相对误差受限的数据流流量测量算法

张 进 赵文栋 彭来献 吴泽民
(解放军理工大学通信工程学院 南京 210007)

摘 要 数据流流量测量的精度采用错误概率和相对误差进行衡量。现有的流量测量算法主要关注如何降低错误概率,而对如何减小相对误差则缺乏研究。考虑到减小相对误差对于流量计费等应用的重要意义,提出了一种相对误差受限的数据流流量测量算法 MT-dlCBF(Multi-Tier *d*-left Counting Bloom Filter)。MT-dlCBF 由多层 dlCBF(*d*-left Counting Bloom Filter)构成,且随着层数的提高,dlCBF 中数据流指纹长度和流量计数器宽度也逐步增加,这样,可减轻长流对于短流的干扰,从而达到减小相对误差的目的。理论分析和仿真实验的结果表明,与 dlCBF 相比,MT-dlCBF 的错误概率略有增大,但相对误差显著减小。此外,在典型的参数条件下,MT-dlCBF 的空间效率略优于 dlCBF。

关键词 流量测量,布鲁姆过滤器,相对误差
中图法分类号 TP393 **文献标识码** A

Per-Flow Traffic Measurement Algorithm with Restrained Relative Error

ZHANG Jin ZHAO Wen-dong PENG Lai-xian WU Ze-min
(Institute of Communications Engineering, PLA University of Science & Technology, Nanjing 210007, China)

Abstract The accuracy of per-flow traffic measurement is evaluated using the metrics of both error probability and relative error. Current research on flow traffic measurement mainly focuses on reducing error probability, while little attention has been paid to alleviating relative error. Motivated by the importance of reducing relative error in certain applications such as usage accounting, this study presented a new algorithm named MT-dlCBF (Multi-Tier*d*-left Counting Bloom Filter) with restrained relative error. MT-dlCBF consists of several tiers of dlCBF (*d*-left Counting Bloom Filter), and dlCBF at higher tier has longer flow fingerprints and wider flow traffic counters than that of dlCBF at lower tier respectively. In this way, the interference of long flow to short ones can be alleviated significantly, resulting in restrained relative error. Analytical and experimental results show that MT-dlCBF provides significant decrement in relative error and trivial increment in error probability compared to dlCBF. Moreover, MT-dlCBF has higher space efficiency than dlCBF under typical parameter settings.

Keywords Traffic measurement, Bloom filter, Relative error

1 引言

网络流量分析是进行计费管理、业务控制、网络异常检测以及网络安全监测等网络管理工作的前提,所分析的流量数据中信息的丰富程度直接影响着上述网络管理工作的效果。随着网络业务环境的日益复杂和网络安全形势的日趋严峻,简单网络管理协议(SNMP)所提供的基于链路或者端口级的流量统计信息由于粒度太粗,已经不能满足当前诸多网络管理工作的需求。而随着网络数据率的飞速提升,若直接对原始的网络流量进行逐包的分析处理,又因其代价极高而不易实现。与端口级和数据包级的网络流量不同,数据流级的网络流量在所包含的信息量和所需处理的数据量之间达到了良好的平衡[1]。构成数据流级的网络流量的基本单位是流记录,其中包含数据流的流标识(通常采用"源 IP、目的 IP、源端口、目的端口、协议类型"五元组作为流标识)、开始时间、结束时间以及流量大小等信息。对数据包级的网络流量进行实时处理,以生成流记录,这一过程称为流测量(flow measurement)[1],其难点在于测量各条数据流的流量(per-flow traffic measurement),简称流量测量。

在高速 IP 网络中,数据包到达间隔短,且并发数据流的数目巨大,若直接进行流量测量,则实现代价极高。现有的骨干网流量测量算法从不同的角度来降低骨干网流量测量的代价,所采用的方法主要包括抽样法、长流法和近似法。抽样法随机抽取一些数据包,根据抽样结果对原始数据流的流量进行估计。当前,Cisco 的 Netflow 所采用的就是抽样法[2]。对于流量较大的数据流,抽样法可以获得较为准确的测量结果;而对于流量较小的数据流,抽样法往往会导致较大的测量误差,甚至漏测了许多流量较小的数据流。根据对网络流量进行采集分析的结果,网络数据流的流量大小服从 Zipf 分布,约 20%的长流,其流量之和占据了链路总流量的 80%[3]。长流法试图对流量较大的长流进行准确的测量,而忽略了流量小的短流。长流法和抽样法均侧重于对长流的测量,然而,对于网络异常检测、网络业务流分类而言,忽略短流会遗漏大量重要的信息。与抽样法和长流法不同,近似法试图对所有的

