网络流水印技术研究进展

张连成 王振兴 刘慧生
(解放军信息工程大学信息工程学院 郑州 450002)

摘 要 网络流水印技术作为一种主动流量分析手段,可有效追踪恶意匿名通信使用者与跳板链后的真实攻击者,具有准确率高、误报率低和观测时间短等优点,在攻击源追踪、网络监管和攻击取证等领域有着重要应用。首先阐述网络流水印技术的基本框架及主要特点,接着对当前基于包载荷、基于流速率和基于包时间的典型网络流水印技术进行简要介绍,然后概述针对网络流水印技术的时间分析攻击、多流攻击和均方自相关攻击等主要攻击手段与反制对策,最后对网络流水印技术的发展前景进行展望。

关键词 网络流水印,包时间,时间间隔,扩频通信,多流攻击,均方自相关攻击,匿名通信,跳板
中图法分类号 TP393 **文献标识码** A

Survey on Network Flow Watermarking Technologies

ZHANG Lian-cheng WANG Zhen-xing LIU Hui-sheng
(College of Information Engineering, PLA Information Engineering University, Zhengzhou 450002, China)

Abstract As active traffic analysis approaches, network flow watermarking technologies can effectively traceback anonymous abusers and network attackers behind a connection chain of stepping stones. As they can achieve high detection rates and low false positive rates within short observation time, flow watermarking technologies have significant applications in many fields, such as attack traceback, network supervision and attack forensic. This paper firstly represented basic framework and major characteristics of flow watermarking technologies, then briefly introduced typical packet payload based, traffic rate based and packet timing based flow watermarking schemes at present, after that, main attack technologies, such as timing analysis attack, multi-flow attack and mean-square autocorrelation attack, and countermeasures of flow watermarking schemes were described, finally, near future research directions were discussed.

Keywords Network flow watermarking, Packet timing, Interval, Spread spectrum, Multi-flow attack, Mean-square autocorrelation attack, Anonymous communication, Stepping stone

1 引言

互联网攻击日益加剧,面对当前复杂的网络环境,及时响应、主动防御成为持续动态维护网络安全的重要保障。然而,大多数网络安全机制却"被动"应对这些网络攻击。特别地,现在的入侵检测机制越来越难以有效跟踪与检测网络攻击源。

事实上,由于网络攻击者很少直接通过自己的计算机发动攻击,在攻击最终目标之前他们更愿意登录一系列的中间跳板(Stepping Stone)或利用匿名通信(Anonymous Communication)系统来隐蔽自己的身份,这使得网络源追溯变得异常困难。

在保护用户通信隐私的同时,匿名通信系统(如 Tor[1]、Crowds[2,3]和 Anonymizer 等)也可能被用于网络犯罪、流言散布和色情传播等恶意行为。使用 IP 包头部信息的传统入侵检测和网络监管方式越来越不适用于这些匿名通信系统[4]。

同时,网络攻击者隐藏身份和防止源追踪的另一个常用手段是使用跳板[5]。并且为更有效地躲避追踪,攻击者还往往在跳板处对数据流进行加密、包重组(Repacketization)、时间扰乱(Timing Perturbation)和添加垃圾包(Chaff Packet)等干扰。

这些匿名通信和跳板技术与手段的使用给攻击源追踪、网络监管和攻击取证等带来严峻挑战。相对于传统的被动流量分析[6-10]而言,网络流水印(Network Flow Watermarking)作为一种主动流量分析手段,可用于追踪通过跳板链进行的网络攻击源或采取匿名通道进行非法通信的恶意用户。通过向发送者的发送流量中主动添加水印(Watermark)来帮助确认发送者和接收者的通信关系,网络流水印技术具有准确率高、误报率低、观测时间短和所需观测数据包数量少等优点,近年来得到学术界的广泛关注。

2 网络流水印框架及特点

网络流水印技术,也叫流标记(Flow Marking)技术,通过

到稿日期:2010-12-21 返修日期:2011-03-24
张连成(1982—),男,博士生,主要研究方向为流量分析、网络安全,E-mail:liancheng17@gmail.com;王振兴(1959—),男,博士,教授,主要研究方向为流量分析、网络与信息安全;刘慧生(1985—),男,博士生,主要研究方向为流量分析、网络安全。

改变或调制发送端数据包的载荷(Payload)、时间间隔(Interval)、间隔到达时延(Inter-Packet Delay,IPD)和间隔重心(Interval Centroid)等信息或流量速率(Traffic Rate)来嵌入水印,在接收端识别该水印,以达到关联发送者和接收者关系的目的。目前,许多网络流水印技术都主要借鉴并将多媒体水印思想应用于网络数据流中[11]以检测跳板[12]和攻击匿名[13]。网络流水印框架如图1所示。

