当网络流经过通信网络传输后，W 仍能被恢复。这些被选取的网络流特征，称为水印载体。根据使用不同的水印载体，网际互联层和传输层的 ANFW 技术主要包括基于流速率特征、基于流内分组间隔特征及基于流时间时隙分割特征等。

3.1 基于流速率特征

此类方法核心思想是选取整个流持续时间内的不同时间段，在水印信息 W 的作用下，通过一定的方法略微调整这些时间段内的网络流速率，以表示水印信息位 w_i（1 或 0），从而达到在网络流中嵌入水印 W 的目的。

Yu 等[21]将 CDMA 无线通信系统使用的 DSSS（direct sequence spread spectrum）机制引入到主动网络流水印中，如图 5 所示，该方法称为 DSSS-W。

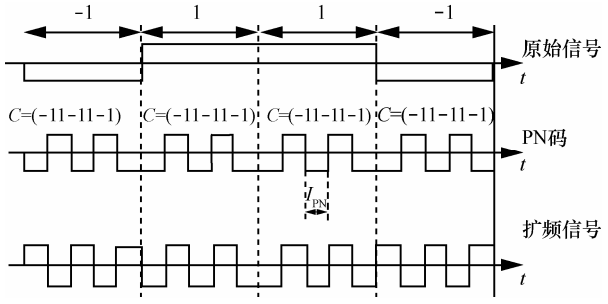


图 5 DSSS 原理

DSSS-W 在发送端利用式(4)将原始水印信号 W 扩频为 W^D，其中，$C=(c_1,\cdots,c_m)$为 PN 码，$w_i, c_j \in \{-1,1\}$（此处用−1 代表水印信息位'0'，下同）。

$$W^D = W \times C = \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} \times \begin{pmatrix} c_1 & \cdots & c_n \end{pmatrix} = \begin{pmatrix} w_1^D \\ \vdots \\ w_n^D \end{pmatrix} \quad (4)$$

w_i^D 为原始水印为 w_i 扩频后对应的水印信号，且 $w_i^D=(w_ic_1 \ \cdots \ w_ic_m)$，$w_ic_j$ 持续时间为 I_{PN}。

接着利用式(5)在 I_{PN} 时间内对流速率进行略微改变，连续应用式(5) m 次即可完成水印位 w_i 的嵌入，剩余水印信息位的嵌入方法相同，从而可完成整个水印 W 的嵌入。

$$T_x = w_i c_j A + S \quad (5)$$

其中，S 为流原始平均速率，T_x 为水印 W 嵌入后的流速率，A（A>0）为调节幅度。

接收端所接收的流速率为 R_x，如式(6)所示。

$$R_x = w_i c_j A + S + z \quad (6)$$

其中，z 为通信网络在流传输过程中产生的噪声。为恢复水印 W，先利用高通滤波器对 R_x 滤除直流分量 S 后得到式(7)中的 R_x'，接着，R_x' 与 PN 码相乘得到 T_x'，如式(8)，并利用低通滤波器滤除噪声 zC。最后应用简单的决策规则恢复出每一个 w_i，从而还原出整个原始水印 W。

$$R_x' \approx w_i c_j A + z \quad (7)$$

$$T_x' = w_i c_j AC + zC \quad (8)$$

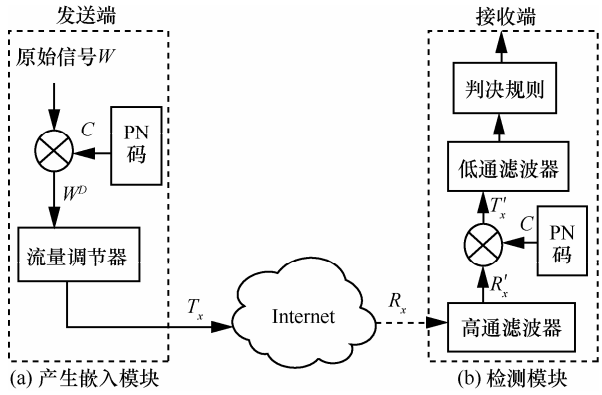


图 6 DSSS 水印产生嵌入与检测模块

图 6 给出了 DSSS-W 方法的整体过程，类似的方法还有文献[28,29]等。

可以看出，此类方法简单易用，例如只需要在 I_{PN} 内（I_{PN} 的值必须合理设置）根据 w_i^D=−1 或 w_i^D=1 使发送端的流 f_i 暂停发送或继续发送即可完成 W^D 在流 f_i 中的嵌入；其次，具有同时并行追踪多个流的能力，对水印 W 可使用一组不同且相关性较小的 PN 码使之扩展为一组不同的 W^D，将这些 W^D 赋予多个不同的流，从而接收端可根据不同 W^D 很容易区分出不同的流。

但此类方法也存在一些明显缺点，只适用于跟踪速率较大、持续时间较长的目标流，目标流

速率较大才能确保嵌入水印位时调节流速率的幅度对流平均速率没有太大影响，以保证所嵌入水印位的隐蔽性，目标流持续时间长才能保证将 W^D 的所有信息位嵌入进目标流中；与后续方法相比，该类方法在流中所能嵌入的水印信息位个数较少，即可嵌入的水印信息 W 的容量 l 较小，这是由于采用 DSSS 原理将一位原始水印 w_i 扩频为 m 位的 w_i^D 才嵌入进流中，从而导致整个流只能携带较少的水印信息位数；对数据分组延迟、抖动、网络噪音流量等的抗干扰能力较弱，即顽健性不强，由于此类方法是以调整和检测流的速率特征来嵌入和恢复水印信息位的，而这些客观因素极易导致流速率特征发生明显变化，使流携带水印信息难以恢复，最终导致此类方法失效。此外，由于在调整多比特水印信息位时采用同一 PN 码，其所标记的流会呈现自相似性，因此 DSSS-W 类方法也容易受到 MSAC（mean-square autocorrelation）攻击[38]。

3.2　基于流内分组间隔特征

为使 ANFW 适用于较短的网络应用流，提高 ANFW 在流中嵌入水印信息 W 的容量，该类方法选取流内分组间隔时间 IPD（inter-packet delay）作为水印载体，通过略微调整多个 IPD 或 IPD 均值大小，来嵌入水印信息位 w_i，实现流内携带水印 W 的目的。

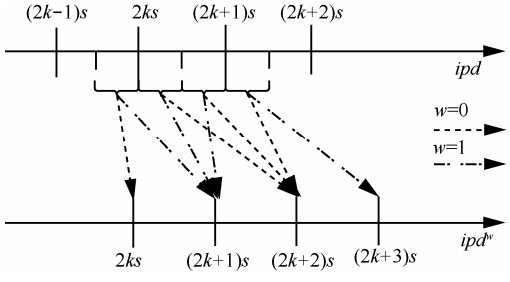


图 7　水印位 w 嵌入前后 ipd 与 ipd^w 的对应关系

Wang 等[30]提出了基于 IPD 的 ANFW 方法 WBIPD(watermark based on IPD)。该方法随机选取发送端流内 2 个数据分组 P_i 和 P_j，计算其 $ipd=t_i-t_j$，t_i 与 t_j 分别为 P_i 和 P_j 到达或离开网络中某节点的时刻，利用式(9)和式(10)改变 ipd 的值为 ipd^w，如图 7 所示，从而完成水印 W 嵌入过程。

$$ipd^w = EM\left(ipd,W,s\right)=\left[q\left(ipd+s/2,s\right)+\Delta\right]s \quad (9)$$

$$\Delta=\left(w_i-\left(q\left(ipd+s/2,s\right)\bmod 2\right)+2\right)\bmod 2 \quad (10)$$