到稿日期:2012-08-30 返修日期:2013-01-06 本文受江苏省自然科学基金项目(BK2010103)资助。
张 进(1979—),男,博士,工程师,主要研究方向为网络测量、网络编码,E-mail:boost_zj@163.com。

数据流的流量进行测量，但是测量结果存在一定的误差。近似法又分为两类，第一类方法首先对流量值进行在线压缩，然后通过离线的解压过程，估算各条数据流的流量[4-8]。此类算法无法支持流量值的在线查询，称这类算法为被动式近似测量算法。另一类近似测量算法采用计数型布鲁姆过滤器[9,10]实现，可以支持流量值的在线查询，称这类算法为主动式近似测量算法。

如上文所述，近似测量算法的测量结果存在一定的误差，衡量测量精度的性能指标主要包括错误概率和相对误差。若某条数据流的流量的真实值为 f，测量值为 $\hat{f}$，则错误概率定义为 $\Pr\{f\neq\hat{f}\}$，相对误差定义为 $|f-\hat{f}|/f$。现有的有关近似测量算法的研究工作侧重于关注如何降低错误概率，而对于如何减小相对误差则缺乏研究。然而，在现实应用中，减小流量测量的相对误差也具有重要的意义。例如，在进行流量计费时，若某条数据流的真实流量为 1，测量值为 10^5，这是无法接受的。事实上，在很多应用场合中，可以接受较高的错误概率，但是无法容忍较大的相对误差[11]。基于上述原因，本文提出了一种相对误差受限的主动式近似测量算法 MT-dlCBF(Multi-Tier d-left Counting Bloom Filter)。与 dlCBF 相比，MT-dlCBF 能够显著降低较大相对误差的产生概率，其代价是错误概率略有提升(由第 3.2 节的分析结果可见，提升的相对幅度<1%)。此外，在典型的参数条件下，MT-dlCBF 的空间效率略优于 dlCBF。

2 算法设计

2.1 dlCBF 算法介绍

MT-dlCBF 由多层 dlCBF 构成，因此，首先对 dlCBF 的结构作介绍。dlCBF 将存储区划分为 d 个等长的块，每块包含若干个桶，每个桶又划分为若干个单元，一个桶单元存放一条数据流的流指纹和流量计数器。图 1 给出了 dlCBF 的结构示意图。图 1 中，dlCBF 的存储区划分为 $d=4$ 个块，分别是 BV_1、BV_2、BV_3 和 BV_4，每个块存储区中包含 5 个桶，每个桶中包含 4 个单元，桶单元用于存放数据流的流指纹和流量计数器，如图 1 所示。

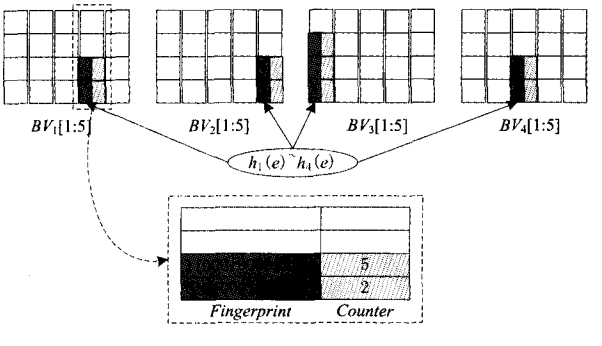


图 1 dlCBF 的结构示意图

dlCBF 更新操作的步骤如下：首先，根据数据流的流标识，不妨设其为 f，利用一个哈希函数 $H(\cdot)$，计算该数据流的流指纹，假设为 p，即 $p=H(f)$；然后，依次在桶 $BV_1[h_1(f)]$，$BV_2[h_2(f)]$，…，$BV_d[h_d(f)]$中进行查找，若某个桶中存放有和 p 一致的流指纹，则将对应桶单元的流量计数器增加 1，其中 $h_1(\cdot)$，$h_2(\cdot)$，…，$h_d(\cdot)$为 d 个哈希函数，用于计算数据流 f 在各个块中的桶地址；若 $BV_1[h_1(f)]$，$BV_2[h_2(f)]$，…，$BV_d[h_d(f)]$中均没有和 p 一致的流指纹，则表明数据流 f 是首次更新，此时，令其流量计数器值为 1，并将其流指纹 p 和流量计数器放入到 $BV_1[h_1(f)]$，$BV_2[h_2(f)]$，…，$BV_d[h_d(f)]$这 4 个桶中负载最轻的那个桶中去；若负载最轻的桶有多个，则选择最左边的那个桶。