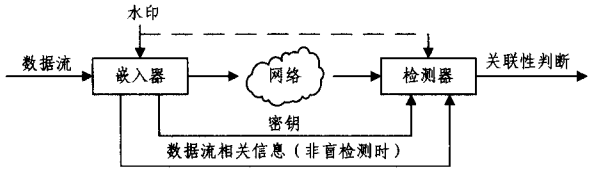

图1 网络流水印框架

当网络数据流经过水印嵌入点(如路由器)时,嵌入器使用密钥(Key)将水印进行编码,通过调制流量特征(如改变数据流的速度)嵌入该水印。嵌入水印后的标记数据流在网络传输时会遭受一些干扰和变形,如中间路由器(或匿名网络、跳板等)的延迟、丢包或重传数据包、包重组和时间扰乱等。最终,当被扰乱之后的标记数据流到达水印检测点,检测器使用与嵌入器同样的密钥(非盲检测时,检测器还需要标记数据流嵌入水印前的相关信息)提取标记数据流中的水印信息,如果与编码时的水印一致,那么就认为这两条数据流之间存在关联。

从上述水印嵌入与检测流程可以看出,网络流水印技术必须具有以下特点:

(1) 机密性(Secrecy)。为防止攻击者观察到标记数据流中水印信息的存在,对需嵌入水印的目标数据流进行的改动应尽可能小,必须具有良好的不可见性(Invisibility),同时也不能过多影响数据流的性能。

(2) 鲁棒性(Robustness)。对于中间可能的干扰(路由器的时间抖动、攻击者的时间扰乱和包重组等)具有比较强的抵抗能力,即在严重干扰情况下依然能保持良好的正确率和较低的误报率。

(3) 唯一性(Uniqueness)。为降低误报率,每条数据流中嵌入的水印消息必须具有唯一性,即不同数据流必须嵌入不同的、可明显区分的水印信息。

(4) 效率(Effectiveness)。在同样准确率的情况下,网络流水印技术应使用数量尽可能少的数据包以提高其适用性和时效性。

3 典型网络流水印技术

目前,学术界已提出多种类型的网络流水印技术,它们具有各自的优势和特点。按照流水印载体的不同,本文将其分为基于包载荷、基于流速率和基于包时间(Packet Timing)的流水印技术3种。

3.1 基于包载荷的流水印技术

基于包载荷的流水印技术通过调制数据流中数据包的应用载荷来嵌入水印,进而达到关联数据流的目的。

Wang等[14]提出一种主动入侵响应框架——休眠水印追踪(Sleepy Watermark Tracing,SWT)。"休眠"是指当没有检测到入侵时,它不会带来任何开销。只有检测到入侵时,它才会活跃起来,并将水印(不同的字符串组合)注入到网络入侵者的返回连接中,并与入侵路径上的中间路由器合作来进行攻击源追踪。通过将休眠入侵响应方案、水印关联技术和主动追踪协议集成在一起,SWT可对通过telnet或rlogin建立的交互式入侵进行高效、准确的源追踪。但该方法基于包载荷内容,与具体协议(telnet、rlogin)有关,不能适应加密情况,适用环境受限,且容易被攻击者检测和过滤。

为追踪僵尸主控机(Botmaster),Ramsbrock等[15]通过在应用层向僵尸网络(Botnet)命令和控制(Command and Control,C&C)消息中添加填充字符使其长度产生差异,进而嵌入水印,以便对基于IRC(Internet Relay Chat)的Botmaster进行有效追踪,即使该流量:(1) 使用SSL/TLS等加密;(2) 经过多个中间节点(如IRC服务器、SOCKs等);(3) 与其他僵尸网络流量混杂。

3.2 基于流速率的流水印技术

基于流速率的流水印技术通过调制数据流的速度来嵌入水印,进而达到关联数据流的目的。

Fu等[16]采用频域分析技术将时域水印转变成特征不变的频率,通过电磁干扰将其嵌入到无线网络数据流中,可有效降低基于流(Flow-based)的无线Mix网络的匿名度,但该方法难以抵御数字过滤(Digital Filtering)技术。

Yu等[17]通过修改发送者流量的速率设计了基于直序扩频(Direct Sequence Spread Spectrum,DSSS)的流水印技术用于追踪匿名通信者,它可达到非常高的检测率和极低的误报率,但只适合流量速率固定的情况。不幸的是,大多数匿名通信流量(如网络浏览、即时通信和远程登录等)的速率却是不固定的[4]。

3.3 基于包时间的流水印技术

追踪经过跳板或匿名Mix节点的交互流量挑战很大,因为此时包头、包长度及包载荷都可能被改变,包时间因此成为流量追踪的重要手段。基于包时间的流水印技术通过调制数据流的时间特征来嵌入水印,进而达到关联数据流的目的。与基于包载荷和基于流速率的流水印技术相比,基于包时间的流水印技术适用性较好,实现和部署相对容易,逐步成为流水印技术的研究热点。

