基于 CERNET 主干信道的 IP 流数据 Trace

史冰，丁伟，高亚东，龚俭
(东南大学 计算机科学与工程学院，江苏 南京 210096)

摘 要：主干互联网的 IP 流数据对研究互联网具有重大价值，但实际公布的这类数据量很少，尤其是没有经过抽样处理的原始数据，原因主要在于主干信道采集难度大和 IP 地址隐私等方面。以 CERNET 一个省网边界（1G×3）采集的 1 个小时的连续的 IP 报头为原始数据，依据相应的省网 IP 地址构成的特点与实际需求，对 IP 地址前缀保留匿名化算法 Crypto-PAn 进行了改进，在提高实现效率的基础上保留了地址类型，用改进后的算法将上述原始数据进行了相应的处理，并将结果在互联网上公布，供有关研究下载。

关键词：IP 流；IP 地址；前缀保留；匿名化；加密算法
中图分类号：TP393 **文献标识码**：A **文章编号**：1000-436X(2006)11A-0214-05

IP Trace data based on a CERNET backbone

SHI Bing, DING Wei, GAO Ya-dong, GONG Jian
(School of Computer Science & Engineering, Southeast University, Nanjing 210096, China)

Abstract: The Internet traffic trace data based on backbone links has significant value for research, but only a very small percentage of this kind of data especially the raw data not sampled are available, the reason mainly lies in two: it's very hard to collect the trace of backbone channel and IP address concerns users' privacy. One hour IP packet header was continually collected at Jiangsu province border (1G×3) of CERNET as the primary data, according to the characteristic of IP address constitution and the actual demand, prefix preserving IP address anonymous algorithm Crypto-PAn was optimized to enhance the efficiency and retain the address types. Finally, the improved algorithm was used to deal with the above primary data and published the result on the Internet for research downloading.

Key words: IP flow; IP address; prefix preserving; anonymization; encryption algorithm

1 引言

基于高速主干互联网的 IP 流数据对研究网络是非常重要的，但目前只有 ISP 和为数不多的互联网科研机构才有条件采集到主干网络的 IP 流数据。IP 流数据中有网络用户的 IP 地址、通信内容等隐私信息，如果不加处理或处理不当就将 IP 流数据向外界公布，势必会侵犯网络用户的隐私权或商业秘密。为满足研究者需求，尽管个别研究机构如 NLNAR[1]、CAIDA[2]、WIDE[3]、LBNL[4]、ACM[5] 对外公布了少量 IP 流数据，但基于主干网的 IP 流数据仍然十分匮乏，网络研究人员不得不利用仿真的方法产生基于主干网的实验数据，这与真实互联网数据之间存在很大差别，势必造成研究结果与实际情况之间有偏差，进而影响到研究结果的正确性和准确性。

为此，CERNET 华东（北）地区网络中心在国家重点基础研究发展计划（“九七三”计划）课题

收稿日期：2006-10-09
基金项目：国家重点基础研究发展规划基金资助项目(“九七三”计划) (2003CB314804)
Foundation Item: The National Basic Research Program of China (973 Program) (2003CB314804)

“网络动态行为和传输控制理论”的支持下，完成了一个基于分光器的分布式千兆信道采集系统 Watcher[6]，它能在连续时间内，以低丢包率对双向全部 IP 报文头部实时采集，同时采集器之间能够进行时钟的同步。在这个系统的支持下，我们于 2005 年 11 月 10 日在江苏省网边界到 CERNET 骨干网之间的光纤主干线路上采集到了 24 小时 IP 流数据（当时的拓扑是 1G×3），采集的长度为报文的前 60 个字节，附加信息包括时戳和流向标志等，具体数据格式如图 1 所示，数据总量 2.5TB。根据采集前对系统的测试，丢包率为 2%。

在采集完成后，已根据时戳完成了对数据的归并整理，并已在这些数据上开始进行有关的研究工作。由于数据量非常庞大，虽然将其全部公布是不可能的，但我们希望能够将其中的关键时段在互联网上公布，使这些宝贵的数据资源能够发挥更大的作用。作为国际惯例，在 IP 流数据公布之前要对其进行净化处理，IP 流净化处理是在最大程度保持流数据原来特性不改变的基础上，将数据中涉及网络用户隐私信息的内容消除或匿名化。