dlCBF 查询操作的步骤如下：首先，根据流标识 f，计算得到流指纹 p；然后，依次在桶 $BV_1[h_1(f)]$，$BV_2[h_2(f)]$，…，$BV_d[h_d(f)]$中进行查找，将这 d 个桶中所有流指纹等于 p 的桶单元中的流量计数器累加起来，作为待查询的数据流的流量估计值。由于不同的流标识经过哈希运算可能产生相同的流指纹，因此，查询结果可能会产生错误。假设 dlCBF 共由 d 个块组成，平均桶负载为 b，流指纹长度为 p 比特，则 dlCBF 的错误概率为

$$P_e=1-(1-\frac{1}{2^p})^{d\cdot b}\approx\frac{d\cdot b}{2^p}$$

2.2 MT-dlCBF 算法描述

MT-dlCBF 由多层 dlCBF 构成，各层 dlCBF 的块数、桶深和平均桶负载一致，但桶的数目逐层减少(每层 dlCBF 所需的桶的数目的计算方法见第 2.1 节)。各层 dlCBF 中流指纹的长度和流量计数器宽度随着层数的提高而递增，如图 2 所示。第 $i(i\geqslant 1)$层 dlCBF 中，数据流指纹长度为 $2^{i-1}\cdot p$ 比特，流量计数器位宽为 $2^{i-1}\cdot c$ 比特。假设最大的流量值为 M，MT-dlCBF 中 dlCBF 的总层数为 T，则需满足 $2^{T-1}\cdot c\geqslant\lceil\log(M+1)\rceil$，因此，MT-dlCBF 的最小层数为

$$T=\lceil\log(\log(M+1)/c)\rceil+1 \quad (1)$$

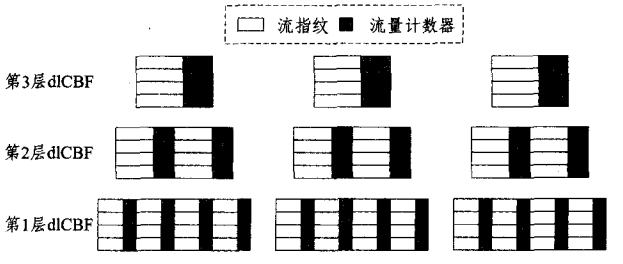


图 2 MT-dlCBF 的结构示意图

由于低层的 dlCBF 的流量计数器位宽较窄，因此，若数据流在低层的 dlCBF 中发生冲突，其相对误差的值也较小；随着层数的提高，流指纹的长度逐层增加，这就降低了高层 dlCBF 发生错误的概率，即，降低了产生较大的相对误差的概率。

MT-dlCBF 的更新操作的基本流程是从最低层的 dlCBF 开始，若发现其流量计数器等于溢出临界值，则转而更新更高一层的 dlCBF，如此递推，直至更新到某层 dlCBF 后，发现其流量计数器小于溢出邻居值，则将其流量计数器增加 1。对于第 i 层 dlCBF 而言，其流量计数器位宽为 $2^{i-1}\cdot c$，因此其溢出临界值为 $2^{2^{i-1}\cdot c}-1$；流量计数器的值一旦达到溢出临界值，则不再增加。

MT-dlCBF 的查询操作和更新类似，也是从最低层的 dlCBF 开始，并根据对当前层的查询结果，判断是否需要继续查询更高一层 dlCBF。设查询结果为 $\hat{C}$，查询开始时，$\hat{C}$初始化为 0；设查询第 i 层 dlCBF 的结果为 $\hat{c}_i$。查询操作从第 1 层 dlCBF 开始；查询完第 i 层 dlCBF 后，将 $\hat{c}_i$ 累加到 $\hat{C}$ 中；若 $\hat{c}_i$ 大于或者等于第 i 层的临界值 $2^{2^{i-1}\cdot c}-1$，则继续查询第 $i+1$