目前,学术界提出了多种基于包时间的流水印技术,按照调制对象的不同,本文将其分为基于间隔到达时延、基于时间间隔和基于间隔重心的流水印技术3类。

3.3.1 基于间隔到达时延的流水印技术

间隔到达时延IPD是指一条数据流中数据包先后到达的时间间隔,通过调制该流量特征可有效嵌入水印信息进行数据流关联。

基于包时间的被动流相关方法很容易受到攻击者在跳板处引入的时间扰乱的影响。针对该问题,Wang等[8]提出一种基于水印的主动流相关技术,即基于IPD的概率流水印技术,它通过稍微调整数据流中独立和随机选定的数据包的IPD嵌入水印位,对于随机时间扰乱具有鲁棒性。但该技术使用固定参数值,导致如下问题:(1) 由于IPD分布的不同,无法保证每个水印位都能被正确嵌入;(2) 当包数量较少,不足以嵌入所有预定水印位时,无法进行正确的源追踪;(3) 由于使用固定的包最大延迟值和嵌入单个水印位所需的包数量,难以有效抵御时间扰乱。

针对上述问题,Park等[18]提出一种自适应概率流水印技

术，其根据待追踪流量的包时间和包大小特征自适应地选择流水印的参数值，能容忍任何形式的时间扰乱。对于平均高达 8000 毫秒的时间扰乱，该技术的检测率可达 100%，且误报率几乎 0%。

为解决时间扰乱问题，Pan 等[19]提出基于包分组(Packet Grouping)的流水印技术。它首先将数据流分为几个大的数据包组，然后进一步将数据包组分成数据包对(Packet Pair)，根据数据包组之间 IPD 的平均差异及水印位的值，来决定是否调整包时间及如何调整，以此嵌入水印。

Wang 等[20]提出追踪 P2P 匿名 VoIP 电话的主动流水印技术，其水印嵌入方式与基于 IPD 的概率流水印技术类似，但该技术并不对数据流的 IPD 进行量化，而只是向左或向右对$\overline{Y_{r,d}}$(冗余 r 下的间隔到达时延平均值)调整大小 a 来实现水印位的嵌入。分析和测试结果表明：1)在互联网上追踪 P2P 匿名 VoIP 电话是可行的；2)低延迟匿名网络难以抵御时间攻击(Timing Attack)。

为躲避追踪，攻击者在跳板处除了进行加密处理和时间扰乱之外，还可能添加无意义的垃圾数据包。添加垃圾包后，数据流中的包数量比其中所标记的包数量要大，难以一一对应，因此可降低流水印技术的准确率。针对该问题，Peng 等[21]提出基于包匹配(Packet Matching)和 IPD 的主动流水印技术，在一定时间限制的假设下，提出在检测率、误报率和计算开销之间权衡的多个算法，用以对垃圾包添加前后数据流中的数据包进行匹配以找出相对应的数据包，然后再进行数据流关联。

已有流水印技术会在数据流中引入大的时延，使得攻击者容易检测甚至移除其中的水印，同时还会降低合法流量的速率。Houmansadr 等[12]提出 RAINBOW 流水印技术，其所用时延只有先前流水印技术的几百分之一。相对于被动流量分析，该技术错误率大大降低，仅需观察几百个数据包即可对数据流进行有效关联，且对丢包和包重组具有鲁棒性。但该技术假设攻击者不愿意(或不能够)主动对通过跳板处的数据流进行变换、变形处理，还假设网络数据流服从独立泊松(Poisson)分布，这些假设一般情况下很难成立；且该技术为非盲检测，需要水印嵌入端的数据流 IPD 数据库支持，部署困难。

3.3.2 基于时间间隔的流水印技术

包重组是许多应用(如 SSH)的自然结果，为防止追踪，攻击者甚至会在跳板处故意进行包合并(Packet Splitting)和包分割(Packet Merging)等，已有流水印技术在面对包重组时效果大大减弱。针对该问题，Pyun 等[22]提出基于时间间隔的流水印(Interval-Based Watermarking，IBW)方案，它将数据流切成固定长度的时间间隔，调整包时间来控制特定时间间隔中的包数量来嵌入水印，能够在包重组存在的情况下追踪恶意数据流。但该方案不能抵御向数据流中添加垃圾包、流合并(Flow Merging)和流分割(Flow Splitting)等手段。

Tor 匿名网络中 TCP 多路传输引入的包重组和延迟会影响 IBW 技术的追踪效果，Huang 等[23]通过研究发现：如果掌握 Tor 的包处理机制，那么通过修改包大小减少 Tor 节点的包重组率、增大时间间隔长度就可对 Tor 匿名用户进行有效关联。

3.3.3 基于间隔重心的流水印技术

假定给定数据流包含足够多的数据包，从随机偏移 $o>0$ 处开始，将后继数据流分为固定时间长度 $T>0$ 的间隔段 $I_i(i=0,1,2,\cdots)$，那么这些间隔段中的包间隔位置(Δt_i)是均匀分布的。假设间隔 I_i 有 $n_i>0$ 个数据包，那么间隔重心可定义为：