在接收端利用式(11)进行水印解码。

$$DE\left(ipd^w,s\right)=q\left(ipd^w,s\right)\bmod 2 \quad (11)$$

其中，s 为量化步长，函数 $q(x,y)$=round(x, y)表示取与 x 最近的整数。

为了提高抗时间干扰攻击的能力，可使用式(12)中多个数据分组对的 ipd 平均值 ipd_{avg} 来代替式(9)中单个的 ipd，如图 8 所示，m 为所选择的数据分组对数目。

$$ipd_{\text{avg}}=\frac{1}{m}\sum_{k=1}^{m}ipd_k \quad (12)$$

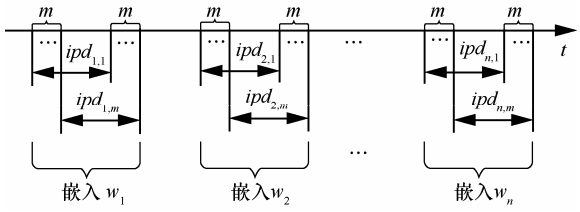


图 8　将 n bit 水印位嵌入 n 个不同 ipd_{avg}

从上述过程来看，WBIPD 巧妙地调整分组间 IPD 来嵌入水印信息位，与 DSSS-W 相比，不仅对流的操作更为细粒度化，使 WBIPD 能应用于较短的流，而且在流中可嵌入更多的水印信息位，能显著增大流携带水印信息 W 的容量。但由于在计算 ipd_{avg} 时需借用缓冲区来暂存流的若干数据分组，会明显增加数据分组的延迟，这使该方法难以跟踪实时性较强的流。

针对 WBIPD 的缺陷，Wang 等[31]在后续研究中以追踪实时匿名 VOIP 电话流量为研究对象，提出一种优于 WBIPD 的 ANFW 方法，该方法先依据一定的概率从流的 n 个数据分组中随机选取 $2r$ 个数据分组 $\{P_1,\cdots, P_{2r}\}$，并与该流的其他数据分组 $\{P_{1+d},\cdots,P_{2r+d}\}$ 构成 $2r$ 个分组对即$<P_1,P_{1+d}>,\cdots,<P_{2r},P_{2r+d}>$，$d$（$d>0$）为增量。

其次，计算每个分组对的 ipd 值，并将此 $2r$ 个 ipd 值随机分为 2 组 IPD^1 和 IPD^2，且$|IPD^1|=|IPD^2|=r$（r 为冗余度，$0<r<(n-d)/2$）。

最后，通过式(13)和式(14)计算 $\overline{Y_{r,d}}$，其中，$ipd_k^1\in IPD^1$，$ipd_k^2\in IPD^2$。

$$Y_{r,d}=\left(ipd_k^1-ipd_k^2\right)\big/2,\ k=1,2,\ \cdots,r \quad (13)$$

$$\overline{Y_{r,d}}=\frac{1}{r}\sum_{k=1}^{r}Y_{r,d} \quad (14)$$

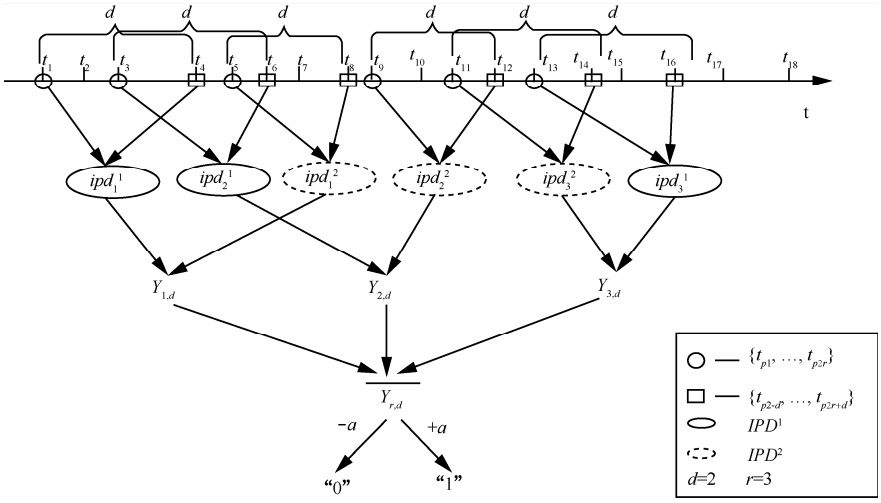


图 9　文献[31]中方法简单示例

由于 $\overline{Y_{r,d}}$ 服从对称中心为 0 的独立同分布，只要对 $\overline{Y_{r,d}}$ 增加或减少增量 a（a>0）就可以使得 $\overline{Y_{r,d}}$ 所服从独立同分布的对称中心由 0 变为−a 或 a，可借用此变化来代表水印位“0”或“1”，从而完成水印 W 的嵌入。图 9 是该方法过程的一个简单示例，其中，r=3，d=3。该方法还借助 RTAI 库[39]，对实时 P2P 匿名 VoIP 电话服务进行了追踪实验，取得了较好效果。此外，Park[20]等也在此方法的提示下也给出了类似的自适应网络流水印算法。

与前述 2 种方法不同，一些研究者采用了非盲水印的思路来操作 IPD[19,33,40]，其中典型代表就是 Houmansadr 等[19]设计的 RAINBOW 方法，原理如图 10 所示。RAINBOW 最大特点在于检测水印 W 时需要参考流的原始 IPD 值，其过程分为 4 步。

水印嵌入器：

1) 计算流内所有 IPD 值 ipd_i^u（即流的原始 IPD 值），并存储在 IPD 数据库中。

2) 通过式(15)及式(16)增加或减少每个 ipd_i^u 来表示水印 W 的每个水印位 w_i 嵌入，如图 11 所示。

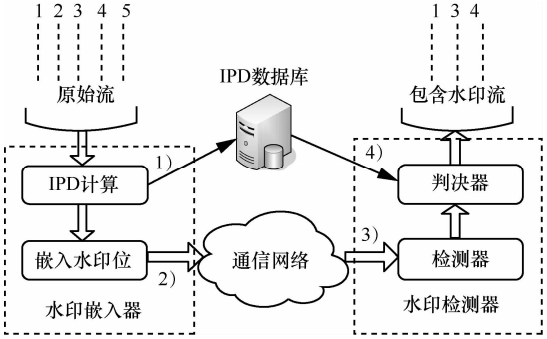


图 10　RAINBOW 模型

$$ipd_i^w = ipd_i^u + e_i a\ ,\ a>0 \tag{15}$$

$$e_i = \begin{cases} +1\ ,\ w_i = 1 \\ -1\ ,\ w_i = 0 \end{cases} \tag{16}$$

水印检测器：

3) 计算每个捕获流内的所有 IPD 值 ipd_i^r，并求 Y=$\{y_i\}$，其中 y_i=ipd_i^r−ipd_i^u。

4) 使用式(17)计算 Y 与 E 的内积值 $N(Y,E)$，其中，E=$\{e_i a\}$。

$$N(Y,E) = \frac{\langle Y,E\rangle}{\|Y\| \bullet \|E\|} = \frac{\sum_{i=1}^{n} y_i e_i a}{\sqrt{\left(\sum_{i=1}^{n} y_i\right)\left(\sum_{i=1}^{n} e_i a\right)}} \tag{17}$$