层，否则，结束查询，返回结果为$\hat{C}$。

3 性能分析

3.1 空间效率

定义 1(折叠系数) 称 $r=\frac{\lceil \log(M+1)\rceil}{c}$ 为流量计数器的折叠系数。

假设测量周期内共有 N 条数据流，其流量大小在区间 $[1,M]$ 内服从参数为 α 的 Zipf 分布，即，流量值 f 等于 $j(1\leqslant j\leqslant M)$ 的概率为

$$\Pr(f=j)=\frac{\theta}{j^{\alpha}} \tag{2}$$

式中，$\theta=(\sum_{j=1}^{M}j^{-\alpha})^{-1}$ 为归一化系数。假设第 i 层 dlCBF 中，数据流的数目为 N_i，令 $N_1=N$。数据流从第 1 层 dlCBF 溢出到第 2 层 dlCBF 中，可能有下列原因：(1)数据流的流量值大于或等于 2^c；(2)2 条或者更多条数据流发生冲突，其叠加起来的流量值大于或等于 2^c。需要注意的是，上述两种原因可能不是完全互斥的。在第 1 层 dlCBF 中，对于任意数据流 F 而言，F 和其他数据流发生冲突的概率即为第 1 层 dlCBF 的查询错误概率，设为 P_1^e。考虑到和 2 条数据流发生冲突的概率相比，3 条或者 3 条以上的数据流发生了冲突的概率极小，于是，有

$$N_2\approx N\cdot(\sum_{j=2^c}^{M}\frac{\theta}{j^{\alpha}}+2P_1^e) \tag{3}$$

式中，$N\cdot\sum_{j=2^c}^{M}\frac{\theta}{j^{\alpha}}$ 为流量值大于或等于 2^c 的数据流的数目，$N\cdot P_1^e$ 为在第 1 层 dlCBF 中发生冲突的数据流的数目，乘以系数 2 表示这些数据流在第 2 层 dlCBF 中均不再发生冲突，显然，这一假设是比较保守的。一般地，溢出到第 $i(i\geqslant 2)$ 层 dlCBF 中的数据流的数目为

$$N_i\approx N\cdot(\sum_{j=2^{2^{i-2}}\cdot c}^{M}\frac{\theta}{j^{\alpha}}+2P_{i-1}^e) \tag{4}$$

由于各层 dlCBF 的块数、桶深和平均负载率一致，且数据流指纹长度成倍递增，因此，有

$$P_i^e=2^{(1-2^{i-1})p}\cdot P_1^e \tag{5}$$

将式(5)带入式(4)，有

$$N_i\approx N\cdot(\sum_{j=2^{2^{i-2}}\cdot c}^{M}\frac{\theta}{j^{\alpha}}+2^{(1-2^{i-2})p}\cdot 2P_1^e) \tag{6}$$

于是，MT-dlCBF 所需的总空间为

$$\begin{aligned}S&=\sum_{i=1}^{T}2^{i-1}\cdot(p+c)\cdot N_i\\&\approx(p+c)\cdot N+\sum_{i=2}^{T}2^{i-1}\cdot(p+c)\cdot N\cdot(\sum_{j=2^{2^{i-1}}\cdot c}^{M}\frac{\theta}{j^{\alpha}}+2^{(1-2^{i-2})p}\cdot 2P_1^e)\\&\approx(p+c)\cdot N\cdot(1+\sum_{i=2}^{T}(2^{i-1}\cdot\theta\cdot\sum_{j=2^{2^{i-1}}\cdot c}^{M}\frac{1}{j^{\alpha}}+2^{(1-2^{i-2})p+i}\cdot P_1^e))\end{aligned} \tag{7}$$

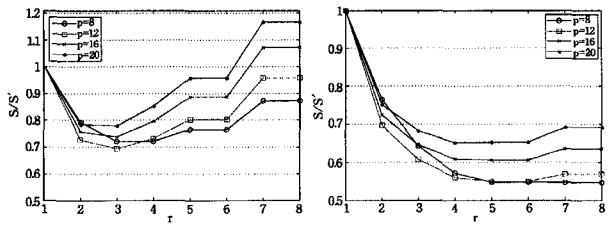
而 dlCBF 所需的总空间为

$$S'=N\cdot(p+2^{T-1}\cdot c) \tag{8}$$

S/S' 即为 MT-dlCBF 和 dlCBF 的空间之比。由式(1)和折叠系数的定义可知，$T=\lceil\log(r)\rceil+1$，代入式(7)和式(8)，即可得到 MT-dlCBF 和 dlCBF 的空间之比与 r 的关系

$$\frac{S}{S'}\approx\frac{p+c}{p+rc}\cdot(1+\sum_{i=2}^{\lceil\log(r)\rceil+1}(2^{i-1}\cdot\theta\cdot\sum_{j=2^{2^{i-2}}\cdot c}^{M}j^{-\alpha}+2^{(1-2^{i-2})p+i}\cdot P_1^e)) \tag{9}$$

