第 26 卷第 4 期 河 北 科 技 大 学 学 报 Vol. 26, No. 4
2005 年 12 月 Journal of Hebei University of Science and Technology Dec. 2005

文章编号: 1008-1542(2005)04-0316-06

基于 Snort 的入侵防御系统的技术研究和实现

王志伟, 郭文东

(河北科技大学 经济管理学院, 河北石家庄 050018)

摘 要: 针对网络安全防御问题, 论述了入侵防御系统的 2 种体系结构——网络 IPS 和主机 IPS, 介绍了防火墙和 PS 之间互动的实现方式。通过将 Snort 安装为内嵌模式, 利用 snort-inline, 结合内嵌式互动技术和外联式互动技术, 设计并实现了一种基于 Snort 的具备了初步入侵防御功能的原型系统。

关键词: IPS; IDS; 防火墙; Snort

中图分类号: TP393.08 文献标识码: A

Research on intrusion prevention system based on Snort and its implementation

WANG Zhi-wei, GUO Wen-dong

(College of Economics and Management, Hebei University of Science and Technology, Shijiazhuang Hebei 050018, China)

Abstract: Focusing on the problem of network security prevention, this paper has discussed two kinds of system structure of intrusion prevention system(IPS) such as as network intrusion prevention system (NIPS) and host-based intrusion prevention system(HIPS), and has made an introduction to the implementation between the IPS and the firewall. Through installing the Snort inline, utilizing snort-inline, and combining the inline interaction technology and outside uniting interaction technology, this paper has designed and realized a prototype system, which is based on Snort and possesses the preliminary function of intrusion prevention.

Key words: IPS; IDS; firewall; Snort

网络安全是一个系统的概念, 有效的安全策略或整体解决方案的制定是网络信息安全的首要目标。传统上用户一般采用防火墙作为网络安全的第 1 道防线, 入侵检测系统(Intrusion Detection System, IDS)作为第 2 道防线[1]。但近一段时间的网络安全事件, 从 MS-SQL Slammer 大爆发到蠕虫、震荡波病毒发作, 都对网络造成了巨大的破坏, 单纯的防火墙加入侵检测策略已经无法满足对安全高度敏感部门的需要。因此, 从 IDS 与防火墙的联动结合发展起来的入侵防御系统(Intrusion Prevention System, IPS)脱颖而出, 它是网络安全领域为弥补防火墙及入侵检测系统的不足而新兴的计算机信息安全技术。不同的 IPS 实现的方式各不一样, 但其共同点是综合了防火墙防御功能和入侵检测系统的网络数据包检测功能, 紧密实现 2 个安全设备的联动, 从而对受保护网络进行更为完善的保护。

1 IPS 概述

IPS 是指不但能检测入侵的发生, 而且能通过一定的响应方式, 实时中止入侵行为的发生和发展, 实时

收稿日期: 2005-05-31; 修回日期: 2005-09-07; 责任编辑: 李 穆
基金项目: 河北省科技攻关项目(042135110)
作者简介: 王志伟(1982-), 男, 河北平山人, 硕士研究生, 主要从事管理信息系统方面的研究。
© 1994-2011 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

保护信息系统不受实质性攻击的一种智能化的安全产品, 它是目前网络安全技术领域中正在兴起的安全技术。

与 IDS 一样, IPS 根据部署方式也可分为 2 大类[2]: 网络 IPS(NIPS) 和主机 IPS(HIPS)。

1) 网络 IPS, 也被称作内嵌式网络 IDS(in-line IDS) 或者是 IDS 网关(GIDS), 其更像是 NIDS 和防火墙的结合体, 和防火墙一样串联在数据通道上, 有 1 个进口和 1 个出口, 有些产品可能多加 1 个监控口以进行维护和数据交换。

不同厂商设计的 IPS 产品可能各有特色, 但大多数网络 IPS 都由探测器和管理器组成。探测器包括流量分析器、检测引擎、响应模块、流量调整器等主要部件, 其组成见图 1。