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

间隔重心代表了间隔 I_i 的平衡点，因此通过对其进行调制可有效关联数据流。

长久以来，人们都相信流量填充(Traffic Padding)、添加掩饰流(Cover Traffic)、包丢弃、流混杂(Flow Mixing)、流分割和流合并等流变换技术能够有效伪装网络数据流，从而达到很好的匿名性。Wang 等[13]对流变换技术的研究结果显示，流变换并不提供人们所盼望或相信的那种匿名性，并提出了基于间隔重心的流水印(Interval Centroid Based Watermarking，ICBW)方案，该方案通过将水印注入到数据流的包间隔时间域中，可使任何足够长的数据流具有独特的可识别性，即使它：(1) 使用大量的掩饰流进行伪装；(2) 与大量其它数据流混合或合并；(3) 被分割成大量子数据流；(4) 有大量数据包被丢弃；(5) 在时间上被自然时延或攻击者故意添加的时延所扰乱。但该方案需要较多的数据包，并且难以抵御多流攻击(Multi-flow Attack)[24]。

现在大多数基于包时间的流水印技术由于标记数据流之间互相冲突，难以并行追踪多条网络数据流；同时，基于直序扩频 DSSS 的流水印技术[17]不适合追踪低速率数据流。通过将基于间隔质心的数据流调制方法和扩频(Spread Spectrum，SS)编码相结合，Wang 等[25]提出基于间隔重心的扩频流水印(Interval Centroid Based Spread Spectrum Watermarking，ICBSSW)方案，它能高效、并行追踪多条网络数据流。接着，Wang 等[26]提出基于双重间隔重心的流水印(Double Interval Centroid-Based Watermarking，DICBW)方案，它通过调制相邻时间间隔对的包时间来追踪恶意数据流。通过将 DICBW 方案与扩频编码相结合，进一步提出用于高效数据流追踪的通用混合流水印框架。

4 网络流水印的攻击方法及对策

网络流水印技术可用于在跳板链和匿名网络中追踪攻击者和恶意用户，即使其使用的网络连接经过加密处理，且存在时间扰乱、包重组和垃圾包等干扰。但这些技术由于要主动修改包速率和包间隔到达时延等流量特征，因此也成为攻击对象，如：追踪者通过电磁干扰调制无线通信流量的速度向其中嵌入水印来追踪恶意用户，但 Fu 等[16]提出基于数字过滤的对策能有效防护无线 Mix 网络来抵御该追踪方式。

由于基于包时间的流水印技术是目前的研究热点，下面主要对基于包时间的流水印技术的攻击方法及对策进行简要介绍。

4.1 基于包延迟的时间分析攻击

Peng 等[27]对基于 IPD 的概率流水印技术进行深入研究，提出一种基于相邻跳板间数据包延迟的时间分析攻击技术。首先采用期望最大化(Expectation Maximization，EM)算法估计量化步长(Quantization Step)和水印延迟比例，接着使用贝叶斯判决规则(Bayes Decision Rule)识别被延迟的标记数据包，然后针对水印嵌入的 4 种不同情况分别给出了水印

恢复和复制的具体步骤，使得攻击者能在某些情况下从跳板链中移除水印或向非跳板链中复制水印。在评估水印检测率、误报率及延迟数据包最小数量之后，通过序列概率比测试(Sequential Probability Ratio Test)来检测水印的存在性，可实时确认跳板链中是否被嵌入水印。研究结果表明，对于流水印技术：(1) 如果参数选择不当，水印很容易被恢复和复制；(2) 常常可快速检测网络数据流中是否存在水印。

4.2 时延规范化攻击

为攻击匿名通信系统的流水印技术，傅翀等[28]提出包时延规范化攻击方法。该方法将数据流中所有时延间隔调整至一个固定值，以防止追踪者嵌入水印信息，从而达到破坏数据流关联的目的。该方法的攻击效果不受追踪者选取的起始时间和用于嵌入水印的时间间隔的影响，可使 ICBW 技术[13]的误判率平均达到 43.51%。

4.3 多流攻击

Kiyavash 等[24]对几种流水印技术(基于时间间隔[22]、基于间隔重心[13]和基于直序扩频[17]的流水印技术)进行研究后发现，由于这些技术将数据流分割成不同的时间间隔会导致数据流间产生时间依赖性，使得攻击者能将多条标记数据流合并起来发起多流攻击。该攻击可用于检测水印的存在性、恢复出水印的秘密参数、将水印从标记数据流中移除，甚至对于那些嵌入不同水印的多条标记数据流也同样有效。