若 $N(Y,E)$小于预先设置的阈值时，则判断当前流包含水印 W，否则与 IPD 数据库中其他流的原始 IPD 作比较，重复步骤 3)和步骤 4)。

可以看出，RAINBOW 只调整一个 IPD 即可在流中嵌入 w_i，水印信息容量完全取决于流的 IPD 数目，其实验结果表明对于较长的流，水印信息容量可达上千比特；对流的 IPD 调节幅度也较小，不易被攻击者察觉，隐蔽性较好；借助数据库保存的原始流 IPD 改善 decoder 端提取水印信息位的准确性；但数据库的使用也使得 RAINBOW 在跟踪流数较多时空间复杂度急剧增大；在流关联时，从待确定流中检测出的水印信息需要逐个与数据库中多条已存在流的 IPD 记录进行对比，明显增加了时间开销，难以应对实时性强的网络应用流，降低了该方法的实用性。

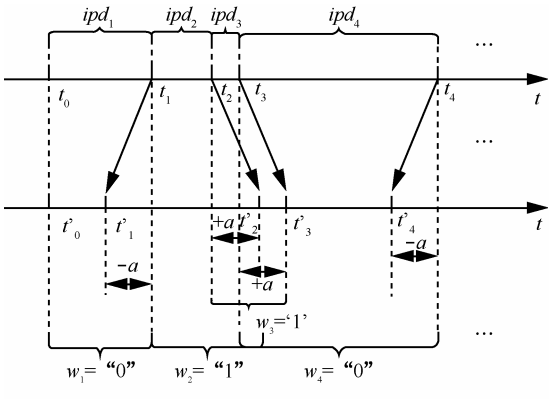


图 11　RAINBOW 嵌入水印位 w_i 的过程

3.3　基于流时间时隙分割特征

为有效应对在匿名通信系统中通过添加哑数据分组（chaff packet）、分组重组（repacketization）、分组丢弃及多流混合等方式破坏流水印，提高 ANFW 技术对通信网络噪声流量的顽健性，该类方法在整个流持续时间内随机选取一个时间段，并将其分割为若干相等的时间间隔，称为时隙（interval），通过改变落在每个时隙内数据分组发送时刻或调整时隙内的数据分组数量来嵌入水印 W。

Wang 等[34]提出了时隙质心水印机制 ICBW（interval centroid based watermarking），如图 12 所示。ICBW 首先从流起始时刻的随机偏移 o(o>0)处开始的一个时间段 T_d，分割为 $2n$ 个长度为 T 的时隙 I_i(i=1,2,⋯, $2n$)。

其次，利用式(18)计算时隙 I_i 的质心，其中 n_i 为 I_i 内出的现数据分组个数，Δt_{i_j} 为 I_i 内第 j 个数据分组距离 I_i 起始位置的时间偏移，服从均匀分布。

$$\mathrm{Cent}(I_i)=\frac{1}{n_i}\sum_{j=0}^{n_i-1}\Delta t_{i_j} \tag{18}$$

再次，将 $2n$ 个 I_i 随机分为 A 和 B 2 组，且 $|A|=|B|=n$。以概率 $1/|W|$从 A、B 中各取 r 个时隙，并按式(19)及式(20)计算此 r 个时隙的质心 A_i 和 B_i。其中，$I^A_{i,j}$ 和 $I^B_{i,j}$ 分别代表嵌入 w_i 时从 A 组和 B 组所选取的 r 个时隙的第 j 个，$N^A_{i,j}$ 和 $N^B_{i,j}$ 为时隙 $I^A_{i,j}$ 和 $I^B_{i,j}$ 含有的数据分组个数。

$$A_i=\frac{\sum_{j=0}^{r-1}\left[N^A_{i,j}\,\mathrm{Cent}\left(I^A_{i,j}\right)\right]}{\sum_{j=0}^{r-1}N^A_{i,j}} \tag{19}$$

$$B_i=\frac{\sum_{j=0}^{r-1}\left[N^B_{i,j}\,\mathrm{Cent}\left(I^B_{i,j}\right)\right]}{\sum_{j=0}^{r-1}N^B_{i,j}} \tag{20}$$

最后，由于 $Y_i=A_i-B_i$ 服从对称轴为 0 的均匀分布，因此，可通过给 A_i 或 B_i 增加 a（$0<a<T$）使 Y_i 所服从均匀分布的对称轴变为 $a/2$ 或 $-a/2$，以此变化来表示水印信息位 w_i，从而完成 w_i 在流中的嵌入。

ICBW 利用均匀分布原理通过调整 2 组时隙内若干数据分组的时间偏移来嵌入一个水印信息位，即使受到流混合、流分割、流合并等因素的干扰，但只要时隙内数据分组数据足够多，仍能通过时隙组质心来减少或消除这些因素带来的影响，保证水印信息位的正确恢复，具有较好的顽健性，实验结果也证明了这点；其水印信息容量比 DSSS-W 要大，

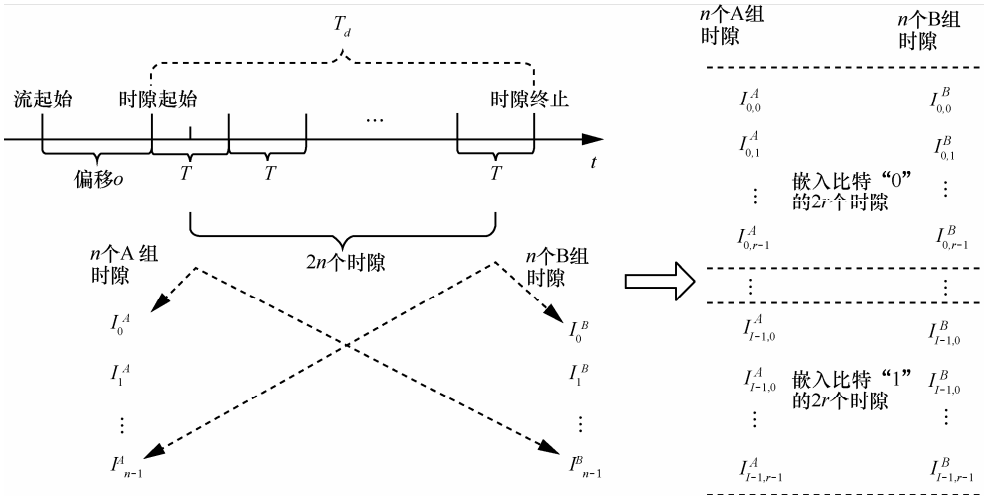


图 12　ICBW 水印技术原理

与 WBIPD 相当，但小于 RAINBOW 方法；然而，ICBW 方法易遭受 MFA(multi-flow attack)攻击[41]，即将经 ICBW 方法处理过的多条流进行对比时，可以造成所嵌入的水印信息 W 的暴露。