目前已有很多通用的处理 IP 地址的算法，但为了顾及宏观通用性，这些算法在完成匿名功能的同时也失去了原始地址的一些微观特性，如地址类型等，因此，本文首先根据原始数据所涉及的地址范围的特点，对一个通用的算法 Crypto-PAn[7,8]算法进行改进，使其更适合于原始数据的微观特征，然后将该算法作用于一个小时的连续时间段的 IP 流数据，并将处理后的 trace 公布在 ftp://202.112.25.22/Public/20051110pub/上。

2　净化的原则

IP 流净化的指导原则是最大程度保持流数据原来特性不改变和最大程度保护网络用户的隐私，主要进行以下三个方面的工作：首先，将 IP 地址匿名化，其次，消除数据中的用户通信内容，最后，重新计算 IP 头中的校验和。

IP 流净化的核心内容是 IP 地址匿名化。CIDR 利用 IP 地址前缀来识别网络，取代了地址分类，路由器是基于 IP 地址最长前缀匹配的转发算法来工作的，前缀关系是 IP 地址间的路由关系和聚类关系的体现。为保证 IP 流最大程度地保持原有特性，地址匿名化采用前缀保留的方法。

有效载荷是网络用户通信内容的实体，如图 1 所示，这部分内容不能出现在发布的数据里面，因此要消除，只保留时戳和完整的头部信息。

校验和是潜在的不安全信息。校验和的计算方法[9]是用首部中每个 16 比特进行二进制反码求和得到的，因此，如果首部只有 IP 地址字段的值发生了改变，为了防止对猜测到的 IP 地址进行验证，需利用匿名化后的 IP 地址重新计算 IP 首部的校验和。

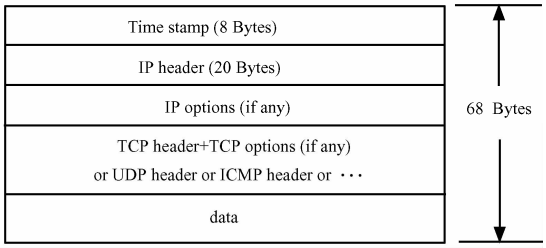

图 1　Watcher 系统采集的原始数据格式

3　原始数据 IP 地址范围特征

为有效合理利用地址空间，减少路由信息，江苏省网根据网内用户特点将 C 类地址的 16 比特前缀作为网络号，16 比特后缀作为主机号来分配和使用 IP 地址，这种地址聚类方式限制了主干路由中路由信息的增长，减少了路由查询和路由波动变化。数据采集时，省网地址集中在 202～222 的网段中，对原始数据中出现的源、宿 IP 地址进行分析，报文数量对应的 I P 地址分布情况如图 2 所示。

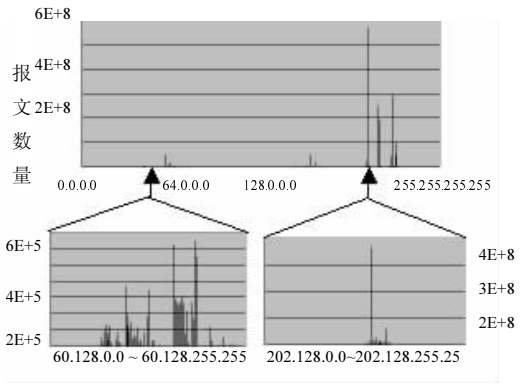

图 2　原始数据集中 IP 地址对应的报文数量分布

原始数据集表现出两个明显的特征：一是地址类型分布不均，报文数量在各地址类型中所占的比重分别为：A 类占 7.59%，B 类占 1.65%，C 类占 90.76%，D 类接近 0%，E 类为 0%。二是区间分布不均，90%以上的报文分布在江苏省网的地址范围 202～222 地址区间内。