4.4 均方自相关攻击

Jia 等[29]提出一种基于单条数据流的攻击方案来检测 DSSS 水印的存在性。由于基于 DSSS 的流水印技术在调制多比特水印信号时采用了同一 PN 码，使得标记数据流具有自相似性。它通过单条标记数据流的流量速率时间序列的均方自相关(Mean-Square AutoCorrelation，MSAC)来检测恶意 DSSS 水印，使对其所用 PN 码毫无所知。该攻击方案复杂度低，比基于多流攻击的 DSSS 水印检测方案[24]更加灵活和准确。

4.5 基于 TCP 流控制机制的 DSSS 水印移除攻击

通过对基于直序扩频 DSSS 的流水印技术的研究，Luo 等[30]发现：(1) 与信号处理中的波幅调制一样，该技术会造成标记数据流产生低吞吐量和高吞吐量的交替周期；(2) 不但不能增强水印的隐蔽性，PN 码反而会增加被检测到的几率，因其提高了低吞吐量周期的次数；(3) 在扩频无线通信时，无线信号被扩展到宽频带区域，而该技术将水印嵌入到单条数据流中，使得单流检测成为可能。基于此，通过定位数据流中的低吞吐量周期，然后检测其中的异常序列，提出基于 TCP 流控制机制的 DSSS 水印移除方法，使得终端用户可有效移除数据流中的扩频水印，且不需要中间路由器、代理或中继节点的支持。

4.6 网络流水印攻击的部分对策

多流攻击利用嵌入过相同水印信息的标记数据流之间的依赖关系来恢复出所嵌入水印的秘密参数，并从数据流中将水印移除。针对多流攻击，Houmansadr 等[31]提出抗多流攻击、基于间隔重心的流水印(MAR-ICBW)方案，它通过将不同数据流中的水印嵌入位置进行随机化处理，可有效消除标记数据流之间的依赖关系，因此能有效抵御多流攻击。

由于基于直序扩频 DSSS 的流水印技术在调整多比特信号时采用同一 PN 码，因此标记数据流具有自相似性，导致攻击者以此可发起 MSAC 攻击。我们使用多个正交 PN 码来扩展信号的不同比特位，并使用相同的 PN 码序列来解扩以恢复信号[32]。由于这些 PN 码是正交的，它们在文献[29]中公式(10)上就相互抵消，因此标记数据流速率的时间序列的均方自相关就不会显现出峰值，进而可有效抵御 MSAC 攻击。

5 网络流水印技术发展趋势分析与前景展望

网络流水印技术具有不受加密影响、准确率高、误报率低和观测时间短等优势，近年来成为学术界关注的热点。但流水印技术由于要主动修改数据流的包载荷、流速率和包时间等流量特征，同样会遭受各种攻击。网络流水印技术及攻击技术的发展必将是矛和盾的反复交替过程。本文认为，目前网络流水印技术存在的主要问题及潜在的研究方向有：

(1) 流水印整体设计。当前网络流水印技术主要借鉴数字水印思想，对于流水印的整体设计问题缺乏足够关注。比如，在数字水印中，信息载体的统计特征常常是重点考虑的方面，然而目前网络流水印技术研究中对网络流量特征对于水印的影响缺乏合适模型[24]。且已有的网络流水印技术大都假设时间扰乱是随机的，网络流量服从泊松分布，然而这些假设往往不太符合实际[33-35]。另外，水印产生、水印编码、数据流同步、载体选择、嵌入点和检测点部署、入侵路径构建、自动化追踪等方面的研究尚未有效开展。

(2) 抗检测和抗攻击能力。数据流加密后，很多流量特征难以使用，目前流水印技术往往使用包时间特征，而通过修改这些特征必然会引起不同的变化，这本身就会造成流水印存在性及参数泄漏等问题。如何进一步提高网络流水印技术的隐蔽性与抗检测、抗时间攻击能力是亟待解决的难题。

(3) 自适应能力。针对不同类型的数据流、不同的网络环境应能自适应地选择水印参数，提高网络流水印技术的环境适应能力，以达到较好的数据流关联目的。

(4) 多流追踪(Multi-flow Traceback)能力。现有网络流水印技术在对多条数据流嵌入水印后，由于要考虑机密性(如时延不能改变太大等)，又要兼顾鲁棒性(如时延改变应能抵御时间扰乱等)，多条标记数据流在经过同一跳板或匿名节点时的相互干扰较大，不利于多流追踪。流水印技术的多流追踪能力亟待提高。

(5) 水印容量评估。信息容量问题是信息隐藏技术中的一个关键技术，同样也是网络流水印的关键技术。但到目前为止，还没有对某种数据流载体可以嵌入多少水印量进行准确计算的理论方法[11]。

(6) 水印嵌入与检测的复杂度。随着网络流水印技术及相应攻击技术的不断向前进步，为提高隐蔽性和抗攻击能力，网络流水印技术的复杂度势必越来越高，但目前尚未进行水印嵌入及水印检测的时间、空间复杂度的相关研究。