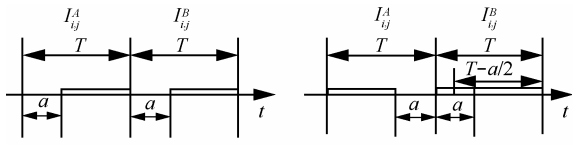
针对 ICBW 的缺点，Wang 等[35]提出了一种可抵抗 MFA 攻击的双时隙质心水印机制 DICBW (double interval centroid based watermark)，如图 13 所示。DICBW 与 ICBW 区别在于：

1) 计算 A_i 和 B_i 时，DICBW 所使用的时隙 $I^A_{i,j}$ 和 $I^B_{i,j}$ 必须为相邻时隙而非随机选取的时隙。

2) 使用式(21)计算时隙 B_i。其中，$\overline{\Delta t^B_{t,j.k}} = T - \Delta t^B_{t,j.k}$，$\Delta t^B_{t,j.k}$ 为 B 组时隙 $I^B_{i,j}$ 内第 k 个数据分组距离时隙 $I^B_{i,j}$ 起始位置的时间偏移量，$N^B_{i,j}$ 为时隙 $I^B_{i,j}$ 内数据分组个数。

$$B_i = \frac{\sum_{j=0}^{r-1}\sum_{k=1}^{N^B_{i,j}} \overline{\Delta t^B_{t,j.k}}}{\sum_{j=0}^{r-1} N^B_{i,j}} \tag{21}$$

水印信息位 w_i 的嵌入过程与 ICBW 方法类似。实验结果表明，与 ICBW 相比，DICBW 在抵抗 MFA 攻击和时间扰动，应对流合并、流分割等流变换等方面有更好的效果。



(a) 嵌入水印比特 “+1” (b)嵌入水印比特 “0”

图 13 DICBW 嵌入水印位过程

为同时应对 MSAC 和 MFA 攻击，Luo 等[36]将 ICBW 与 DSSS-W 结合，提出了 ICBSSW(interval centroid based spread spectrum watermarking scheme)方法，此方法先使用 PN 码将水印信息位 w_i 扩频为 w_i^D，与 DSSS-W 不同的是，w_i^D 为的嵌入不是通过调制流速率实现的，而是使用 ICBW 方法中的调整时隙质心差实现的。ICBSSW 综合了 ICBW 与 DSSS-W 的优点，不仅能在同一网络节点并行跟踪多个流，而且由于采用不同的 PN 码来标记不同的流，使得这些流即使遭受 MSAC 和 MFA 攻击的情况下也很难呈现出所携带水印信息的规律，具有较好的隐藏性，同时在应对流混合、流分割、流合并等方面也具有较好的效果。但 ICBSSW 计算过程相对于 ICBW 和 DSSS-W 要复杂一些，时空开销也要多一些。与 ICBSSW 类似的方法还有文献[32]。

与 ICBW，ICBSSW，DICBW 不同，Pyun 等[37]提出的 IBW 水印技术是通过改变相邻时隙对 I_i 和 I_{i+1} 中数据分组数目来嵌入水印信息位 w_i。IBW 有 load 和 clear 2 种基本操作。load 操作是将时隙 I_{i-1} 内的所有数据分组延迟到时隙 I_i 内，而 clear 操作是将时隙 I_i 内的所有数据分组延迟到 I_{i+1} 内。当 w_i=0 时，对时隙 I_i 内的数据分组进行 load 操作，同时对时隙 I_{i+1} 数据分组进行 clear 操作；相反，当 w_i=1 时，则对 I_i 和进行 clear 操作，同时在 I_{i+1} 进行 load 操作。为避免嵌入多个水印信息位时多个时隙对间产生冲突，应保证 2 个连续的时隙隔对之间至少有一个时隙，以起到隔离作用。虽然 Pyun 等从理论分析和实验两方面证明 IBW 方法对时间扰动和分组重组干扰有较好的抵抗性，但由于该方法通过改变时隙内数据分组数目来嵌入水印位信息，因此难以处理添加哑数据分组的干扰，而且也容易遭受 MFA 攻击。

此外，SWIRL (scalable watermark that is invisible and resilient to packet losses)[42]呈现采用了另一种时隙特征变换的流水印方法。该方法将流时间分成若干时隙对，每一时隙对中的 2 个时隙按时间先后顺序分别命名为 base interval 和 mark interval。首先对 base interval 利用式(18)计算其时隙质心 C_{base}，并利用量化公式将 C_{base} 转变为一个服从均匀分布的量 v。其次，将 mark interval 均匀分割为 h 个子间隔，每个子间隔又均分为 m 个 slot，并依据 h 个子间隔与 v 的排列关系从每个子间隔中选出一个 slot。最后，将每个子间隔中未被选中 slot 内的数据分组通过延迟操作改变到已选中的 slot 内，从而完成水印信息位的嵌入。从实验结果来看，该方法在大规模流量的情况下可以应对分组丢失、网络抖动的干扰，能有效抵御 MFA 攻击、Tor 拥塞攻击[43]等，但攻击者可通过注入特定的流让 SWIRL 来嵌入水印信息，并将此时的流与其原先的时间模式进行对比即可了解 SWIRL 嵌入水印信息的情况[44]。

除使用上述 3 类流时间特征外，也有研究者提出了基于流内分组乱序特征的 ANFW 方法 PROFW(packet reordering based flow watermarking)[45]。分组序是指数据分组报头中的序号信息，如 TCP 中的序号、IPSec 数据分组的认证头

(authentication header)和封装安全载荷(encapsulating security payload)中的序号等，在自然通信状态下不可避免会出现流内数据分组发送与到达顺序不一致的分组乱序现象。PROFW 首先将水印 W 看作为 k 个数的排列 A，让 A 中的每种排列与不同的格雷码 CW_i 一一对应，且这些 CW_i 间还必须能满足一定的汉明距离关系。然后，借用乱序密度 RD(reorder density)求出不偏离正常乱序行为下各 CW_i 出现的概率 P_i。最后，选择函数以 P_i 从流中选择出数据分组并对其分组序根据 CW_i 进行改变，以完成嵌入水印 W。从其原理来看，虽然该方法能够保证流中所隐藏水印信息的隐蔽性，但只对包含大量数据分组的流才能取得较大的水印容量，不适用于普通的流，而且很显然在应对哑数据分组、分组丢失、重组分组等因素干扰时顽健性较差。

3.4　典型主动网络流水印方法综合对比

前面着重概述了网际互联层和传输层多种代表性的 ANFW 方法的核心思想及各自的优缺点。为了更直观地理解这些主动网络流水印方法的特点，在研究和分析文献中各自方法实验测试结果的基础上，此处将采用隐蔽性、水印容量、嵌入水印时的时空开销、提取水印时的难易程度、盲/非盲性、顽健性和实用性等评价指标从总体上对这些典型 ANFW 方法进行集中对比，如表 1 所示。

3.5　主动网络流水印技术所面临威胁

AFNW 技术实质是通过调整流的特征来隐藏水印信息，这些水印信息不仅在通信网络中遭受各种因素的干扰而变形，而且也会成为攻击者蓄意探测与移除的目标，因此 AFNW 技术所面临的安全威胁主要来自 2 个方面。

1) 通信网络干扰因素

被嵌入水印的流在经过通信网络传输到达目的端的过程中不可避免地会遭受一些因素干扰，减弱水印效果。如延迟抖动[46,47]、网络拥塞[48]、分组变换(分组分割、分组重组、分组合并、分组丢失等)[49]，这些干扰因素一方面来自于通信网络本身的自然特性[1]，另一方面很可能是攻击者主观故意产生[50]。