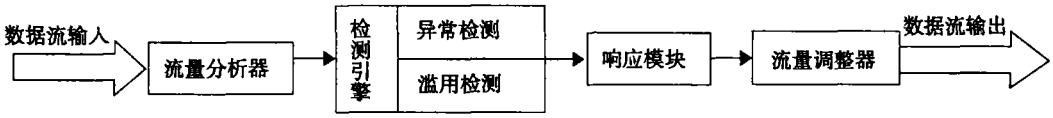

图 1　探测器的组成

Fig. 1　Constitution of detector

2) 主机 IPS, 其安装在受保护系统上, 与操作系统相结合, 监视系统状态, 防止非法的系统调用[3]。

主机 IPS 一般都采用"沙箱(sandbox)"技术检测入侵行为, 即允许用户定义规则, 以确定应用程序和系统服务的哪些行为是可接受的, 哪些是违法的, 跟 IDS 中的异常检测有些相似。例如: 管理员可在 IPS 的规则中规定 IIS 进程不得删除任何注册表项或 Windows 系统文件, 因此 IIS 每次进行系统调用时都会被截获并禁止执行。

主机 IPS 一般都由代理和数据管理器组成, 见图 2。代理驻留在被保护的主机上, 截获系统调用并进行检测和阻断, 然后通过可靠的通信信道与管理器连接。管理器主要有 2 个功能: ①报警, 告知管理员攻击的详细信息及是否被成功阻断等; ②执行一些管理任务, 如为各个代理设置规则、定义防御参数等。代理首先要截获系统调用或者系统消息, 然后才能进行检测和做出阻断响应。

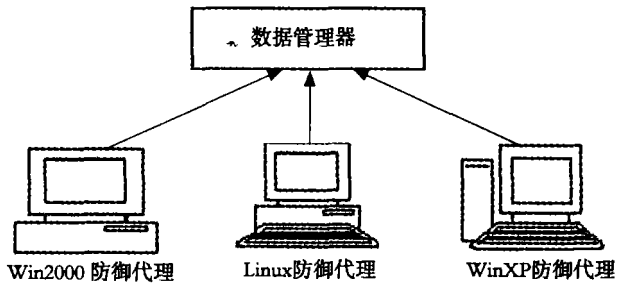

图 2　主机 IPS 的组成

Fig. 2　Constitution of HIPS

2　防火墙和 IPS 之间互动的实现方式[4]

在目前的网络安全防御体系中, 防火墙与 IDS 之间可以实现互动, 从而实现系统的安全, 比较典型的互动接口协议有 Check Point 公司的 OPSEC 和天融信公司的 TOPSEC。同样, 防火墙和 IPS 产品之间的互动有以下 2 种方式。

1) 通过开放接口实现互动　即防火墙或者 IPS 产品开放一个接口供对方调用, 按照一定的协议进行通信、传输警报。这种方式比较灵活, 防火墙可以行使它第 1 层防御功能 ——访问控制; IPS 可以行使它第 2 层防御功能 ——检测入侵, 丢弃恶意通信, 确保这个通信不能到达目的地, 并通知防火墙进行阻断。

此外, 通过开放接口实现互动不影响防火墙和 IPS 产品的性能, 对于 2 个产品的自身发展比较好。但是, 由于是 2 个系统的配合, 所以要重点考虑防火墙和 IPS 产品互动的安全性。在目前的技术水平上, 这种方式是最有可能实现的。

2) 紧密集成实现互动　即把 IPS 技术与防火墙技术集成到同一个硬件平台上, 在统一的操作系统管理下有序地运行, 其工作流程见图 3。

这种方式实际上是把 2 种产品集成到一起, 所有通过这个硬件平台的数据不仅要接受防火墙规则的验证, 还要被检测判断是否有攻击性, 以达到真正的实时阻断。对于这种紧密集成的安全平台, 由于 IPS 产品和防火墙本身都是很庞大的系统, 所以实施的难度比较大, 集成后的性能也会受很大的影响。