图 3 为 $M=2^{20}-1$ 时，不同的 p 取值下，MT-dlCBF 和 dlCBF 的空间之比。图 3(a)中，Zipf 分布的参数 $\alpha=1.5$；图 3(b)中，$\alpha=2$。由图 3 可见，r 逐步增大时，S/S' 存在先减小、后增大的趋势，特别是图 3(a)中，这一趋势较为明显。这是因为 c 越小，则第 1 层 dlCBF 所需的空间越小，但是高层 dlCBF 所需的空间越大；反之，c 越大，则第 1 层 dlCBF 所需的空间越大，但是高层 dlCBF 所需的空间相对越小。因此，c 存在一个最佳取值，使得 MT-dlCBF 的总空间最小。对比图 3(a)和图 3(b)还可以发现，Zipf 分布的参数 α 越大，S/S' 随着 r 的增大而增加的趋势越不明显。这是因为 α 越大，意味着流量分布越不平均，大流量的数据流所占的比例越小，因而导致 MT-dlCBF 中高层 dlCBF 所需的空间越小。根据对实际网络流量的采集分析结果，真实网络流量的 α 取值在 1.5 到 2 之间[12]。因此，在设计 MT-dlCBF 时，可以假设 $\alpha=1.5$，对高层 dlCBF 的空间作较为保守的分配。



(a)$\alpha=1.5$　　(b)$\alpha=2$

图 3　$M=2^{20}-1$ 时，不同的 p 和 z 取值下，MT-dlCBF 和 dlCBF 的空间之比

3.2 错误概率

MT-dlCBF 在查询时，首先从第 1 层 dlCBF 开始，若发现第 1 层 dlCBF 的流量计数器发生溢出，则继续查询第 2 层 dlCBF，如此递推，直至查询到某层 dlCBF，发现其流量计数器没有溢出为止。查询的 dlCBF 的层数越多，则发生查询错误的概率越大。设第 i 层 dlCBF 的查询错误概率为 P_i^e，于是，MT-dlCBF 中，对于任意数据流，其查询错误概率的上限 $\overline{P_e}$ 为

$$\overline{P_e}=1-\prod_{i=1}^{T}(1-P_i^e) \tag{10}$$

式中，T 为 MT-dlCBF 的总层数。将式(5)代入式(10)，得

$$\overline{P_e}=1-\prod_{i=1}^{T}(1-2^{(1-2^{i-1})p}\cdot P_1^e) \tag{11}$$

由于 $P_1^e>P_2^e>\cdots>P_T^e$，且 $P_2^e\approx 0$，于是有

$$\begin{aligned}\overline{P_e}&=1-\prod_{i=1}^{T}(1-P_i^e)\\&<1-(1-P_1^e)(1-P_2^e)^{T-1}\\&\approx 1-(1-P_1^e)(1-(T-1)P_2^e)\\&=P_1^e+(T-1)P_2^e-(T-1)P_1^eP_2^e\\&<P_1^e+(T-1)P_2^e\end{aligned} \tag{12}$$

由式(12)可见，$\overline{P_e}$ 和 dlCBF 的错误概率 P_1^e 非常接近。令

$$\overline{P_e}'=1-\prod_{i=1}^{\infty}(1-2^{(1-2^{i-1})p}\cdot P_1^e) \tag{13}$$

显然，$\overline{P_e}'>\overline{P_e}$。图 4 给出了不同的 p 取值下，$\frac{\overline{P_e}'-P_1^e}{P_1^e}$ 的数值计算的结果。由图 4 可见，和 dlCBF 相比，MT-dlCBF 的错误

概率的相对增加幅度非常有限，例如，当 $p=10$ 时，MT-dlCBF 的错误概率相对于 dlCBF 仅仅增加了约 0.1%，在实际应用中，如此小的相对增长幅度可以忽略不计。此外，由图 4 可见，随着 p 增加，$\frac{\overline{P_e}'-P_1^e}{P_1^e}$ 呈指数下降（注意，图 4 的纵坐标是对数坐标），这一结果同样可以由式(12)解释，由于

$$\frac{\overline{P_e}'-P_1^e}{P_1^e}\approx\frac{\overline{P_e}-P_1^e}{P_1^e}\approx\frac{P_1+(T-1)P_2^e-P_1^e}{P_1^e}=\frac{(T-1)P_2^e}{P_1^e} \tag{14}$$