2) 水印信息蓄意探测及移除

是指攻击者在不知道任何 ANFW 技术的细节下，通过一定的手段尝试探测或识别网络流中存在的水印信息，进而破坏或移除这些水印信息，以逃避追踪审查，如针对 ICBW 和 IBW 水印机制的探测[22,51]、针对 DSSS 水印机制的探测[38,52]以及同时针对多种水印机制的探测[41,53]等。表 2 总结了当前水印机制遭受的各种攻击及防范措施。

4　未来研究方向展望

从前述内容可知，主动网络流水印技术已引起国内外网络安全研究人员的极大关注，已逐渐成为网络安全领域一项重要的研究内容。尽管当前主动网络流水印技术具备应对加密流量、匿名通信环境、隐蔽性好等优势，但从其原理及表 1、表 2 来看，主动网络水印技术仍然存在潜在问题尚未很好解决，本文认为今后可从如下方面展开科研工作。

4.1　提高和改善 AFNW 技术性能

1) 设计更为健壮的同步机制，以降低水印收发双方在较大网络噪声干扰下编解码水印信息错位的概率。一种值得考虑的方法是借鉴通信中同步原理的思想[59]来改善现有 ANFW 方法的同步机制，

表 1　　**典型 ANFW 方法特点比较**

方法	隐蔽性	水印容量	时空开销	提取难度	NW/BW	顽健性	实用性
DSSS-W[21]	★★★☆☆☆	★★☆☆☆☆	★★☆☆☆☆	★★☆☆☆☆	BW	★★☆☆☆☆	★★★☆☆☆
WBIPD[30]	★★★☆☆☆	★★★☆☆☆	★★★★☆☆	★★★☆☆☆	BW	★★★☆☆☆	★★★★★☆
Ref.[31]	★★★★★★	★★★☆☆☆	★★★☆☆☆	★★★★☆☆	BW	★★★★☆☆	★★★★☆☆
RAINBOW[19]	★★★★★☆	★★★★★★	★★★★★★	★☆☆☆☆☆	NW	★★☆☆☆☆	★☆☆☆☆☆
ICBW[34]	★★★★☆☆	★★★★☆☆	★★★☆☆☆	★★★★☆☆	BW	★★★★★☆	★★★★★☆
DICBW[35]	★★★★★☆	★★★☆☆☆	★★★★☆☆	★★★★★☆	BW	★★★★★★	★★★★☆☆
ICBSSW[36]	★★★★★☆	★★☆☆☆☆	★★★★★☆	★★★★☆☆	BW	★★★★★★	★★★★☆☆
IBW[37]	★★☆☆☆☆	★★★☆☆☆	★★★★★☆	★★★☆☆☆	BW	★★★☆☆☆	★★★☆☆☆
SWIRL[42]	★★☆☆☆☆	★★★☆☆☆	★★★★★★	★★★★★☆	BW	★★★★☆☆	★★☆☆☆☆
PROFW[45]	★★★☆☆☆	★★☆☆☆☆	★★★★☆☆	★★★☆☆☆	BW	★★☆☆☆☆	★☆☆☆☆☆

表 2 现有针对 AFNW 攻击及防范状况

安全问题分类	攻击名称	影响的 ANFW	防范措施
I 型安全问题	分组延迟	ALL	N/A
	分组变换	ALL	参见文献[54]
II 型安全问题	ESWD 探测[51]	基于分组间隔特征	N/A
	FQZQ 探测[22]		
	SWDM 探测[55]		
	MSAC 攻击[38]	基于 DSSS-W[21]方法及其改进	参见文献[56]
	LZPL 探测[52]		N/A
	MFA 攻击[41]	ICBW[34] & IBW[37] & Multiple Offsets/Positions[41]	参见文献[57, 58]
	BACKLIT 攻击[53]	DSSS-W[21]	N/A
	LH 攻击[44]	RAINBOW[19] & SWIRL[42]	参见文献[44]

注：ALL：基于分组间隔特征、流速率和流时隙分割的 ANFW; N/A: 防范措施目前暂不存在。

例如可使用曼彻斯特码来编码水印信息，并通过改变相邻流时间时隙内数据分组数量差值来模拟曼彻斯特编码中的跳变，以使调制后的流整体上具有自同步性或者借鉴群同步思想[59]，将水印信息分割成组，并在每组头部加入额外同步码（如巴克码）后按组进行编码发送，以便通过每组的同步性来提高流整体的同步性。

2) 改善并行追踪多流及抵抗分流的能力。现有 ANFW 方法在兼顾隐蔽性和顽健性的前提下，对流内 IPD 的改变幅度不大，被水印标记的多条流不仅在经过同一网络节点（如 OR、跳板主机）会发生相互干扰，而且在网络传输过程中也可能面临先分解再合并问题[60]，造成水印信息失效。因此，如何提升 ANFW 方案应对此类问题的能力是推进 ANFW 实用化所亟待解决的问题。

3) 提升 ANFW 对流的自适应能力。不同网络应用（如 Web[61]、视频[62]、VoIP[63]、游戏[64]等）所产生的流量时间特征差异较大，需要研究针对不同类型流能够自动选择合适水印信息编码方式及相关参数的流水印技术，以弥补现有 ANFW 方案仅适用于单一类型流的不足，取得更好的数据流关联效果。

4) 增强 ANFW 在网络延迟、抖动、分组重传等因素干扰下的顽健性。即使被 ANFW 标记流的多个 IPD 在该流传输过程中受这些因素干扰而发生改变，接收方仍能以较大概率正确恢复出水印信息，使这些干扰因素对流内水印信息的影响控制在可接受范围。可从增加水印信息位对应的 IPD 冗余数、改善水印信息嵌入的方式（如借鉴数字喷泉编码[65]）等角度来综合考虑此问题。

5) 提高水印信息嵌入与检测过程的实时性。现有的 ANFW 方案着重关注水印信息隐蔽性与顽健性，很少顾及时空计算复杂度。但在实际应用中，实时性是必须的，特别是在资源有限条件下追踪实时性较强的流时，更需要低时空复杂度的 ANFW 方法。对于此问题，一方面需要对 ANFW 算法本身进行改进优化，另一方面也可借鉴文献[66]方法，考虑将 ANFW 算法硬件化或固件化。

6) 探索新型 ANFW 机制。针对攻击者能利用概率统计方法对现有 ANFW 方案产生的流时间水印信息进行干扰、探测及破坏，除增强已有 ANFW 方案的隐蔽性外，积极开发新型 ANFW 机制也是解决问题途径之一。ANFW 本质是在网络流特征中秘密隐藏信息，因此可考虑借鉴一些较新颖的信息隐藏[67,68]及隐蔽通信技术[69,70]思想应用在相关网络流特征上，以产生新的 ANFW 方案。

4.2 加深 ANFW 相关理论研究

1) 水印容量估算模型。水印容量代表了 ANFW 利用流特征来携带信息的能力，是衡量 ANFW 性能重要指标之一。目前多数 ANFW 方案仅通过人工估计或简单试验来给出水印容量，准确性较差，也不利于充分发掘 ANFW 方案的潜力。因此，针对不同水印机制应研究如何建立流数据分组数目、流持续时间、自身水印编码方式等多种因素综合的数学模型，以较为准确地估测自身水印容量。