此外, 这种安全平台与"胖防火墙"的概念有着本质的区别。后者是以防火墙功能为主, 其他的安全功能

© 1994-2011 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

只是作为一种补充,它在本质上还是防火墙;而前者是将防火墙、IDS、防病毒和脆弱性评估等技术的优点与自动阻止攻击的功能融为一体,由紧密集成方式实现互动的动态防御。

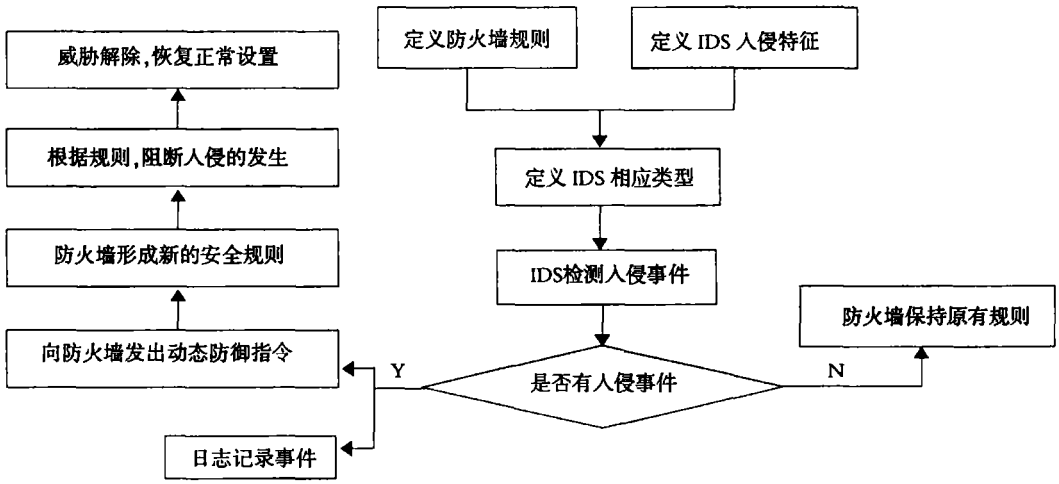

图 3 动态防御流程图

Fig. 3 Flow chart on dynamic prevention

3 基于 Snort 的入侵防御系统的设计与实现

IPS 与 IDS 的主要区别就是自动阻断攻击。由于 Snort 在整体结构上充分利用了插件机制,这种特点使它更灵活,更便于系统功能的增加,使程序具有很强的可扩展性。利用 Snort 的这种内部组织结构和 IPS 的特点,可以设想,只要为 Snort 增加一个能够阻断数据包的模块(假设称该模块为"在线处理模块"),并把 Snort 置于在线的位置,当 Snort 检测到入侵时通过对该模块的调用,就可以达到阻断含有入侵倾向数据流的目的。而由于有了 Hogwash 项目,Snort 具有了内嵌式 IDS 的功能。该原型系统将通过安装内嵌模式的 Snort,从而使系统实现初步的入侵防御功能。

3.1 安装 Snort 为内嵌模式

在内嵌模式下运行 Snort,人们必须为系统提供内嵌网络连接的能力,这意味着必须将 IDS 作为桥的某种形式运行。可以使用 2 种方式实现:一是将系统作为正常的网桥;二是转发数据包同时提供网络地址转换功能。这里笔者将运行系统作为正常的网桥。图 4 显示了以内嵌模式连接到 Internet 的简单网络系统[5]。

在内嵌模式下安装 Snort 的软件要求如下。

1) Red Hat 8.0 Linux 系统 它是以 Linux-2.4.18-14 内核为基础的 Linux 系统,编译包含 Netfilter 架构。Netfilter 提供了一个抽象、通用化的框架,该框架定义的子功能能够实现状态包过滤子系统、NAT 系统、内核数据包拷贝等防火墙的基本功能。

2) IPTables-1.2.7a.tar.bz2 它是源码公开的基于状态的防火墙子系统,该程序配置防火墙规则,基于笔者定义的链表检查每个数据包,同时提供 Libpcap 库函数的实现。下述命令将通知编译器内核的目录,安装 IPTables 并安装 Snort 内嵌补丁要求的 Libipq 库。

```
make KERNEL_DIR= /usr/src/linux-2.4.18-14
make install KERNEL_DIR= /usr/src/linux-2.4.18-14
make install-devel
```

3) Libpcap-0.7.1.tar.gz 它是一个针对 Linux 系统的包捕获库。该库的特别之处在于它既可以捕获发往本地主机的包,也可以截获发往网络上其他主机的包。

4) Libnet-1.0.2 它是一个通用网络 API,提供了一些协议的接口,实现和封装了数据包的截获等有关过程的函数库。

5) Bridge-utils-0.9.6.tar.gz 是实现 Linux 的网桥的软件包,使 Linux 防火墙工作在网桥模式下。

© 1994-2011 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

6) Bridge-nf-0. 0. 7-against-2. 4. 19. diff. txt　它是 Linux 的桥模式补丁, 这将使 Red Hat 8。内核同时执行桥和防火墙的功能。安装补丁的命令如下。