总之，网络流水印技术作为主动流相关技术，在跳板检测和匿名通信攻击等方面得到广泛应用。随着网络流水印技术的不断发展，它必将在攻击源追踪、网络监管和攻击取证等方面发挥越来越重要的作用。

参 考 文 献

[1] Dingledine R, Mathewson N, Syverson P. Tor: the second- gen-

eration onion router[C]// Proceedings of the 13th USENIX Security Symposium. 2004, San Diego. CA, USA: USENIX Association, 2004: 303-320

[2] Reiter M K, Rubin A D. Crowds: anonymity for web transactions[J]. ACM Transactions on Information and System Security, 1998, 1(1): 66-92

[3] Reiter M K, Rubin A D. Anonymous web transactions with crowds[J]. Communications of the ACM, 1999, 42(2): 32-38

[4] Zhang Lu, Luo Jun-zhou, Yang Ming. An improved dsss-based flow marking technique for anonymous communication traceback [A]// Proceedings of International Symposium on Multidisciplinary Autonomous Networks and Systems (MANS'09), 2009 [C]. Brisbane, Australia: IEEE Computer Society, 2009: 563-567

[5] Zhang Yin, Paxson V. Detecting stepping stones [A]// Proceedings of the 9th USENIX Security Symposium 2000[C]. Denver, Colorado: USENIX Association, 2000: 171-184

[6] Staniford-Chen S, Heberlein L T. Holding intruders accountable on the internet[A]// Proceedings of the 1995 IEEE Symposium on Security and Privacy(SP'95), 1995[C]. Oakland, CA, USA: IEEE, 1995: 39-49

[7] Wang Xin-yuan, Reeves D S, Wu S F. Inter-packet delay based correlation for tracing encrypted connections through stepping stones[A] // Proceedings of the 7th European Symposium on Research in Computer Security (ESORICS'02), 2002[C]. Zurich, Switzerland: Springer-Verlag, 2002: 244-263

[8] Wang Xin-yuan, Reeves D S. Robust correlation of encrypted attack traffic through stepping stones by manipulation of inter-packet delays[A]// Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS'03), 2003[C]. Washington, DC, USA: ACM, 2003: 20-29

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

[10] Zhu Ye, Fu Xin-wen, Gramham B, et al. Correlation-based traffic analysis attacks on anonymity networks[J]. IEEE Transactions on Parallel and Distributed Systems, 2010, 21(7): 954-967

[11] Houmansadr A, Coleman T, Kiyavash N, et al. On the channel capacity of network flow watermarking [A] // Proceedings of 16th ACM Conference on Computer and Communications Security (CCS'09), 2009[C]. Chicago, IL, USA: ACM Press, 2009: 2

[12] Houmansadr A, Kiyavash N, Borisov N. Rainbow: a robust and invisible non-blind watermark for network flows[A] // Proceedings of the 16th Annual Network & Distributed System Security Symposium (NDSS'09), 2009[C]. San Diego, CA, USA: The Internet Society, 2009: 224-236

[13] Wang Xin-yuan, Chen Shi-ping, Jajodia S. Network flow watermarking attack on low-latency anonymous communication systems[A] // Proceedings of 2007 IEEE Symposium on Security and Privacy(SP'07), 2007[C]. Oakland, California, USA: IEEE Computer Society, 2007: 116-130

[14] Wang Xin-yuan, Reeves D S, Wu S F, et al. Sleepy watermark tracing: an active network-based intrusion response framework [A]// Proceedings of 16th International Conference on Information Security (IFIP/Sec'01), 2001[C]. Paris, France: Kluwer Academic Publishers, 2001: 369-384

[15] Ramsbrock D, Wang Xin-yuan, Jiang Xu-xian. A first step toward live botmaster traceback[A]// Proceedings of the 11th International Symposium on Recent Advances in Intrusion Detection(RAID'08), 2008[C]. Boston, MA, USA: Springer, 2008: 59-77

[16] Fu Xin-wen, Zhu Ye, Graham B, et al. On flow marking attacks in wireless anonymous communication networks[A] // Proceedings of 25th IEEE International Conference on Distributed Computing Systems (ICDCS'05), 2005[C]. Columbus, OH: IEEE Computer Society, 2005: 493-503

[17] Yu Wei, Fu Xin-wen, Graham S, et al. Dsss-based flow marking technique for invisible traceback [A] // Proceedings of 2007 IEEE Symposium on Security and Privacy (SP'07), 2007[C]. Oakland, CA, USA: IEEE Computer Society, 2007: 7-21

[18] Park Y H, Reeves D S. Adaptive timing-based active watermarking for attack attribution through stepping stones[A] // Proceedings of the 2nd International Workshop on Security in Distributed Computing Systems(SDCS'05), 2007[C]. Washington, DC, USA: IEEE Computer Society, 2007: 107-113

