# 网络数据报文捕获技术的应用与分析

吕伟泽
（大庆油田信息技术公司北京分公司，北京 100043）

摘 要 首先针对数据报文捕获技术概念与工作特征以及应用环境展开分析，然后以当前在该领域中的主要技术，以及未来发展方向作为重点加以讨论，对于切实加强关于网络数据报文捕获技术的认识有着一定的积极意义。
关键词 网络；报文捕获；应用；特征
中图分类号 G2 文献标识码 A 文章编号 2096-0360（2015）03-0046-02
DOI:10.16604/j.cnki.issn2096-0360.2015.03.023

在信息时代之下，人们的生活和工作都开始融入大量数据。数据一方面使得整个社会的运行效率大幅度提升，另一个方面，其所必然带来的整个社会对于数据的依赖，进一步加剧了数据安全问题的紧迫性。并且随着整个网络环境中数据传输需求的不断增加，网络环境中的数据安全问题和安全信息过滤需求也日渐突出，这种需求特征在企业环境中尤其突出，如何打造安全可靠的内部网络环境，并且实现面向外网的流畅访问，是目前的突出问题。

## 1 数据报文捕获技术概念与特征

对于目前的网络安全需求而言，网络带宽不断提升，数据传输速率和容量都有了质的飞跃，对应的万兆网络防火墙系统、入侵检测/防御系统、高性能路由器、千兆级网络实时监控系统、高带宽的网络审计系统等技术层出不穷，本身成为当前网络安全体系中重要的支持框架，尤其是在面对大流量网络环境的时候，其价值尤其得到体现。但是诸多安全技术的基础，都在于网络数据报文捕获技术网络应用，作为当前网络安全应用最基本的功能模块之一，网络数据报文捕获技术的成熟与发展状态，直接关系到网络安全环境上层的诸多应用有效性，因此必须引起重视。

综合当前网络环境的发展特征，随着光纤造价成本的降低以及相关技术的不断成熟，传统的10Mbps共享局域网环境已经在近年来迅速升级到100 Mbps乃至于1 000 Mbps数据传输环境，对应地网络环境中的数据流量同样有大幅提升，甚至于在骨干网络中，Gbit传输速率已经不足为奇。这些都为数据报文捕获技术提出了新的挑战。

从应用层面看，对于网络安全应用系统的工作方式，可以依据其对于现有网络的参与状况分为监听模式和过滤模式两类。其中监听模式也称为并联工作模式，其网络应用系统并不完全参与既有网络环境的工作，而是在一个旁观者的位置上对数据展开抓取和处理。此种工作方式本身不会对网络环境的工作状态有所影响，但是数据是直接从公网进入到局域网环境中的，因此此种工作方式对于报文的检测，相对而言存在一定的滞后特征，但是却不会对网络环境中的数据传输造成任何效率方面的影响。而过滤模式又称为串联工作模式，从外网进来的数据首先要进入到网络安全应用系统中展开检查和过滤，而后才能进一步发送给内部局域网使用和传输。常规而言的防火墙、代理网关、路由器等均是采用这一工作模式，此种模式安全性能要优于前者，但是在数据量增加的环境之下，其相关安全应用系统自身的运算处理能力将成为整个网络传输环境的瓶颈存在。

相比之下，监听模型式不占用网络资源，数据报文的捕获和后续操作不会对网络正常通讯产生任何影响；而过滤工作模型中，网络安全应用必须能够做到快速大量地面向数据包展开处理和过滤，否则就会面临数据包丢失乃至于系统锁死的尴尬局

作者简介：吕伟泽，工作单位为大庆油田信息技术公司北京分公司。

面。鉴于当前过滤模型是主要的应用方式，因此数据报文捕获技术作为网络安全应用系统的关键环节，其工作效率和可靠程度成为当前行业内部关注的重点。

## 2 数据报文捕获技术的主要应用与发展方向分析

在Unix系统环境下，数据报文捕获技术存在于数据链路层，就当前的应用状况看，常见的报文处理技术包括三种，即BSD分组过滤器（BPF，Berkeley Packet Filter）、SVR4的数据链路提供者接口（DLPI，Data Link Provider Interface），以及Linux的SOCK-PACKET接口。三种技术均有不同的应用特征。

首先对于BPF技术而言，其工作在整个系统的内核层面，在内核环境中展开了过滤器的设置，在对数据包展开对应的过滤之后，将用户需要的数据提交给用户进程。在相应的工作系统中，每一个数据链路的对应驱动程序在展开对于一个分组的处理时，都首先调用BPF。为了提升效率，BPF采用循环缓存工作机制，两个缓存交替展开工作，并且采用基于寄存器的过滤器，这对于当前内存系统已然成为整个系统性能核心瓶颈问题，无疑是一种缓解。其次，SVR4的DLPI展开工作时，其本身会保持对于协议的相对独立状态，并且其本身时访问数据链路层所提供服务的接口，通过发送和接受信息来实现具体功能。DLPI接口定义了数据链路层面向网络层提供服务的具体规则，其使用者既可以是面向用户的应用程序，也可以是访问数据链路层的高层协议，相对于BPF技术而言，该项技术的表现从整体效率方面比较低。而最后的SOCK-PACKET接口技术则主要通过设置套接字类型以及数据类型来展开工作，但是它没有类似于BPF的强缓冲区，在内核过滤器方面也有所欠缺，因此整体效率都受到极大制约，对于当前相对比较重视网络效率的环境而言，存在显著不足。

就目前在网络数据报文捕获技术体系中的突出应用特征而言，数据丢包、用户态和内核态之间的数据包拷贝以及内核中断处理已经成为当前的突出不足。基于此种问题，当前在报文捕获技术的相关发展领域，其主要方向也都围绕这些问题展开。

首先，充分利用网络处理器，实现对于报文捕获的加速，是当前发展的突出特征之一。网络处理器能够在工作环境中切实实现对于网络数据采集方面的功能效率，在实时的报文捕获和深入分析方面表现良好，并且并联的工作方式出现在被监控的网络环境中，也能够支持其实时特征较强的高效率网络环境。其次，零拷贝技术也是当前发展的突出特征，对于这一方面而言，其基本思想和实现方式是将数据报文的拷贝次数尽量压缩和减少，主要是在从网络设备到用户程序空间传递的过程中注重拷贝次数的缩减，同时注重减少CPU的参与程度，降低其负载。

## 3 结论

网络数据报文捕获系统的整体工作状态和效率，直接关系到当前网络环境的安全水平，因此必须引起充分重视。作为多种网络安全应用的基础，报文捕获技术的优化以及性能的提升，是大容量网络得以深入发展的基础，实际工作中应当以当前需求作为依据展开对于技术的优化，才能切实找到该项技术的发展方向。

参考文献

[1]王佰玲，方滨兴，云晓春，等.零拷贝报文捕获平台的研究与实现[J].计算机学报，2005，28（1）.

[2]张承，蒋东兴，刘启，等.新浅析网络监控系统对网络性能的影响[J].小型微型计算机系统，2002，23（09）.