patch -pl < bridge-nf-0. 0. 7-against-2. 4. 19. diff

7) Mysql　入侵检测数据的存储数据库。

8) Snort-inline-2. 0　它是实现入侵防御功能的关键, 该软件使用 Snort 2. 0作为高效、稳定的内核。

9) Snort-inline. tgz　它是 Snort 的内嵌补丁, 只有安装了该软件, 才能使 Snort 工作在内嵌模式下。

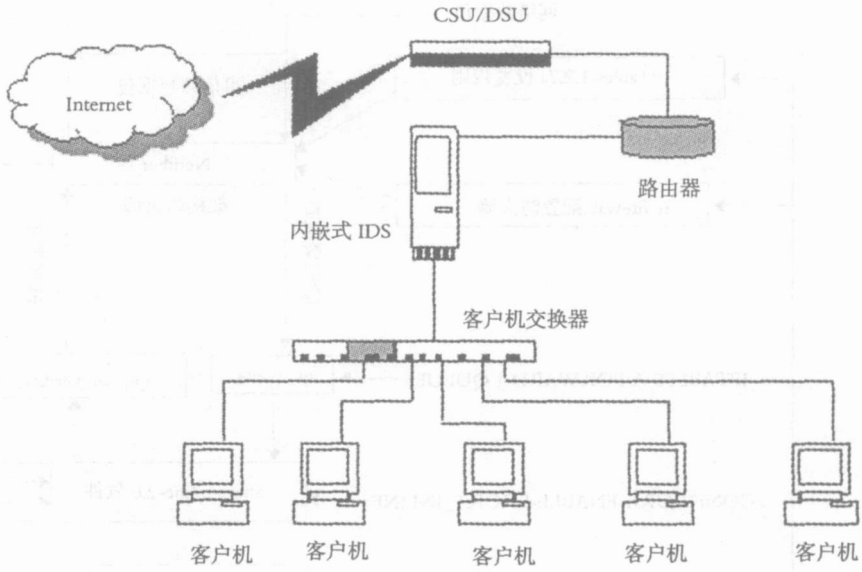

图 4　内嵌网络图

Fig. 4　Diagram of in-line network

10) Snortrules-current. tar. gz　它是 Snort 的规则, 应该安装最新的 Snort 规则, 然后在 OptTreeNode (规则选项) 结构中增加 2 个标志位: reject 和 drop。

11) rc. firewall　它是 rc. firewall 脚本, 配置了该软件后, 将使 Snort 和防火墙可以交互。

除此之外, 笔者还编写了外联式的输出插件, 将根据特定的报警, 通过 IPTables 添加防火墙的规则, 从而阻断入侵数据的通道。

3. 2　系统的架构

本 IPS 由事件分析单元(IPS_ANL)、响应单元(IPS_RSP)、审计单元(IPS_FAU) 和管理控制单元(IPS_MAN) 构成。

1) 事件分析单元(IPS_ANL)　其由 Netfilter, IPTables, ip_queue 内核模块、netlink 接口、libipq 库、Snort-inline-2. 0 程序及其规则集构成, 采用相关的分析检测技术, 对经过的信息进行分析, 提取信息中所包含的事件特征。

2) 响应单元(IPS_RSP)　其由 libipq 库、IPTables 和 Netfilter 钩子程序构成, 根据定义的策略对事件分析单元发送的消息进行响应。它有 4 种响应手段: 记录、报警、阻断和丢弃。

3) 审计单元(IPS_FAU)　其由 Mysql 数据库构成, 在违反安全策略的事件发生时, 对事件发生的时间、主体和客体等信息进行记录和审计。

4) 管理控制单元(IPS_MAN)　其由笔者编写的接收策略中心配置的 Iptables 规则和 Snort-inline 规则构成, 对其进行配置后, 负责 IPS 的定制策略、审阅日志以及系统状态管理, 同时控制整个系统的运作。

3. 3　系统实现原理

图 5 显示了本 IPS 的整体工作流程[6]。

本 IPS 的工作原理是: 将 Snort 以在线的工作方式安装后, 通过 rc. firewall 脚本改变使用 IPTables 的方式, 并且配置防火墙, 调用 IPTables 配置防火墙规则。基于笔者定义的链表检查每个数据包, 同时提供 Libpcap 库函数的实现; 然后实时的从 Netfilter 中通过 Libpcap 库函数截取网络数据包, 并且通过 ip_queue 内核模块和 netlink 接口, 将网络数据包从内核态读取到用户态。如果网络数据包是可信源的数据包, 就直接让它通过该检测系统, 减少检测的匹配负载, 从而提高系统的性能。Snort-inline-2. 0 使用 libipq 库, 通过 netlink 接口从内核态的 Netfilter 的 QUEUE 数据队列中获取数据包, 进行规则匹配, 它将通过模式匹配和

