

ACL 技术研究及应用

杨 梅^{1,2}, 杨平利¹, 宫殿庆¹

(1. 西北核技术研究所, 陕西 西安 710024;

2. 西安交通大学 电信学院 计算机系, 陕西 西安 710049)

摘 要:访问控制列表是路由交换设备的一组条件控制指令列表,是实现包过滤技术的核心内容,它是一种数据流分类和过滤技术,在网络安全中发挥着重要的作用;访问控制列表也是一种服务级别协定,用于支持和提高网络的服务质量。首先介绍了访问控制列表的定义、分类、工作原理和功能,其次以实例的方式给出了访问控制列表的几种典型应用,通过应用实例说明了访问控制列表在网络安全中具体使用方法和特点,最后给配置使用时的要点、规则和使用时的建议。

关键词:访问控制列表;服务级别协定;路由器;IP/TCP 协议

中图分类号:TP393

文献标识码:A

文章编号:1673-629X(2011)06-0145-05

Access Control List Technology Studying and Application

YANG Mei^{1,2}, YANG Ping-li¹, GONG Dian-qing¹

(1. Northwest Institute of Nuclear Technology, Xi'an 710024, China;

2. Dept. of Computer, School of Electronic and Information Engineering,

Xi'an Jiaotong University, Xi'an 710049, China)

Abstract: Access control list (ACL) refers to the dictation list of router joint, which forms an orderly condition collection by a group of permit an deny sentences to control the data package of controlling the port turnover. ACL is a technology, which uses data stream classification and filtration to improve network's security. ACL is also a service level agreement (SLA), which is used to enhance the quality of service in network. Introduce in detail about ACL's conception, classification, principle and function. The typical applications are discussed in some cases, which display the method of how to use ACL. It also presents the matching principle and some advice to reduce making mistakes when use the ACL.

Key words: access control list; service level agreement; router; IP/TCP protocol

随着计算机和网络技术的高速发展,网络规模日益庞大,网络应用越来越多,网络规模和应用的不扩大和提升将网络的安全提到了重中之重的位置^[1]。网络安全是一个比较广泛的概念,通常可用划分VLAN、设置访问控制列表、加防火墙等方法实现网络的安全控制;访问控制列表作为网络安全中的一项重要技术,与硬件防火墙配合使用可周密细致地实现网络防控与管理。

1 访问控制列表介绍

1.1 访问控制列表的概念和功能

访问控制列表 (Access Control List, 以下简称

ACL) 是一种有序的语句集^[2]。它基于在路由交换设备接口上设置的规则与报文进行匹配,然后根据匹配结果确定允许或拒绝报文流的通过。

ACL 主要应用在路由交换设备的指令列表和操作系统中,它是客户端和网络服务提供者之间协商的一种服务级别协定 (Service Level Agreement, 简称 SLA)^[3],用于支持和提高网络的服务质量。

1.2 访问控制列表基本原理

从工作过程上看,ACL 是一种经由路由交换设备对数据包进行判断、分类和过滤的技术。使用包过滤技术,在路由交换设备上读取第二层、第三层及第四层数据包头中的信息并将这些信息和预先设定的规则对包进行比较和过滤,根据比较的结果确定对数据包进行转发或者丢弃,从而达到访问控制的目的。一个数据包由接口进入路由交换设备后,首先察看路由表,看包的目的地是否在路由表条目中,在则根据路由表送至相应的接口,否则将数据包丢弃;当数据到达相应的接口后,查看接口上是否有 ACL 配置,有则根据

收稿日期:2010-11-26;修回日期:2011-02-28

基金项目:国家研究计划项目 (ZZYJS 17050901);银河-5 深度并行计算机系统项目 (18051001)

作者简介:杨 梅 (1976-),女,陕西子长人,硕士研究生,工程师,研究方向为计算机及应用。

ACL 的规则, 比对数据报文, 判断是否允许该数据包通过, 如果不符合 ACL 所有规则, 就不能通过设备被丢弃, 如果没有配置 ACL, 数据包直接通过。ACL 工作流程如图 1 所示。