4 净化算法

路由器基于 IP 地址前缀最长匹配实现一个一致的转发算法，因而前缀保留的 IP 地址匿名化算法能保持 IP 地址间的路由关系和前缀聚类关系这种特性。另外，原始数据是分别存储在不同的存储器上，为保证 IP 地址匿名化结果的一致性，要求算法具有分布式并行处理能力。Crypto-PAn 采用 Rijndael[10, 11]加密算法作为随机函数构造了一个能够实现 IP 地址前缀保留的匿名化函数，只要选择相同的密钥，相同 IP 地址的匿名化结果是一致的，可以应用在并行和分布式环境下，非常适合 Watcher 系统流数据的 IP 地址匿名化。

4.1 Crypto-PAn 算法简介

IP 地址 $a=a_1a_2\cdots a_n$，文献[1]中利用 Rijndael 加密算法构造的匿名化函数 $F(a):= a_1'a_2'\cdots a_n'$。其中

$a_i'=a_i \oplus f_{i-1}(a_1a_2\cdots a_{i-1})$，$i=1,2,\cdots,n$

f_i 是 $\{0,1\}^i$ 到 $\{0,1\}$ 的函数，L 表示最高位比特，R 表示 Rijndael 加密算法，P 为填充函数，K 为密钥，则 f_i 可以表示为：$f_i(a_1a_2\cdots a_i):=L(R(P(a_1a_2\cdots a_i),K))$

Crypto-PAn 匿名化函数可以用二叉树表达，原地址空间用一棵完整的二叉树表示，匿名化函数是在地址树的某些节点上进行翻转，图 3 所示为匿名化函数树的前 4 比特。

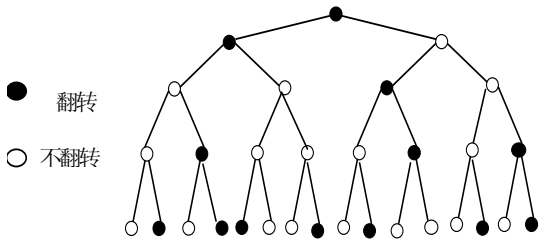

图 3 匿名化函数树

Rijndael 分组长度和密钥长度均可独立地设定为 32 比特的任意倍数，最小 128 比特，最大 256 比特，匿名化过程中先对填充串进行加密，用加密后的填充串作为真正的填充串。给定一个 IP 地址，依次取它的前 0，1，2,…,31 比特前缀，用填充串将其扩展至 128 比特，然后分别对其加密，得到 32 个 128 比特的密文，每个只取其第 1 比特位，按照由高位到低位的顺序得到一个 32 比特的匿名化树节点序列，翻转节点用“1”表示，不翻转的节点用“0”表示。将这个 32 比特的序列与原来的 IP 地址 a 按位异或就得到匿名化后的 IP 地址 a'。

4.2 改进的 Crypto-PAn 算法

从原始数据集的特征来看，数据具有明显的地址类型分布和区间分布特征，因而 Crypto-PAn 在处理该数据集过程中势必存在大量重复计算的现象，其计算复杂度有可以降低的空间。Crypto-PAn 实现了地址前缀保留，但 IP 地址原来的 ABCDE 类型没有保持，破坏了地址类型分布的特征。不涉及用户隐私权的私有地址、组播地址、本机回路测试地址也进行了匿名化，并且这些地址以外地其它地址也有可能匿名化成这些地址。此外，原始数据地址分布主要集中在江苏省网范围内，因此，对 Crypto-PAn 算法的改进基于下面三点考虑：一是在不影响安全性能的前提下降低其时间复杂度，二是净化后的流数据保留尽可能多的微观信息，如地址类型和一些特殊的地址，三是使改进后的算法更能适应原始数据特征。

改进后的算法将 IP 地址的 16 比特前缀和 16 比特后缀的匿名化是分开进行。预先计算所有 IPv4 地址匿名化后的前 16 比特，并将结果保存在内存中，匿名化过程中，只对 IP 地址的 16 比特后缀进行计算，然后在预先计算好的 16 比特前缀中查找对应的结果，最后将两者结合成一个完整的 IP 地址。此外，算法保留了地址类型和不涉及用户隐私的地址。最后，算法消除了有效载荷的内容，并根据匿名化后的 IP 地址值重新计算了 IP 首部的校验和。