2) 同类水印方法综合评价模型。探索该模型可为同类 ANFW 方案间统一的比较与评价提供严格、有效的理论评判依据，也为 ANFW 的改善与

革新提供有利参考。一种思路是可先对表 1 所列出的若干评价指标有效量化，然后再借鉴现有综合评价方法（如主成分分析法、数据分组络分析法、模糊评价法）对量化的指标进行有机融合以生成综合评价模型。

3) 水印机制安全等级模型。借鉴数字水印安全等级评价方法[71]，研究评估水印机制安全级别模型，以评估各 ANFW 机制安全级别，并建立类似于 TCSEC[72]的安全等级策略，指导用户针对不同的网络应用需求定制不同安全级别的 ANFW 方案。

4.3 推动 ANFW 部署与应用

1) ANFW 技术与现有相关网络系统整合。研究如何将 ANFW 技术与 IDS/IPS、防火墙等安全系统整合，以弥补现有网络安全系统在网络入侵追踪（如可疑加密流量追踪）能力方面的不足；研究基于普通客户端的流水印软件或插件，可借鉴文献[73]的方法开发基于浏览器的 ANFW 插件，与布置在服务器端的 ANFW 模块相配合，为用户访问 Web 服务过程提供一种轻量级的安全机制。研究 ANFW 模块在自治域内关键链路上的部署及与其他追踪技术[74,75]协作问题，以高效追踪网络攻击流，达到准确构建入侵路径、定位入侵源等目的。

2) 拓展 ANFW 的应用范围。随着 Internet 发展呈多元化趋势，探索 ANFW 技术如何保障新兴 Internet 服务与应用网络通信安全也是需要关注的研究领域。如研究 ANFW 技术如何发现和检测云环境下共驻同一物理平台的多个虚拟机之间通过网络流量来泄露隐私信息的问题[76]；设计和测试能够适用于移动互联网[77,78]环境的 AFNW 方法；可借助未来网络试验床[79]及仿真工具[80]，研究与开发面向未来网络体系结构及通信模式的 ANFW 方案。

5 结束语

主动网络流水印技术是数字水印思想与主动网络流量整形及分析相结合的产物。其在匿名通信关系确认、跳板主机检测、僵尸网络主控机追踪等网络安全领域的应用，体现出较大的实用价值，已成为具有现实意义的研究方向。现有的 ANFW 印技术研究已在流水印产生原理、流水印载体选择（即流特征选择）、流水印嵌入与检测等方面取得了一定进展，初步实现了主动网络水印技术的基本目的，但在一些关键问题上，现有进展仍然不足，尤其在面对各种复杂网络干扰、蓄意检测攻击下提高水印技术的顽健性、隐蔽性等方面，需要更为深入的研究和探索。随着主动网络流水印技术不断成熟和完善，其在今后的网络安全领域中必将起到更加积极、广泛的作用。

参考文献：

[1] YLONEN T. The secure shell (SSH) protocol architecture[EB/OL]. http://www.ietf.org/rfc/rfc4251.txt, 2006.

[2] IPSEC WORKING GROUP. IP security protocol (IPSec) [EB/OL]. http://datatracker.ietf.org/wg/ipsec/, 1995.

[3] ZHANG Y, PAXSON V. Detecting stepping stones[A]. Proc of the 9th USENIX Security Symposium[C]. Denver, Colorado, 2000. 171-184.

[4] BLUM A, SONG D, VENKATARAMAN S. Detection of interactive stepping stones: algorithms and confidence bounds[A]. Proc of the 7th International Symposium on Recent Advances in Intrusion Detection[C]. Sophia Antipolis, France, 2004. 258-277.

[5] HE T, TONG L. Detecting encrypted stepping stone connections[J]. IEEE Transactions on Signal Processing, 2007, 55(4): 1612-1623.

[6] ROBERT S, JIE C, PING J, *et al*. A survey of research in stepping-stone detection[J]. International Journal of Electronic Commerce Studies, 2011, 2(2):103-126.

[7] DINGLEDINE R, MATHEWSON N, SYVERSON P. Tor: the second-generation onion router[A]. Proc of the 13th USENIX Security Symposium[C]. San Diego, USA, 2004. 303-320.

[8] REITER M K, RUBIN A D. Anonymous Web transactions with crowds[J]. Communications of the ACM, 1999, 42(2): 32-38.

[9] FREEDMAN M J, MORRIS R. Tarzan: a peer-to-peer anonymizing network layer[A]. Proc of the 9th ACM Conference on Computer and Communications Security[C]. Washington DC, USA, 2002. 193-206.

[10] PASSERINI E, PALEARI R, MARTIGNONI L, *et al*. FluXOR: detecting and monitoring fast-flux service networks[A]. Proc. of the 5th Detection of Intrusions and Malware, and Vulnerability Assessment[C]. Paris, France, 2008. 186-206.

[11] 江健，诸葛建伟，段海新等.僵尸网络机理与防御技术[J].软件学报，2012, 23(1):82-96.
JIANG J , ZHUGE J W, DUAN H X, *et al*. Research on botnet mechanisms and defenses[J]. Journal of Software, 2012,23(1):82-96.

[12] HOLZ T, GORECKI C, RIECK K, *et al*. Measuring and detecting fast-flux service networks[A]. Proc of the 15th Network and Distributed System Security Symposium (NDSS'08)[C]. San Diego, USA, 2008.

[13] YODA K, ETOH H. Finding a connection chain for tracing intruders[A]. Proc of the 6th European Symposium on Research in Computer Security[C]. Toulouse, France, 2000.191-205.

[14] ZHU Y, FU X W, GRAHAM B, *et al*. On flow correlation attacks and countermeasures in mix networks[A]. Proc of 2004 Privacy Enhancing Technologies(PET'04) [C]. Toronto, Canada, 2004. 207-225.

[15] DONOHO D L, FLESIA A G, SHANKAR U, *et al*. Multiscale stepping-stone detection: detecting pairs of jittered interactive streams by exploiting maximum tolerable delay[A]. Proc of the 5th International Symposium on Recent Advances in Intrusion Detection[C]. Zurich,

Switzerland, 2002. 17-35.

[16] WANG X, REEVES D , WU S F. Inter-packet delay based correlation for tracing encrypted connections through stepping stones[A]. Proc of the 7th European Symposium on Research in Computer Security[C]. Zurich, Switzerland, 2002 . 244-263.

[17] COX J, MILLER L , BLOOM J , *et al*. Digital watermarking[M]. San Francisco:Morgan-Kaufmann, 2001.

[18] 程光，龚俭. 互联网流测量[M]. 南京:东南大学出版社，2008.
CHENG G, GONG J. Internet Flow Measurement[M]. Nanjing: Southeast University Press, 2008.

[19] HOUMANSADR A, KIYAVASHY N, BORISOV N. Rainbow: a robust and invisible non-blind watermark for network flows[A]. Proc of the 16th Network and Distributed System Security Symposium (NDSS'09)[C]. San Diego,USA, 2009.

[20] PARK Y H , REEVES D S. Adaptive watermarking against deliberate random delay for attack attribution through stepping stones[A]. Proc of the 9th International Conference on Information and Communications Security[C]. Zhengzhou, China, 2007.

[21] YU W, FU X W, GRAHAM S, *et al*. DSSS-based flow marking technique for invisible traceback[A]. Proc of the 2007 IEEE Symposium on Security and Privacy[C]. Oakland, USA , 2007.18-32.