© 1994-2011 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

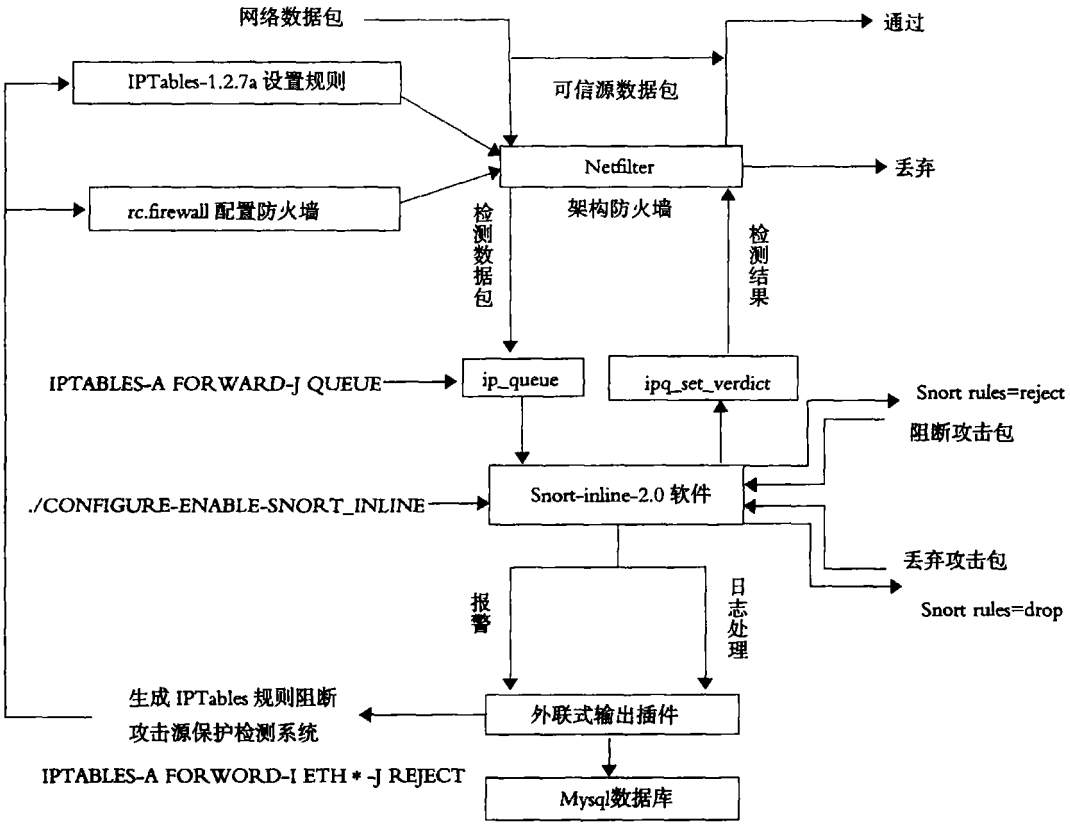

图 5 IPS 整体流程图

Fig. 5 Whole flow chart on IPS

状态检测技术进行检测。如果被捕获的数据包与某规则相匹配,说明 Snort 已经发现攻击行为,通过 libipq 库函数 ipq_set_verdict 经 netlink 接口与 Netfilter 通讯,并且判断该规则的选项树节点(OptTreeNode, OTN)结构中 2 个标志位的值。如果 drop 为 1,则调用在线处理模块,丢弃该包并输出报警信息。如果 reject 为 1,调用在线处理模块,阻断该包,输出报警信息。假如该包的协议类型为 TCP,则向数据源发送 RESET 报文,终止该连接;假如协议类型是 UDP,则向数据源发送 ICMP 端口不可达报文,终止该连接,同时通知数据库组件记录该攻击事件。如果匹配失败,则由 Netfilter 根据 rc.firewall 和 IPTables 配置的防火墙规则进行相应处理。与此同时,外联式输出插件经过判别如果发现系统渗透、大规模拒绝服务攻击、非授权访问等安全威胁,将通过一定的联动协议将阻断要求传递到防火墙端,通过 IPTables 生成相应的防火墙规则,从而实现入侵源数据通道的封堵,以达到降低匹配次数、较少报警、保护 IPS、提高系统性能的目的。