由式(5)可知，$P_2^e=2^{-p}\cdot P_1^e$，代入式(14)，得

$$\frac{\overline{P_e}'-P_1^e}{P_1^e}\approx(T-1)2^{-p} \tag{15}$$

需要指出的是，上文中我们分析的是错误概率的上限，考虑到实际应用中大部分网络数据流的流量较小，只有少部分数据流才会溢出到第 2 层以及更高层的 dlCBF 中，因此，MT-dlCBF 的平均错误概率小于 $\overline{P_e}$。

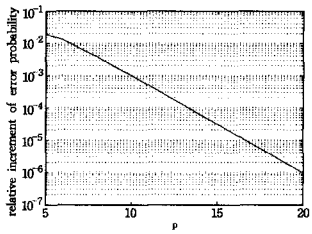


图 4　MT-dlCBF 的错误概率相对于 dlCBF 的错误概率的增长幅度

4　仿真实验

本节采用真实的骨干网流量数据，对 MT-dlCBF 的性能进行仿真分析，并和 dlCBF 进行比较。实验所采用的流量数据来源于 CAIDA 所提供的 Abilene-I 和 Abilene-III 骨干网流量数据，前者采集自 OC-48 链路，后者采集自 OC-192 链路，分别称为 OC-48 Trace 和 OC-192 Trace。实验数据的详细信息见表 1。

表 1　实验所采用的骨干网流量数据的详细信息

名称	持续时间	总包数	总流数	最大流长	平均流长
OC-48 Trace	583.778s	33367912	255607	806428	130.5
OC-192 Trace	264.745s	28468064	599898	1983653	47.5

图 5 给出了 OC-48 Trace 和 OC-192 Trace 中数据流的流量分布的 CCDF 曲线。作为对比，图 5 同时还给出了在区间 $[1,2\times10^6]$ 内，α 分别取 1.5 和 2 的 Zipf 分布的 CCDF 曲线。由图 5 可见，用 Zipf 分布对实际网络数据流的流量分布进行建模时，参数 α 取值在 1.5 到 2 之间。

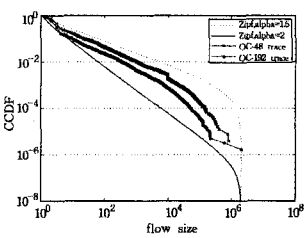
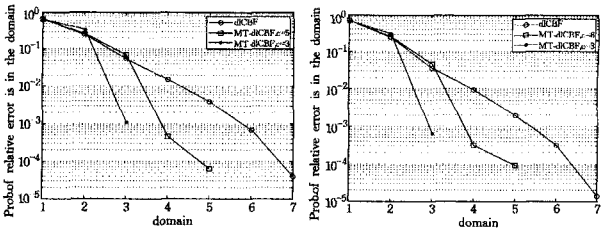


图 5　所采用的真实流量数据中流量大小的分布

图 6 给出了 MT-dlCBF 和 dlCBF 的相对误差概率分布曲线。图 6 中，横坐标为区间号，第 1 个区间的覆盖范围为(0,1]，第 2 个区间的覆盖范围为(1,10]，第 3 个区间的覆盖范围为(10,100]，…，第 7 个区间的覆盖范围为(10^5，$+\infty$)；纵坐标为相对误差 R 落在第 i 个区间内的概率。图 6(a)为采用 OC-48 Trace 进行仿真实验的结果，图 6(b)为采用 OC-192 Trace 进行仿真实验的结果。图 6 中，dlCBF 的块数取 $d=4$，桶深设为 4，平均桶负载设为 3，流指纹长度为 8。对于 OC-48 Trace，其最大流长为 806428，故设置 dlCBF 中流量计数器位宽为 20 比特；对于 OC-192 Trace，其最大流长为 1983653，故设置 dlCBF 中流量计数器位宽为 21 比特。



(a) OC-48 Trace　　(b) OC-192 Trace

图 6　MT-dlCBF 和 dlCBF 的相对误差的概率分布

由图 6 可见，随着区间序号的增大，MT-dlCBF 的相对误差落在区间中的概率明显小于 dlCBF，当区间序号增大到一定程度时，MT-dlCBF 的相对误差落在该区间中的概率为 0（由于纵坐标采用的是对数坐标，因此概率为 0 的点在图 6 中没有显示出来）。可见，与 dlCBF 相比，MT-dlCBF 具有更小的相对误差。另外，由图 6 还可以看出，最大流量值 M 一定时，c 值越小，则 MT-dlCBF 的相对误差越小。这一结果很容易解释，因为 c 越小，则低层 dlCBF 的计数范围越小，因此低层 dlCBF 的最大相对误差越小；而随着层数的提高，流指纹长度逐步增加，发生测量错误的概率也越来越小，这就极大地抑制了大的相对误差的产生概率。