[19] Pan Zheng, Peng Hong, Long Xian-zhong, et al. A watermarking-based host correlation detection scheme[A]// 2009 International Conference on Management of e-Commerce and e-Government, 2009[C]. Nanchang, China: IEEE Computer Society, 2009: 493-497

[20] Wang Xin-yuan, Chen Shi-ping, Jajodia S. Tracking anonymous peer-to-peer voip calls on the internet[A]// Proceedings of the 12th ACM Conference on Computer and Communications Security (CCS'05), 2005[C]. Alexandra, Virginia, USA: ACM, 2005: 81-91

[21] Peng Pai, Ning Peng, Reeves D S, et al. Active timing-based correlation of perturbed traffic flows with chaff packets[A]// Proceedings of the 25th IEEE International Conference on Distributed Computing Systems Workshops (ICDCSW'05), 2005[C]. Columbus, OH, USA: IEEE Computer Society, 2005: 107-113

[22] Pyun Y J, Park Y H, Wang Xin-yuan, et al. Tracing traffic through intermediate hosts that repacketize flows[A] // Proceedings of the 26th IEEE International Conference on Computer Communications (Infocom'07), 2007[C]. Anchorage, AK, USA: IEEE, 2007: 634-642

[23] Huang Di-jiang, Agarwal U. Countering repacketization watermarking attacks on tor network[A]// Proceedings of the 8th International Conference on Application Cryptography and Network Security (ACNS'10), 2010[C]. Beijing, China: Springer, 2010: 232-249

[24] Kiyavash N, Houmansadr A, Borisov N. Multi-flow attacks against network flow watermarking schemes[A]// Proceedings of 17th USENIX Security, 2008[C]. San Jose, CA, USA: USENIX Association, 2008: 307-320

[25] Wang Xiao-gang, Luo Jun-zhou, Yang Ming. An interval centroid based spread spectrum watermark for tracing multiple network flows[A] // Proceedings of the 2009 IEEE International Conference on Systems, Man, and Cybernetics, 2009[C]. San Antonio, TX, USA: IEEE, 2009: 4000-4006

[26] Wang Xiao-gang, Luo Jun-zhou, Yang Ming. A double interval centroid-based watermark for network flow traceback[A]// Proceedings of the 2010 14th International Conference on Computer Supported Cooperative Work in Design(CSCWD'10), 2010[C]. Shanghai, China: IEEE, 2010: 146-151

(下转第 42 页)

级网表，并通过 ModelSim 进行仿真后生成 VCD 文件，最后利用 Synopsys 公司开发的门级仿真软件 PrimePower 建立功耗数据采集平台对网表和 VCD 文件进行功耗仿真。后端的数据分析包括功耗波形文件处理，相关系数计算均基于 Matlab 程序完成。

图 2 为 20 个样本条件下，PRESENT 加密第一轮密钥 K_1 的 16 个 4 位密钥块对应的 16 条相关性曲线。其中 X 轴表示 16 个 4 位密钥块，Y 轴表示每个 4 位密钥块的 16 个候选值，Z 轴表示每个 4 位密钥块的每个候选值对应的 Pearson 相关性系数。对于每一个 4 位密钥块来说，具有最大 Pearson 相关系数的相关性曲线对应的密钥候选值即为正确的密钥块值。从图中可看出 $k_{1,0}=1, k_{1,1}=7, k_{1,2}=1, k_{1,3}=0, k_{1,4}=0, k_{1,5}=6, k_{1,6}=3, k_{1,7}=e, k_{1,8}=0, k_{1,9}=2, k_{1,10}=3, k_{1,11}=9, k_{1,12}=4, k_{1,13}=9, k_{1,14}=5, k_{1,15}=7$。

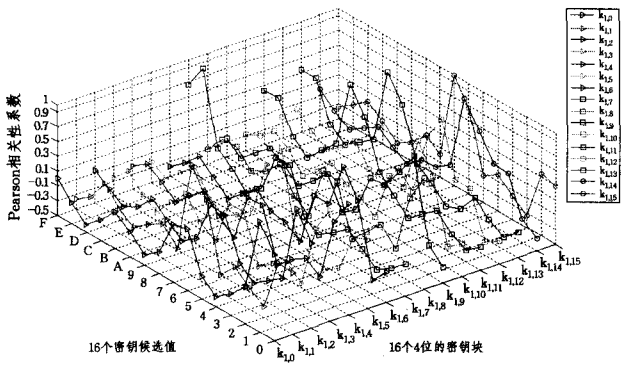

图 2　第一轮密钥 K_1 的 16 个密钥块对应的功耗相关性曲线

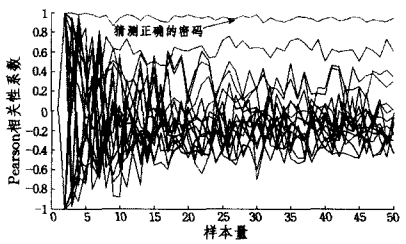

图 3　不同样本量某 4 位密钥块 16 个候选值对应的 Pearson 相关性系数

图 3 所示为不同样本量下猜测某 4 位密钥块值时，所有 16 个候选值对应相关功耗曲线的最大 Pearson 相关性系数图。其中，X 轴表示样本量大小，Y 轴表示 16 个候选值的 Pearson 相关性系数。可以看出在仿真环境下，当样本量大于 5 时，正确密钥块候选值对应相关功耗曲线的最大 Pearson 相关性系数在 16 个候选值中最大。