1) 预先计算。Crypto-PAn 是对地址每个比特分别进行匿名化函数计算的，不管相同前缀或相同的 IP 地址出现过多少次，Crypto-PAn 都对其重新进行匿名化，90%以上的报文分布在 202～222 地址区间内，因而存在重复计算相同前缀的情况。如果将所有地址匿名化后的值提前计算好，可以解决重复计算问题，但同时又会出现另外的情况：所有 IPv4 地址所需内存空间是 32×2^{32}bit=16.38GB，显然是不可行的。如果在对地址匿名化之前仍用 Crypto-PAn 算法预先计算 IP 地址匿名化后的 16 比特前缀，所需内存空间只有 16×2^{16}bit=128MB，不仅更符合省网对地址分配特点，而且可以解决一部分的重复计算问题。对 IP 地址 16 比特后缀的计算也是按照 Crypto-PAn 原来的方法从原 IP 地址的第 17 位逐位进行，然后将预先计算的 16 比特前缀与之结合起来，从而完成整个匿名化过程。从改进后的匿名化过程可以看出，预先计算没有降低

Crypto-PAn 算法的安全性，但大大提高了实现的效率。如图 4 所示，在 PIII Xeron700GHz×2CPU，2G 内存的 Linux 操作系统上，选择 256 位密钥，Crypto-PAn 处理能力为 20,044 个报文 / 秒，采用预先计算的 Crypto-PAn 处理能力达 34,764 个报文 / 秒。

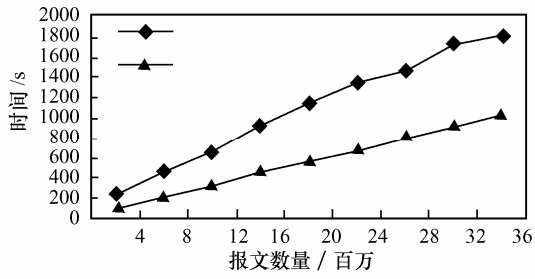

图 4　实验结果对比

2) 地址类型保留。在分类的网址体系中，地址类型标识位从最高位开始的第 1 到 4 位，如 A 类地址的最高位是“0”。CIDR 利用 IP 地址前缀来识别网络，相同类型的 IP 地址必然有若干位相同的前缀，为了能保持匿名化前后的 IP 地址类型不发生变化，则需要对地址类型标识位进行保留，对 Crypto-PAn 匿名化过程进行修改，相应匿名化函数的前若干位保持为 0，如 A 类地址最高位比特不进行匿名化过程，匿名化函数仍保持为“0”不变，即匿名化过程依次取它的前 1，2，…,31，其余的步骤按上面的操作方法进行。其它类地址与此类似。

3) 保留不涉及用户隐私的地址。私有地址、组播地址、本机回路测试地址、全 0 和全 1 的地址不涉及用户隐私权，对上述地址不进行匿名化。预先计算的另一个作用是可以由 IP 地址的 16 比特前缀判定私有地址、组播地址、本机回路测试地址，以实现保留这些地址不进行转换。

预先计算可以在地址类型保留的前提下进行，将这些不需要匿名化的地址集合记为 H，将 H 以外的 IP 地址集合记为 L，F 为匿名化函数。H 中的地址不进行匿名化处理，但要进行预先计算。为防止 H 以外的地址匿名化后映射到 H 空间上来，按照下面的办法处理：x∈L，F(x)=y，若 y∈H，则 y 匿名化后 F(y)=z，一定满足 z∈L，则 x 匿名化的最终结果取 F(x)=z。

5　结果数据

用改进后的算法在 Xeron2.4GHz×2CPU，2G 内存的 Linux 操作系统上，将 2005 年 11 月 10 日 19 时至 20 时一个小时的数据净化处理，该数据共 159GB，包含 2343875720 个报文，处理耗时 47 643s。