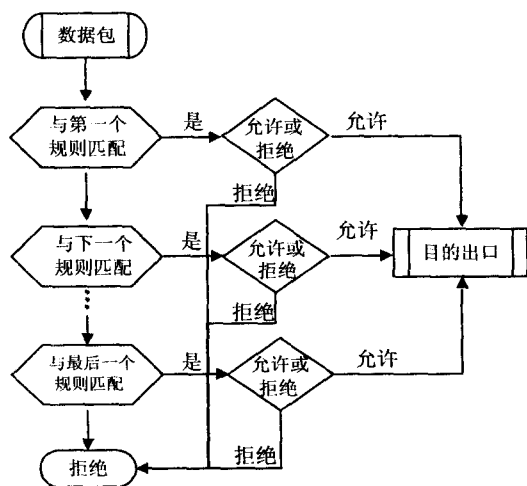


图 1 访问控制列表工作流程图

从协议支持方面, ACL 通过因特网协议 (Internet Protocol, 简称 IP) 和传输控制协议 (Transfer Control Protocol, 简称 TCP) 来完成包过滤和分类控制^[4]。IP 协议是一个以报文形式网络中交换数据的协议, 作为网络层协议, IP 协议包括路由寻址和控制信息; TCP 协议是面向连接的协议, 建立在 IP 之上, TCP 协议规定了数据传输中数据信息的格式以及数据正确到达的方法, IP 数据包组成如图 2 所示。

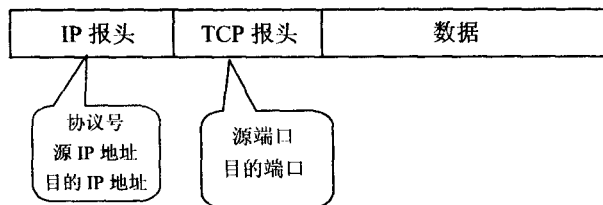


图 2 IP 数据包组成 (IP 所承载的上层协议为 TCP)

图 2 中 IP 数据包对于 TCP 来说, 协议号、源 IP 地址、目的 IP 地址、源端口和目的端口这 5 个元素组成了一个 TCP 相关, ACL 就是利用这些元素定义规则并对数据包进行过滤的。

2 访问控制列表的分类

ACL 作为网络安全控制的一种有效手段, 广泛应用于内外互联的网络中。下面给出一个典型的网络拓扑图 (见图 3), 用来举例说明 ACL 的分类和在网络中的应用。

图中的网络由企业内部局域网和国际互联网 (Internet) 组成, 内部网采用网管型交换机实现部门 VLAN 的划分和访问控制, 在部门下可接若干个普通交换机进行扩充; 内部网通过路由器实现 VLAN 间的通信和

服务器的连接, 其中路由器一个接口可接入互联网。

内部网划分网管中心、财务部门和人事部门 3 个 VLAN。网络拓扑图和子网分配见图 3 和表 1。

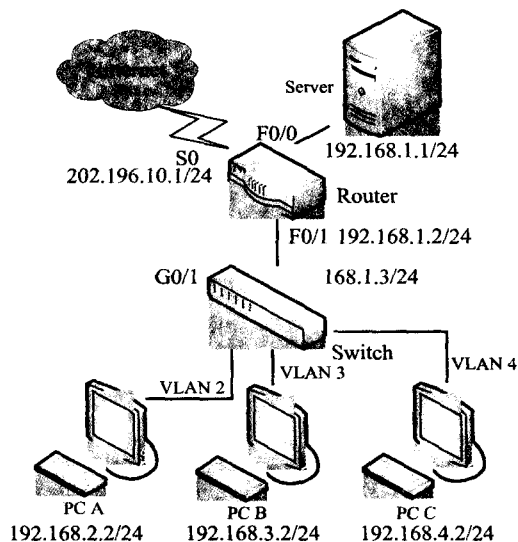


图 3 典型网络的拓扑图

表 1 子网分配表

VLAN 号	子网	部门
VLAN 2	192.168.2.0/24	网管中心
VLAN 3	192.168.3.0/24	财务
VLAN 4	192.168.4.0/24	人事

ACL 在网络设备上实现方式多样, 定义形式因设备不同也不太一致, 但基本可分为以下几类: 标准 ACL、扩展 ACL、自定义 ACL^[5]。

2.1 标准访问控制列表

标准 ACL 又叫 IP ACL, 它只对源 IP 地址和子网掩码进行控制, 标号在 1 ~ 100 之间, 可用名称来代替编号。标准 ACL 应用示例如下:

```
Router(config)#ip access-group 12/* 定义 ACL 的编号为 12。
```

```
Router(config)#access-list 12 deny host 192.168.2.2 host 192.168.1.1/* 主机 192.168.2.2 不能访问服务器 192.168.1.1。
```

```
Router(config)#access-list 12 permit any host 192.168.1.1/* 允许其他主机能访问服务器。
```

```
Router(config_0/1)#ip access-group 12 in /* 应用编号为 12 的 ACL 到端口 1 上。
```