结束语　本文对 PRESENT 密码算法抗相关功耗分析能力进行了研究，提出了一种针对 PRESENT 分组密码的相关功耗分析方法，并通过仿真实验进行了验证。仿真实验表明，PRESENT 易遭受相关功耗分析威胁，通过对 5 个样本功耗曲线进行相关功耗分析，可恢复第一轮的 64 位密钥，结合密钥扩展方案得到 2^{16} 个 PRESENT 主密钥候选值，并进行暴力破解恢复 80 位 PRESENT 主密钥。为了避免这类攻击对密钥安全造成的威胁，需要对采用 PRESNET 的加密硬件及智能卡进行相应防护。因此，设计能够抵抗相关功耗分析的 PRESENT 密码算法电路是下一步的研究方向。

参 考 文 献

[1] ECRYPT. The Side Channel Cryptanalysis Lounge. http://www.crypto.ruhr-uni-bochum.de/en_sclounge.html,2010-4-15

[2] Kocher P, Jaffe J, Jun B. Differential Power Analysis [C]// CRYPTO '99. LNCS 1666. Springer-Verlag,1999:388-397

[3] Bogdanov A, Knudsen L R, Leander G, et al. PRESENT: An Ultra_lightweight BlockCipher[EB/OL]. http://www.ist_ubisecsens.org/publication/present_ches2007.pdf,2007-04-03

[4] Brier E, Clavier C, Olivier F. Correlation power analysis with a leakage model[A]// Joye M, Quisquater J J, eds. Cryptographic Hardware Embedded System-CHES 2004[C]. Volume 3156 of Lecture Notes in Computer Science. Springer-Verlag, 2004: 16-29

[5] 褚杰，丁国良，邓高明，等. DES 差分功耗分析攻击设计与实现[J]. 小型微型计算机系统，2007,11(11):2071-2073

[6] 李浪，李仁发，Sha E H-M. 安全 SoC 抗功耗攻击研究综述[J]. 计算机科学，2009,36(6):16-18

[7] 邬可可，李慧云，于峰崎. 对同步流密码设备的相关性功耗分析(CPA)攻击[J]. 高技术通讯，2009,19(11):1142-1147

(上接第 11 页)

[27] Peng Pai, Ning Peng, Reeves D S. On the secrecy of timing-based active watermarking trace-back techniques[A]// Proceedings of the 2006 IEEE Symposium on Security and Privacy (SP'06), 2006[C]. Berkeley, California, USA: IEEE Computer Society, 2006:334-349

[28] 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

[29] Jia Wei-jia, Tso F P, Ling Zhen, et al. Blind detection of spread spectrum flow watermarks[A]// Proceedings of the 28th IEEE International Conference on Computer Communications (Infocom'09), 2009[C]. Rio de Janeiro, Brazil: IEEE Computer Society, 2009:2195-2203

[30] Luo Xia-pu, Zhang Jun-jie, Perdisci R, et al. On the secrecy of spread-spectrum flow watermarks[A]// Proceedings of the 15th European Symposium on Research in Computer Security (ESORICS'10), 2010[C]. Athens, Greece: Springer, 2010:232-248

[31] Houmansadr A, Kiyavash N, Borisov N. Multi-flow attack resistant watermarks for network flows[C] // Proceedings of IEEE International Conference on Acoustic, Speech, and Processing (ICASSP'09). Taipei, Taiwan: IEEE, 2009:1497-1500

[32] Zhang Lian-cheng, Wang Zhen-xing, Wang Qing-long, et al. Msac and multi-flow attacks resistant spread spectrum watermarks for network flows[A]// Proceedings of 2010 2nd IEEE International Conference on Information and Financial Engineering (ICIFE'10), 2010[C]. Chongqing, China: IEEE, 2010:438-441

[33] Paxson V, Floyd S. Wide-area traffic: the failure of poisson modeling[J]. IEEE/ACM Transactions on Networking, 1995, 3(3):226-244

[34] Abry P, Veitch D. Wavelet analysis of long range dependent traffic[J]. IEEE Transactions on Information Theory, 1998, 44(1):2-15

[35] 邵立松，窦文华. 自相似网络通信量模型研究综述[J]. 电子与信息学报，2005,27(10):1671-1676