数据在经过 IP 地址匿名化、消除有效载荷内容、重新计算校验和后，可以安全地对外公布。净化后的数据只保留时戳和完整的头部信息，数据格式如表 1 所示。TCP 数据包长度为 48 字节，UDP、ICMP 等数据包为 36 字节，如果 IP 首部含有选项内容，则保留的长度依据选项字段的长度相应增加。

表 1　　公布的 IP 流数据格式

时戳	报文头(TCP)	时戳	报文头(UDP)	…
8 字节	40 字节	8 字节	28 字节	…

先期公布的数据中，每个文件存储 3 百万个报文，文件以该 3 百万个报文中第一个报文的到达时间命名，以二进制格式存储，数据总量 110GB，以压缩包的形式发布。

6　结束语

真实的主干互联网流数据对网络研究具有重要的价值，但数据中的隐私信息要在净化后才能被研究使用，本文根据原始数据集的特征和 IP 流净化的实际需要对 IP 地址匿名化算法 Crypto-PAn 进行了改进，不仅在保证数据安全的前提下提高了算法执行效率，而且使净化后的 IP 流数据最大限度地保持了 IP 流数据的原有特性。最后，本文公布了净化处理后的 IP 流数据。

参考文献：

[1] The Passive Measurement and Analysis [EB/OL]. http://pma.nlanr.net/Traces/, [2005]2006-5-10.

[2] The Cooperative Association for Internet Data Analysis[EB/OL]. http://www.caida.org/data/, 2006-5-10.

[3] Measurement and Analysis on the WIDE Internet [EB/OL]. http://tracer.csl.sony.co.jp/mawi/, [1999]2006-5-9.

[4] Lawrence Berkeley National Laboratory and The International Computer Science Institute [EB/OL]. http://www.icir.org/enterprise-tracing /download.html, [2005]2006-3-11.

[5] Association for Computing Machinery [EB/OL]. http://ita.ee.lbl.gov/index.html, [2000]2006-3-22.

[6] Watcher1.0 总体设计手册[R].东南大学计算机科学与工程学院江苏省网络技术重点实验室，2004.7.
Watcher1.0 system design handbook [R]. School of Computer Science

and Engineering, Southeast University, Jiangsu Province Key Lab of Computer Networking Technology.2004-7.

[7] XU J, FAN J, AMMAR M H, *et al.* Prefix-preserving IP address anonymization: measurement-based security evaluation and a new cryptography-based scheme[J]. Computer Networks, 2004,46(2):253-272.

[8] Cryptography-based Prefix-preserving Anonymization[EB/OL] http://www.cc.gatech.edu/computing/Telecomm/cryptopan/, 2005-7-1.

[9] BRADEN R, BORMAN D, PARTRIDGE C. RFC1071,Computing the internet checksum.[EB/OL]. New York:IETF. http://www.ietf.org/rfc/rfc1071.txt?number=1071, 1988-9[2006-6-8].

[10] DAEMEN J, RIJMEN V. 高级加密标准(AES)算法 Rijndael 的设计[M]. 北京：清华大学出版社, 2003,31-52.
DAEMEN J, RIJMEN V. The design of Rijndael AES:the advanced encryption standard [M].Beijing:Tsinghua University Press. 2003,31-52.

[11] DAEMEN J, RIJMEN V. AES Proposal: Rijndael[R]. 1999-3-9.

[12] PANG R, ALLMAN M, PAXSON V, *et al*. The devil and packet trace anonymization[J]. Computer Communication Review, 2006, 36(1):29-38.

作者简介：

史冰（1975-），男，山东汶上人，东南大学硕士生，工程师，主要研究方向为网络行为学。

丁伟（1962-），女，江苏南京人，东南大学教授、博士生导师，主要研究方向为网络行为学、计算机体系结构。

高亚东（1982-），男，江苏盐城人，东南大学硕士生，主要研究方向为网络行为学。

龚俭(1957-)，男，上海人，东南大学教授、博士生导师，主要研究方向为大规模网络的入侵检测、网络行为学、计算机体系结构。