3.4 性能评估

经过试验,该原型系统能够有效地阻断测试的多种攻击,达到了设计的目的。该方法简单、灵活,不需要改动整体结构和 Snort 原有的规则,只是在其原有的系统和规则的基础上给 PV 结构和 OptTreeNode 结构增加了几个标志位,只需要为之添加 IPTables 底层库和 Libnet,增加一些函数即可实现。而且这种设计方法会根据不同的攻击级别做出不同的处理,减少了因为误报而阻断一个合法的数据包的可能性。但是在试验中笔者也发现:由于采用 ip_queue 内核模块和 netlink 接口,将网络数据包从内核态读取到用户态,延缓了数据的处理速度,降低了网络速度,而且也给系统的安全带来了不稳定性,所以仍然需要对系统继续进行研究、改进和完善。

4 结束语

IPS 有望结束防火墙、IDS、漏洞扫描与评估、防病毒等安全产品间彼此孤立、缺少联动的分裂局面。正如其名称所蕴含的那样,IPS 具有检测入侵和对入侵做出反应 2 项功能,可以说是将防火墙、IDS 系统、防病

© 1994-2011 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

毒和脆弱性评估等技术的优点与自动阻止攻击的功能融为了一体。尽管在技术上仍有很多未克服的问题,但正如攻击技术不断发展一样, IPS 也会不断更新、成熟。

参考文献:

[1] DESAI, NEIL. Intrusion Prevention Systems: the Next Step in the Evolution of IDS[EB/OL]. http://securityfocus.com/printable/infocus/1670, 2003-02-27.

[2] TED H. Understanding IPS and IDS: Using IPS and IDS Together for Defense in Depth[EB/OL]. http://www.sans.org, 2004-02-23.

[3] 宋献涛, 纪　勇. 网络防护: 从 IDS 到 IPS[J]. 计算机安全, 2003, (11): 26-28.

[4] 崔晓垣. 网络入侵防御系统研究[J]. 信息安全与通信保密, 2005, (3): 109-111.

[5] CASWELL B, BEALE J. Snort 2.0 Intrusion Detection[M]. 宋劲松译. 北京: 国防工业出版社, 2004. 367-386.

[6] 卿　昊, 原宏春. 入侵防御系统(IPS)的技术研究及其实现[J]. 通信技术, 2003, (6): 101-103.

(上接第 **311** 页)

表 1　获取的曲线上部分坐标值

Tab.1　Part of coordinates of the curve

横坐标(时间/s)	1.094	1.797	2.734	4.492	5.898	6.367	...
纵坐标(位移/mm)	0.168	0.170	0.173	0.175	0.178	0.180	...

比较图 6 与原始曲线图 1 可以看出,通过获得的坐标值重新绘制的图线与原扫描图线符合得非常好,应用坐标值计算的结果也准确地反映了实验结果。

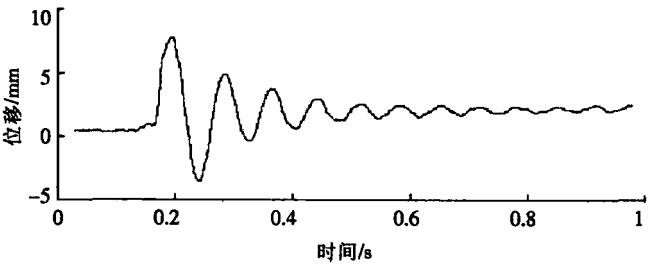

图 6　通过获取的坐标值重绘的图线

Fig.6　Redrawing image of coordinates

3　结束语

通过上述图形数字化的过程可以看出,这种方法与计算机图像处理紧密结合,取点密集,返回坐标值精确度高,且整个过程可以通过 MATLAB 语言自动完成,比人工取点的方法省时,省力,实验数据处理误差小,是一种实用、快捷的实验图形数字化方法。

参考文献:

[1] 张宜华. 精通 MATLAB5[M]. 北京: 清华大学出版社, 1999.

[2] 陈桂明, 张明照, 戚红雨. 应用 MATLAB 语言处理数字信号与数字图像[M]. 北京: 科学出版社, 2000.

[3] HARALICK R M, SHAPIRO L G. Survey: image segmentation[J]. Computer Vision Graphics Processing, 1985, 129: 100-132.

[4] 潘　峰, 刘文予, 朱光喜. MATLAB 在图像处理与研究中的应用[J]. 计算机应用研究, 1999, 16(12), 73-75.

© 1994-2011 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net