[22] 傅翀，钱伟中，赵明渊等. 匿名通信系统时间攻击的时延规范化防御方法[J].东南大学学报(自然科学版)，2009, 39(4):738-741.
FU C, QIAN W Z, ZHAO M Y, *et al*. Delay normalization method of defending against timing-based attacks on anonymous communication systems[J]. Journal of Southeast University (Natural Science Edition), 2009, 39(4):738-741.

[23] RAMSBROCK D, WANG X Y, JIANG X Z. A first step towards live botmaster traceback[A]. Proc of the 11th International Symposium on Recent Advances in Intrusion Detection[C]. Cambridge, USA, 2008. 59-77.

[24] 王小刚. 基于网络流水印的入侵追踪技术研究[D].南京:东南大学，2012.
WANG X G. Research on Intrusion Traceback Exploiting Network Flow Watermarking[D]. Nanjing: Southeast University, 2012.

[25] WANG X Y, REEVES D S , WU S F，*et al*. Sleepy watermark tracing: an active network-based intrusion response framework[A]. Proc of the IFIP TC11 16th Annual Working Conference on Information Security: Trusted Information: the New Decade Challenge[C]. Paris, France, 2001. 369-384.

[26] ZHAO Q J , LU H T. A PCA-based watermarking scheme for tamper-proof of Web pages[J]. Pattern Recognition, 2005, 38(8):1321-1323.

[27] HUANG H J, WANG Y J, XIE L L, *et al*. An active anti-phishing solution based on semi-fragile watermark[J]. Information Technology Journal, 2013, 12(1):198-203.

[28] HUANG J W, PAN X, FU X W, *et al*. Long PN code based DSSS watermarking[A]. Proc of the IEEE INFOCOM 2011[C]. Shanghai, China, 2011. 2426-2434.

[29] FU X W, ZHU Y , GRAHAM B, *et al*. On flow marking attacks in wireless anonymous communication networks[A]. Proc of the 25th IEEE International Conference on Distributed Computing Systems (ICDCS'05)[C]. Columbus, USA , 2005. 493-503.

[30] WANG X Y , REEVES D S. Robust correlation of encrypted attack traffic through stepping stones by manipulation of interpacket delays[A]. Proc of the 10th ACM Conference on Computer And Communications Security[C]. Washington DC, USA, 2003. 20-29.

[31] WANG X Y, CHEN S P , JAJODIA S S. Tracking anonymous peer-to-peer VoIP calls on the internet[A]. Proc of the 12th ACM Conference on Computer And Communications Security[C]. Alexandria, USA , 2005. 81-91.

[32] ZHANG L, LUO J Z , YANG M. An improved DSSS-based flow marking technique for anonymous communication traceback[A]. Proc of the 2009 Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing(UIC-ATC'09)[C]. Brisbane, Australia, 2009. 563-567.

[33] 张连成，王振兴，徐静. 一种新的隐形流水印技术[J]. 应用科学学报, 2012,30(5):524-530.
ZHANG L C, WANG Z X, XU J. A novel invisible and private flow watermarking scheme[J]. Journal of Applied Sciences, 2012, 30(5): 524-530.

[34] WANG X Y, CHEN S P, JAJODIA S S. Network flow watermarking attack on low-latency anonymous communication systems[A]. Proc of the 2007 IEEE Symposium on Security and Privacy[C]. Oakland, USA, 2007.116-130.

[35] WANG X G, LUO J Z, YANG M. A double interval centroid-based watermark for network flow traceback[A]. Proc of the 14th International Conference on Computer Supported Cooperative Work in Design[C]. Shanghai, China, 2010. 146-151.

[36] LUO J Z, WANG X G, YANG M. An interval centroid based spread spectrum watermarking scheme for multi-flow traceback[J]. Journal of Network and Computer Applications, 2012, 35(1):60-71.

[37] PYUN Y J, PARK Y H, WANG X Y, *et al*. Tracing traffic through intermediate hosts that repacketize flows[A]. Proc of IEEE INFOCOM 2007[C]. Anchorage, USA, 2007. 634-642.

[38] JIA W J, TSO F P, LING Z, *et al*. Blind detection of spread spectrum flow watermarks[A]. Proc of the IEEE INFOCOM 2009[C]. Rio de Janeiro ,Brazil, 2009. 2195-2203.

[39] RTAI T. Real time application interface(RTAI)[EB/OL]. http://www.rtai.org , 2012.08.23 .

[40] 张璐，罗军舟，杨明. 基于正交流量特征的多维流水印技术[A]. 2010 年全国通信安全学术会议论文集[C]. 昆明，中国，2010. 243-248.
ZHANG L, LUO J Z, YANG M. Orthogonal flow characteristics based multi-dimensional flow watermarking technique[A]. Proc of the 2010 China Communication Security Symposium[C]. Kunming, China, 2010. 243-248.

[41] KIYAVASH N, HOUMANSADR A , BORISOV N. Multi-flow attacks against network flow watermarking schemes[A]. Proc of the 17th conference on USENIX Security Symposium[C]. San Jose, USA, 2008. 307-320.

[42] HOUMANSADR A , BORISOV N. SWIRL: a scalable watermark to detect correlated network flows[A]. Proc of the 18th Network and Distributed System Security Symposium 2011[C]. San Diego, USA, 2011.

[43] EVANS N S, DINGLEDINE R, GROTHOFF C. A practical congestion attack on Tor using long paths[A]. Proc of the 18th Conference on

USENIX Security Symposium[C]. Montreal, Canada, 2009. 33-50.

[44] LIN Z , HOPPER N. New attacks on timing-based network flow watermarks[A]. Proc of the 21th Conference on USENIX Security Symposium[C]. Bellevue, USA, 2012. 1-16.

[45] 张连成，王振兴，徐静. 一种基于包序重排的流水印技术[J].软件学报，2011, 22(2):17-26.
ZHANG L C, WANG Z X, XU J. Flow watermarking scheme based on packet reordering[J]. Journal of Software, 2011, 22(2):17-26.

[46] ANGRISANI L, CAPRIGLIONE D, FERRIGNO L, *et al*. Packet jitter measurement in communication networks: a sensitivity analysis[A]. Proc of the IEEE International Workshop on Measurement and Networking 2011[C]. Anacapri, Italy, 2011. 146-151.

[47] BREGNI S, BARUFFALDI A, PATTAVINA A. Active measurement and time-domain characterization of IP packet jitter[A]. Proc of the IEEE Latin-American Conference on Communications 2009[C]. Medellin, Columbia, 2009. 1-6.

[48] ALLMAN M , PAXSON V. TCP congestion control[EB/OL]. http://tools.ietf.org/html/rfc5681, 2009.

[49] POSTEL J. Transmission control Protocol[EB/OL]. http://www.ietf.org/rfc/rfc793.txt, 1981.

[50] PENG P, NING P, REEVES D S. On the secrecy of timing-based active watermarking trace-back techniques[A]. Proc of the 2006 IEEE Symposium on Security and Privacy[C]. Oakland, USA, 2006. 334-349.

[51] WANG X G , LUO J Z, YANG M. An efficient sequential watermark detection model for tracing network attack flows[A]. Proc of the 16th IEEE International Conference on Computer Supported Cooperative Work in Design[C]. Wuhan, China, 2012. 236-243.