标准 ACL 的优点是配置简单、容易理解, 但功能有限, 一般应用在接入层交换机上。

2.2 扩展访问控制列表

扩展 ACL 是应用最为广泛的一种, 几乎可以应用在所有路由交换设备上。与标准 ACL 相比, 扩展 ACL 能够对 IP 五元组进行控制 (源 IP 地址、目的 IP 地址、协议号、源端口、目的端口)。扩展 ACL 的标号在 101 ~ 300 之间, 可用名称来代替编号。扩展 ACL 的用法

示例如下:

```
Router(config)#ip access-group extend 101/* 定义 ACL 的编号为 101。
```

```
Router(config)#access-list 101 permit icmp any 192.168.1.1 0.0.0.0/* 允许目的地址 192.168.1.1 主机的 ICMP 报文。
```

```
Router(config)#access-list 101 deny tcp any 192.168.1.1 0.0.0.0 eq 23/* 禁止目的地是 192.168.1.1 的 Telnet 报文。
```

```
Router(config)#access-list 101 deny ip 192.168.2.0.0.0.255 192.168.1.1 0.0.0.0/* 禁止源地址 192.168.2.0 网段主机访问服务器。
```

```
Router(config_f0/1)# ip access-group 101 in/* 应用到接口。
```

2.3 自定义访问控制列表

在某些网络环境中,需要用一些特殊的字段来描述报文的特征来达到网络控制的要求。如要对报文的以太网报头中的源 MAC 和目的 MAC 地址、VLAN 号、TCP 报文中的 TCP 标志和一些特殊的协议的报文控制,仅使用标准或扩展 ACL 都不能达到要求,但可使用自定义 ACL^[6]。自定义 ACL 的标号是 401~600,可用名称代替编号。自定义 ACL 的示例和用法如下:

```
Router(config)#ip access-group 501/* 定义 ACL 编号为 501
```

```
Router(config)#access-list 501 permit mac 01-02-03-04-05-06 ip 192.168.1.1 0.0.0.0/* 允许源 MAC 地址是 01-02-03-04-05-06 的主机访问 192.168.1.1。
```

```
Router(config)#access-list 501 permit ip 192.168.0.450.0.0.0 vlan 2/* 允许 VLAN2 的主机访问 192.168.1.1。
```

```
Router(config_f0/1)# ip access-group 501 in/* 应用到接口。
```

3 访问控制列表在网络中的应用

在七层网络模型中,路由交换设备工作在第三层(网络层)^[7],负责去掉收到数据包的第二层(数据链路层)的信息来查看第三层信息,根据路由表来确定数据包的路由,再检查 ACL;若允许通过,则再进行第二层信息的封装,最后将该数据包转发。

ACL 是网络安全防御的前沿阵地,它提供了一种机制,可以控制路由器交换设备不同接口的信息流,该机制允许使用 ACL 来管理信息流,以制定内部网安全的访问控制策略,所以 ACL 在网络安全中起着重要的作用,下面介绍几个典型应用。

3.1 访问控制列表在设备保护方面的应用

网络层设备本身相当于一台运行着的主机,也有其特有的操作系统,可通过 Telnet、SNMP 或 HTTP 访问、更新配置或进行版本升级^[8]。因此除了网管员外,应确保无关人员不能攻击网络层设备或篡改其配置,利用 ACL 可以实现下面的控制功能。

3.1.1 控制网络设备访问权限

为方便网络设备的管理,网管员可通过虚拟连接(Virtual Port)实现对网络设备的远程访问,称为虚拟

端口连接(Virtual Type Terminal,简称 VTY),VTY 与 ACL 结合使用可以控制只有设定主机才能对网络设备进行访问,降低被攻击和非法侵入的风险。