结束语　本文提出一种相对误差受限的主动式网络数据流量近似测量算法 MT-dlCBF。与现有的主动式近似测量算法相比，在同等测量错误概率下，MT-dlCBF 能够将相对测量误差控制在较小的范围内，从而使得测量结果具有更好的公平性。此外，在典型的参数条件下，MT-dlCBF 算法的空间效率略优于 dlCBF 算法。MT-dlCBF 算法尤其适用于流量计费、业务流 QoS 保障等对于相对误差较敏感的场合。

参 考 文 献

[1] Trammell B, Boschi E. An introduction to ip flow information export[J]. IEEE Communications Magazine, 2011, 49(4): 89-95

[2] Systems C. NetFlow [OL]. http://www.cisco.com/web/go/netflow

[3] Estan C. New Directions in Traffic Measurement and Accounting[C]//Proc. of ACM Sigcomm. 2002: 323-336

[4] Kumar A, Xu Jun. Space-Code Bloom Filter for Efficient Per-Flow Traffic Measurement[C]//Proc. of IEEE Infocom. 2004: 315-328

[5] Lu Yi, Montanari A, Prabhakar B. Counter Braids: A Novel Counter Architecture for Per-Flow Measurement[C]//Proc. ACM SIGMETRICS. 2008: 121-132

[6] Lu Yi, Prabhakar B. Robust Counting Via Counter Braids: An Error-Resilient Network Measurement Architecture[C]//Proc. IEEE Infocom. 2009: 522-530

[7] Lieven P, Scheuermann B. High-Speed Per-Flow Traffic Measurement with Probabilistic Multiplicity Counting[C]//Proc. of IEEE Infocom. 2010: 1253-1261

(下转第 118 页)

个 20 欧的电阻，通过探头连接电阻的两端，将电压信号传送给示波器进行采集，然后转换为密码芯片的功耗，并通过 USB 传输到 PC 机存储，示波器的采集过程由 PC 机上用 LabView 编写的虚拟仪器控制平台实现自动控制，整个控制流程为：

1)控制平台首先为 FPGA 密码芯片注入密钥；

2)通过 RS232 接口为密码芯片提供随机明文输入；

3)当密码芯片进行 RSA 迭代加密算法时，触发示波器记录电阻两端的功耗输出(采样频率为 250MHz，每条轨迹共采样 10000 个点)，并控制示波器实时向 PC 机传输功耗数据。

通过上述过程测得该密码芯片在加密迭代过程中的功耗波形如图 1 所示。

图 1　加密迭代过程中的功耗波形

图 1 为 AES 算法在执行第一次迭代过程中的 S 盒运算的功耗曲线，在每一个采样发生时刻，该波形的功耗值均服从正态分布，由于 AES 算法在执行过程中，第一次迭代的 S 盒运算所泄露的功耗信息常常被 DPA 攻击所利用[8]，因此衡量该过程熵的增长速度具备更高的实际意义。

通过大量的统计工作，并依据式(5)，近似得到该密码芯片在某一采样时刻功耗量的分布 z 服从参数为(5.4，0.3)的正态分布，状态转移矩阵 P 如图 2 所示。

$$\bar{X}=\frac{1}{n}\sum_{i=1}^{n}X_i,\ s^2=\frac{1}{n-1}\sum_{i=1}^{n}(X_i-\bar{X})^2 \tag{6}$$

1	2	3	4	5	6	7	8	9	10
0.04	0.07	0.09	0.12	0.2	0.18	0.12	0.1	0.06	0.02
0.01	0.06	0.1	0.14	0.21	0.19	0.1	0.12	0.05	0.02
0.02	0.04	0.08	0.15	0.23	0.2	0.13	0.07	0.04	0.04
0.04	0.09	0.07	0.12	0.18	0.2	0.1	0.12	0.05	0.03
0.03	0.06	0.07	0.13	0.22	0.16	0.14	0.09	0.07	0.03
0.05	0.06	0.08	0.14	0.23	0.19	0.12	0.08	0.03	0.02
0.02	0.04	0.08	0.15	0.23	0.2	0.13	0.07	0.04	0.04
0.04	0.07	0.09	0.12	0.2	0.18	0.12	0.1	0.06	0.02
0.03	0.06	0.07	0.13	0.22	0.16	0.14	0.09	0.07	0.03
0.01	0.06	0.1	0.14	0.21	0.19	0.1	0.12	0.05	0.02