[52] LUO X P, ZHANG J J, PERDISCI R , *et al*. On the secrecy of spread-spectrum flow watermarks[A]. Proc of the European Symposium on Research in Computer Security 2010[C]. Athens, Greece, 2010. 232-248.

[53] LUO X P, ZHOU P, ZHANG J J, *et al*. Exposing invisible timing-based traffic watermarks with BACKLIT[A]. Proc of the 27th Annual Computer Security Applications Conference[C]. Orlando, USA, 2011.197-206.

[54] PENG P, NING P, REEVE D S , *et al*. Active timing-based correlation of perturbed traffic flows with chaff packets[A]. Proc of the 25th International Conference on Distributed Computing Systems Workshops[C]. Columbus, USA, 2005.107-113.

[55] WANG, X G, YANG M, LUO J Z. A novel sequential watermark detection model for efficient traceback of secret network attack flows[J]. Journal of Network and Computer Applications, 2013, 36(6): 1660-1670.

[56] ZHANG L C, WANG Z X , WANG Q L , *et al*. MSAC and multi-flow attacks resistant spread spectrum watermarks for network flows[A]. Proc of the 2nd IEEE International Conference on Information and Financial Engineering[C]. Chongqing, China, 2010. 438-441.

[57] HOUMANSADR A, KIYAVASH N, BORISOV N. Multi-flow attack resistant watermarks for network flows[A]. Proc of the 2009 IEEE International Conference on Acoustics, Speech and Signal Processing[C]. Taipei, China, 2009. 1497-1500.

[58] GONG X, RODRIGUES M, KIYAVASH N. Invisible flow watermarks for channels with dependent substitution, deletion, and bursty insertion errors[EB/OL]. http://arxiv.org/pdf/1302.5734v1.pdf, 2013.

[59] 樊昌信，曹丽娜.通信原理（第 6 版）[M].北京:国防工业出版社，2006.
FAN C X , CAO L N. Communication Principles(6th Edition)[M]. Beijing: National Defence Industry Press, 2006.

[60] BALDINI A, DE C L , RISSO F. Increasing performances of TCP data transfers through multiple parallel connections[A]. Proc of the 2009 IEEE Symposium on Computers and Communications[C]. Sousse, Tunisia,2009. 630-636.

[61] IHM S, PAI V S. Towards understanding modern web traffic[A]. Proc of the 2011 ACM SIGCOMM on Internet Measurement Conference (IMC'11)[C]. Berlin, Germany,2011. 295-312.

[62] RAO A , LEGOUT A, LIM Y S, *et al*. Network characteristics of video streaming traffic[A]. Proc of the 7th Conference on Emerging Networking Experiments and Technologies(CoNEXT '11)[C]. Tokyo, Japan, 2011.

[63] XI B W, CHEN H, CLEVELAND W S, *et al*. Statistical analysis and modeling of Internet VoIP traffic for network engineering[J]. Electronic Journal of Statistics, 2010, 4:58-116.

[64] RATTI S, HARIRI B, SHIRMOHAMMADI S. A survey of First-Person shooter gaming traffic on the Internet[J]. IEEE Internet Computing, 2010,14(5):60-69.

[65] ARCHIBALD R, GHOSAL D. A covert timing channel based on Fountain Codes[A]. Proc of the 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom'12)[C]. Liverpool, UK, 2012. 970-977.

[66] ROY S D, LI X, SHOSHAN Y, *et al*. Hardware implementation of a digital watermarking system for video authentication[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2013, 23(2): 289-301.

[67] HOLUB V, FRIDRICH J. Digital image steganography using universal distortion[A]. Proc of the 1st ACM Workshop on Information Hiding And Multimedia Security[C]. Montpellier, France, 2013.59-68.

[68] FATEMEH D , SAEED M. Watermarking in binary document images using fractal codes[J]. Pattern Recognition Letters, 2014, 35:120-129.

[69] 钱玉文，赵邦信，孔建寿等. 一种基于 Web 的可靠网络隐蔽时间信道的研究[J]. 计算机研究与发展，2011，48(3): 423-431.
QIAN Y W, ZHAO B X, KONG J S, *et al*. Robust covert timing channel based on web[J]. Journal of Computer Research and Development, 2011, 48(3): 423-431.

[70] SEBASTIAN Z, GRENVILLE A, PHILIP B. Stealthier inter-packet timing covert channels[A]. Proc of the 10th International IFIP TC 6 Networking Conference[C]. Valencia, Spain, 2011.458-470.

[71] FURON T, BAS P. A new measure of watermarking security applied on QIM[A]. Proc of 14th International Conference on Information Hiding(IH'12)[C]. Berkeley, USA, 2012. 207-223.

[72] WIKIPEDIA. Trusted computer system evaluation criteria (TCSEC) [EB/OL].http://en.wikipedia.org/wiki/Trusted_Computer_System_Evaluation_Criteria, 2013.

[73] MOHAN D, JUSTIN S, RENATA T, *et al*. Fathom: a browser-based network measurement platform[A]. Proc of the 2012 ACM conference on Internet Measurement Conference(IMC'12)[C]. Boston, USA,

2012.73-86.

[74] SNOEREN A C, PARTRIDGE C, SANCHEZ L A, *et al*. Single-packet IP traceback[J]. IEEE/ACM Transactions on Networking, 2002 ,10(6): 721-734.

[75] LIN I H, PENG S H. A probabilistic packet marking scheme with LT code for IP traceback[J]. Journal of Internet Technology, 2013, 14(2): 189-202.

[76] BATES A, MOOD B, PLETCHER J, *et al*. Detecting co-residency with active traffic analysis techniques[A]. Proc of the 2012 ACM Workshop on Cloud Computing Security Workshop[C]. Raleigh, USA, 2012. 1-12.

[77] 罗军舟, 吴文甲, 杨明. 移动互联网：终端、网络与服务[J].计算机学报, 2011, 34(11):2029-2051.
LUO J Z, WU W J , YANG M. Mobile Internet: terminal devices, networks and services[J].Chinese Journal of Computers, 2011, 34(11): 2029-2051.

[78] 周昌令, 钱群, 赵伊秋等.校园无线网用户群体的移动行为聚集分析[J].通信学报，2013,34(Z2):111-116.
ZHOU C L, QIAN Q, ZHAO Y Q , *et al*. Modularity analysis of users' mobile behavior in campus wireless network[J]. Journal on Communications, 2013,34(Z2):111-116.

[79] NDN Testbed[EB/OL]. http://named-data.net/ndn-testbed/, 2013-11.

[80] AFANASYEV A, MOISEENKO I, ZHANG L X. NDNSIM: NDN Simulator for NS-3[R]. NDN Technical Report NDN-0005, 2012.

作者简介：

郭晓军（1983-），男，山西长治人，东南大学博士生，主要研究方向为网络安全、网络测量及网络管理。

程光（1973-），男，安徽黄山人，东南大学教授、博士生导师，主要研究方向为网络安全、网络测量与行为学及未来网络安全。

朱琛刚（1982-），男，江苏南京人，东南大学博士生，主要研究方向为多媒体内容分析与安全、机器学习。

TRUONG Dinh-Tu（1979-），男，越南人，东南大学博士生，主要研究方向为网络安全、云计算。

周爱平（1982-），男，江苏泰州人，东南大学博士生，主要研究方向为网络测量、网络安全。