在图 3 网络中,如果路由器只允许信息中心网段的计算机虚拟登录,则可在路由器 F0/1 接口上作如下配置:

```
Router(config)#ip accesslist extended convty/* 定义 ACL 名称为 convty。
```

```
Router(config)#permit 192.168.2.0 0.0.0.255 192.168.1.3 0.0.0.0/* 允许 vlan2 网段的主机访问端口 F0/1。
```

```
Router(config)#Line vty 0 4/* 以下是在 VTY 的 5 个虚连接通道中应用 ACL。
```

```
Router(config_vty)#ip access-group convty in
```

```
Router(config_vty)#ip access-group convty out
```

3.1.2 在 SNMP 协议中的应用

简单网络管理协议(Simple Network Management Protocol,简称 SNMP)在网络中有广泛的应用^[9]。但因其只要求无证实的传输层协议 UDP,存在很大的安全访问隐患,因此在网络设备上启用 SNMP,定义访问设备团体名(Community Name)的读、写权限的同时,最好利用 ACL 定义访问源地址列表,以避免因团体名泄漏而造成设备信息的泄漏。

根据图 3 的网络结构,如果在路由器上启用 SNMP,可在路由器上作如下配置:

```
Router(config)#snmp-agent community read public/* 定义 SNMP 的共同体名为 public,权限为 Read。
```

```
Router(config)#ip accesslist extended consnmp/* 定义 ACL 名 consnmp。
```

```
Router(config)#permit 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255/* 对应用 SNMP 协议设备的访问源地址设置标准 ACL。
```

```
Router(config)#snmp-server community public consnmp/* 在 SNMP 协议团体名中应用 ACL。
```

3.1.3 防止外部 IP 地址欺骗和非法探测

内部局域网一般使用私有 IP 地址,这样即可节约 Internet 公用网址又可有效保证网络安全。黑客为了攻击内部网络,可以采用 IP 诈骗的技术,伪装成一个内部或可信的外部 IP 地址对目标进行攻击。为此可以在路由器的入口方向上建立 ACL 进行阻止。

例如非法访问者对内部网络设备发起攻击前,往往会用 Ping 或其他命令探测网络^[10]。在图 3 网络中可以在 S0 接口上配置禁止从外部用这些命令的 ACL 来实现防范:

```
Router(config)#ip accesslist extended 109/* 定义 ACL 名 109。
```

```
Router(config)#access-list 109 deny icmp any any echo/* 禁止使用 Ping 命令。
```

```
Router(config)#access-list 109 deny icmp any any echo-reply
```

```
Router(config)#access-list 109 deny icmp any any unreachable/ * Ping 命令的回复为 Unreachable。
```

```
Router(config)#access-list 109 deny icmp any any traceroute /  
* 禁止使用 Traceroute 命令。
```

```
Router(config_s0)#ip access-group 109 in / * 应用到接口。
```

```
Router(config_s0)#ip access-group 109 out
```

3.2 访问控制列表在病毒防护方面的应用

计算机病毒(特别是系统漏洞病毒)常用端口进行传播和攻击^[11],可以在路由交换设备上设置 ACL 进行防范。例如若想要控制 Blaster 蠕虫的扫描和攻击,在图 3 网络中可以在路由器的 S0 上配置如下 ACL 进行防范。

```
Router(config)#ip accesslist extended 110/ * 定义 ACL 号 110。
```

```
Router(config)#access-list 110 deny tcp any any eq 135 / *  
以下封锁 Tcp 和 Udp 的 135、139、445 等端口。
```

```
Router(config)#access-list 110 deny udp any any eq 135
```

```
Router(config)#access-list 110 deny tcp any any eq 139
```

```
Router(config)#access-list 110 deny udp any any eq 139
```

```
Router(config)#access-list 110 deny tcp any any eq 445
```

```
Router(config_s0)#ip access-group 110 in /应用到接口。
```

```
Router(config_s0)#ip access-group 110 out
```

3.3 基于时间的访问控制

基于时间的 ACL 是根据天中的不同时段,或是星期中的不同天,或二者的结合来控制对网络资源的访问。它属于 ACL 一种新的用法,可对流入和流出网络的数据进行附加控制。该 ACL 可用编号,也可以命名。基于时间的 ACL 定义如下:

3.3.1 定义时间范围

定义时间范围分两步,指定时间范围和定义时间范围^[12]。时间定义可是单一的天,也可是某几天,方法如下:

```
Router(config)#time-range time-range-name/ * 进入 time-range 模式并给出一个时间范围名。
```

```
Router(config-time-range)#absolute [start time date][end  
time date]/ * 定义时间范围,格式为日/月/
```

```
Router(config-time-range)#periodic days-of-the-week hh:  
mm to [days-of-the-week] hh:mm / * 定义产生作用的具体时间。
```