图 2　密码芯片门级翻转数量的转移矩阵

图 2 描述了该密码芯片在采样时刻顺序推移的过程中，门级翻转个数的变化，并以转移矩阵的形式表现出来。

依据定理 2，我们计算得到该密码芯片在加密过程中功耗波形的熵率为 2.733，该值表示密码芯片在加密过程中，功耗波形的熵随机器时间以 2.733 的速率近似线性地增长，同时在相对意义下可以衡量密码芯片抵御功耗攻击的能力，因为功耗波形的熵越大，就表示其不确定性越大。如果某密码芯片的熵率较高，则在相同的机器周期内其产生功耗波形的熵值就越大，因此，攻击者要获得特定的功耗数据就会越困难，所以抵御功耗攻击的能力越强。

结束语　本文在前人研究成果的基础上，提出了基于熵率的密码芯片抵御功耗攻击能力的量化方法，依据该方法可以宏观地量化密码芯片在加密迭代运算时熵随时间的增长速度，并动态地衡量密码芯片在功耗攻击下的防御能力。实验结果证明，熵率值的大小主要是依据门级翻转数量的概率分布，同时我们也知道，在均匀分布下，随机变量的熵将会达到最大值，使密码芯片在加密迭代运算过程中的门级翻转数量接近均匀分布，这将会极大地提高密码芯片抵御功耗攻击的防御能力。

参 考 文 献

[1] 吴克辉. 基于汉明重的 PRESENT 密码代数旁路攻击[J]. 计算机科学，2011，12(38)：53-56

[2] 姚剑波. 层次化的侧信道攻击风险量化评估模型[J]. 计算机工程与应用，2011，11(3)：131-133

[3] 姚剑波，张涛. 基于互信息博弈的侧信道攻击安全风险评估[J]. 计算机科学，2012，6(39)：69-71

[4] JoyeM，Paillier P，Schoenmakers B. On second-order differential power analysis[C]//Proc of Cryptograph ic Hardware and Embedded Systems (CHES 2005)，LNCS 3659. Springer-Verlag，2005：293-308

[5] 童元满. 基于细粒度任务调度的防功耗分析模幂方法[J]. 计算机工程，2006，32：31-33

[6] Veyrat-Charvillon N，Standaert F-X. Mutual information analysis：how，when and why? [C] // The Proceedings of CHES 2009，Lausanne，Switzerland，September 2009. Lecture Notes in Computer Science，vol. 5747，Springer，Berlin，2009：429-443

[7] Standaert F-X，Veyrat-Charvillon N，Oswald E，et al. The world is not enough：another look on second-order DPA[C]//The Proceedings of Asiacrypt 2010，Singapore，December 2010. Lecture Notes in Computer Science，vol. 6477. Springer，Berlin，2010：112-129

[8] Rivain M，Dottax E，Prouff E. Block ciphers implementations provably secure against second-orderside-channel analysis[C]// The Proceedings of FSE 2008，Lausanne，Switzerland，February 2008. LectureNotes in Computer Science，vol. 5086. Springer，Berlin，2008：127-143

(上接第 83 页)

[8] Li Tao，Chen Shi-gang，Ling Yi-bei. Fast and Compact Per-Flow Traffic Measurement through Randomized Counter Sharing[C]// Proc. of IEEE Infocom. 2011：1799-1807

[9] Fan L，Cao P，Almeida J，et al. Summary Cache：a Scalable Wide-area Web Cache Sharing Protocol [J]. IEEE/ACM Transactions on Networking，2000，8(3)：281-293

[10] Bonomi F，Mitzenmacher M，Panigrahy R，et al. An Improved Construction for Counting Bloom Filters[C]//Proc. of European Symposium on Algorithms. 2006：678-680

[11] Tsidon E，Hanniel I，Keslassy I. Estimators Also Need Shared Values to Grow Together[C]//Proc. IEEE Infocom. 2012：1390-1398

[12] 周明中. 大规模网络 IP 流行为特性及其测量算法研究[D]. 南京：东南大学，2006. 8