3.3.2 应用已定义的时间范围

以图 3 网络为例,假设在 2010 年 9 月 1 日至 2011 年 1 月 10 日的上班时间(周一至周五的上午 8 点至下午 6 点),禁止办公用户使用 QQ、联众游戏、MSN。可通过设置如下的 ACL 来实现。

```
Router(config)#ip access_list extended 112 / * 定义 ACL 名 112。
```

```
Router(config)#time-range working-time / * 设置时间限制的  
名称为 working-time。
```

```
Router(config-time-range)#absolute start 00:00 1 September
```

```
2010 end 23:59 10 January 2011 / * 设置 ACL 时间范围 2010 年 9  
月 1 日至 2011 年 1 月 10 日。
```

```
Router(config-time-range)#periodic Monday 08:00 to Friday  
18:00/ * 设置 ACL 在每星期中有效的时间范围是周一至周五的  
上午 8 点至下午 6 点。
```

```
Router(config)#access-list 112 deny tcp 192.168.0.0 0.0.  
255.255 any eq 1863 time-range working-time/ * 禁止 MSN 使用  
的 TCP 的 1863 端口。
```

```
Router(config)#access-list 112 deny udp 192.168.0.0 0.0.  
255.255 any eq 4000 time-range working-time / * 禁止 MSN 使用  
的 TCP 的 4000 端口。
```

```
Router(config)#access-list 112 deny tcp 192.168.0.0 0.0.  
255.255 any eq 8000 time-range working-time/ * 禁止 QQ 登录使  
用的 8000 端口。
```

```
Router(config)#access-list 112 deny tcp 192.168.0.0 0.0.  
255.255 any eq 3128 time-range working-time / * 禁止代理服务  
器主要部署使用的 TCP3128 端口。
```

```
Router(config)#access-list 112 deny tcp 192.168.0.0 0.0.  
255.255 any eq 8080 time-range working-time / * 禁止代理服务  
器主要部署使用的 TCP8080 端口。
```

```
Router(config)#access-list 112 permit ip any any / * 允许所有  
有数据流。
```

```
Router(config)#interface s0
```

```
Router(config-s0)#ip access-group 112 out/ * 应用到接口。
```

使用基于时间 ACL 时注意以下两点,一是 ACL 时间范围是基于路由器的时钟的,应保证路由其时钟的设置正确性;二是在 Time-range 命令中同时使用 Absolute 和 Periodic,只有匹配 Absolute 时间之后才匹配 Periodic 时间。

ACL 作为网络安全的有效手段,当其安全特性被充分合理有效利用时,路由器变成一个有效、稳定、坚固的防御体系,可以极大地提高网络的安全性。

4 配置访问控制列表原则

ACL 配置灵活,功能强大,设置过严会影响网络的正常通信,设置过松则达不到安全控制的效果,所以设置时可以参考以下几个原则。

1) 最小特权原则。

设置 ACL 时只给受控对象安全访问所必须的最小的权限,即被控制的总规则是各个规则的交集,只满足部分条件的是不容许通过的。

2) 最靠近受控对象原则。

ACL 自上而下按语句的顺序逐条检测并依次执行,只要符合条件就立刻转发,不再继续检测下面的语句,必须谨慎地设置 ACL 的语句次序。

3) 默认丢弃原则。

在很多路由交换设备上默认最后一句为 ACL 加入了拒绝所有数据包(Deny Any)^[13],即丢弃所有不

符合条件的数据包,配置时要特别注意以免造成网络中断。

4)接口引用原则。

在应用 ACL 时,因为标准 ACL 只限于过滤源地址,若将 ACL 应用在源端口会阻止报文流向其他端口,所以应将其应用在靠近目的端口的位置;而扩展 ACL 根据其使用的目的和特点则应尽量放在过滤源的位置上。同时,对于一个协议,一个接口的一个方向上同一时间内只能设置一个 ACL。

5)应用有效原则。

ACL 在被应用到端口前对数据流不产生控制。因此在定义 ACL 后,必需将其应用到路由交换设备的某接口或某种协议上,并指明方向(接口方向以路由交换设备为参考点,进入路由交换设备为 IN 方向,出路由交换设备为 OUT 方向)。另外,在已有 ACL 末尾添加新的表项并不能改变其原有的功能,若要改变,必须重新创建一个 ACL 并应用于设备接口上才能生效。

6)注解语句原则。

正确管理和维护 ACL 比较困难,特别是大规模的网络,因此要将 ACL 的每一条规则作详细的注解,并对配置的 ACL 和每一条规则的改变做日志,以备日后追踪修改。

5 结束语

ACL 的主要作用是基于已经建立的标准允许或拒绝报文流,虽然它不能完全保证网络的安全,但由于 ACL 的配置简单易行且不用增加硬件设备,与防火墙配合使用不但提升网络的性能,而且还可减轻网络防火墙的负担。因此结合实际情况,在网络中合理适当

地使用 ACL 进行访问权限控制,网络性能将会得到很大提升。

参考文献:

- [1] 潘文婵,章 韵. 路由器访问控制列表在网络安全中的应用[J]. 计算机技术与发展,2010,20(8):160-62.
- [2] 李 新,孙忠涛. 高校校园网安全管理研究[J]. 中国现代教育装备,2010(9):27-29.
- [3] Aura G, Wongthavarawat K. Software Framework for QoS Support in Home Networks[J]. Computer Networks, 2003(5):7-22.
- [4] 兀 俊. ACL 访问控制列表在交易连接平台上的应用[D]. 上海:复旦大学,2008.
- [5] Held G, Hundley K. CISCO 访问表配制指南[M]. 前导工作室,译. 北京:机械工业出版社,2005.
- [6] Zeinalipour-Yazti D. Topologically Aware Overlay Networks Using Domain Names[J]. Computer Networks, 2006(16):3064-3082.
- [7] 李 强. 访问控制列表(ACL)在网络安全设计中的应用[J]. 计算机与网络,2004(7):60-61.
- [8] Tanenbaum A S. Computer Networks[M]. Beijing: Published by Tsinghua University, 2005.
- [9] Forouzan S R. TCP/IP 协议族[M]. 第3版. 谢希仁,译. 北京:电子工业出版社,2007.
- [10] 王 芳. 路由器访问控制列表及其应用技术研究[D]. 郑州:解放军信息工程大学,2007.
- [11] 石 光. 网络安全技术综述[J]. 长沙铁道学院学报(社会科学版),2007,8(3):180-181.
- [12] 周 星,汪国安,张 震. 网络层访问控制列表的应用[J]. 河南大学学报(自然科学版),2004(3):67-68.
- [13] 潘常春. 主机网络安全及其关键技术研究[J]. 广西教育学院学报,2005(4):63-67.

(上接第124页)

- [2] 黄付刚,李兰君. 基于模糊-PID 控制的锅炉汽包水位自适应研究[J]. 机电信息,2010(6):101-103.
- [3] 丁 虎. PID 参数整定新方法在锅炉蒸汽压力系统中的应用[J]. 哈尔滨工业大学学报,2010,42(1):163-168.
- [4] 卓旭升. 汽包锅炉的一种非线性串级控制设计[J]. 控制工程,2010,17(S0):22-24.
- [5] 辛广路. 锅炉运行与操作指南[M]. 北京:机械工业出版社,2006.
- [6] 张小桃. 基于现场数据的汽包压力动态建模研究与仿真[J]. 动力工程,2004,24(3):370-374.
- [7] 秦富童,岳丽华. 应用 BP 神经网络的目标识别效果评估[J]. 计算机工程与应用,2010,46(5):148-150.
- [8] Chen Haorui. Analysis on the percolation from root zone of winter wheat: Combination of a numerical model and BP Artificial Neural Network[C]//2010 International Conference on Information and Emerging Technologies (ICIET). [s. l.]: [s. n.], 2010:213-217.
- [9] 朱喜娜,陆 达,范汉青. 基于 BP 算法 PID 控制器的研究[J]. 计算机技术与发展,2010,20(5):183-186.
- [10] Petrovl M. Fuzzy PID Control of Nonlinear Plants[C]//2002 First International IEEE Symposium "Intelligent Systems". [s. l.]: [s. n.], 2002:30-35.
- [11] 黄友锐,曲立国. PID 控制器参数整定与实现[M]. 北京:科学出版社,2010.
- [12] Jiang Guoyin. Research on Credit Rating Method Based on BP NN [C]//International Conference on Service System and Service Management. [s. l.]: [s. n.], 2007:1-4.