文章编号：1672-2892(2011)02-0238-06

网络安全技术在城市级供电系统数据网中的应用

张冀晛，吴中川

(海军驻绵阳地区特种装置军事代表室，四川 绵阳 621000)

摘 要：叙述信息系统安全的概念，讨论信息系统安全体系框架的各个组成部分及其之间的关系。以某城市级供电局网络安全的现状为对象，对网络结构、安全策略部署上的薄弱环节进行分析。根据信息安全体系结构，从网络基础平台、业务系统接入、安全防护等几方面总结未来的业务及安全需求，提出相关解决措施。根据网络安全设计原则和不同安全技术的特点，设计供电局网络改造整体方案。通过以上方案，较为全面地解决了电力企业数据网络由于历史原因造成的安全防范措施的缺失问题，能够有效发现安全隐患，并及时提供解决手段、提前预防和即时升级的能力，是较为高效的电力系统数据网络安全系统。

关键词：安全；信息技术；电力数据网；网络安全

中图分类号：TP393.08 **文献标识码：**A

County-suburb power grid data network system based on network security technology

ZHANG Ji-xian, WU Zhong-chuan

(Military Representative Room of Navy Special Equipment in Mianyang area, Mianyang Sichuan 621900, China)

Abstract: The paper analyzes the concept of information safety and discusses the relationship among member parts of information security system frame. Taking the security situation of County-city Power Grid's data net system as an example, the weaknesses of the net structure and security strategy dispose are analyzed. According to the system structure, the future task and safety requirements on the net basic platform, operation system connector and security protection are concluded; relative solutions are proposed. Based on the principles of net safety design and the characteristics of different safety technologies, a new project is put forward. Through this new system, the problem of lacking security protection measurements, which has been existed in power industries for a long period, has been solved. It can provide the ability of timely fault finding, corresponding solving methods, the capabilities of precaution and instant upgrade, which is an efficient and optimized power grid data network system.

Key words: safety; information technology; power data network; network safety

电力是国家的支柱产业，电网的安全生产风险不仅意味着国家财产遭受经济损失的风险，而且可能会危害人民的生命安全，因此电网安全是国家安全重要组成部分。为保障电网安全生产运行，电网公司对作为信息系统承载平台的计算机网络安全性和可靠性要求越来越高。同时，多数电力企业的数据网络在建设初期较少或者根本就没有考虑诸如安全防范的相应措施，留下许多安全隐患[1-2]。加上缺乏必要防范技术人才和解决手段，各种应急处理工作目前都处于自发、无序的状态，这样的局面显然远远不足以对付当前可能发生的各种病毒与恶意攻击以及其他的计算机犯罪等突发性安全事件。在这种情况下，加强对电力数据网络的监管及风险防范就变得十分重要。

1 国内外现状

目前人们重点关注的网络安全问题主要有：1) 安全算法；2) 网络安全检测和防御技术；3) 网络安全是一个体系，包括网络的综合防护能力、检查评估能力、应急处理能力和预警反击能力等。另外，自适应的网络安全产

收稿日期：2010-12-14；修回日期：2011-02-16

品、自动分析网络状态的安全管理产品乃至构建网络安全自防御体系也都是网络安全的研究热点。主要的网络安全技术有：病毒防范技术、防火墙技术、入侵检测技术、访问控制技术、漏洞扫描技术、安全审计技术、数据加密技术、数字签名技术等。分别采用隔离、用户鉴别和访问控制技术，对网络进行分级、分段和内外网的隔离管理；利用口令、物理特征等方法鉴别用户真实身份，严格进行用户的访问权限控制与授权管理，保护系统和资源免受非法访问与入侵；采用链路层、网络层和应用层的数据加密技术来保证业务数据、管理信息数据在传输过程中的机密性和完整性。

这些安全产品在一定程度上提高了电力数据网的安全水平，但仍然有许多问题需要解决：一方面仅仅通过部署安全产品很难完全覆盖电力数据网的安全问题；另一方面，信息安全问题不是静态的，仅仅部署安全产品则是一种静态的解决办法。通常，在产品安装和配置后较长一段时间内，它们都无法动态调整以适应安全问题的变化。只有把对计算机网络系统安全的静态防范、被动防范和分散防范转变成动态防范、主动防范和集中整体防范，建立完备系统的防范、检测与响应的动态安全防御机制，才能保证计算机网络系统的安全[3]。

2　信息系统安全体系中的技术体系框架

信息系统安全的总需求是物理安全、网络安全、数据安全、信息内容安全、信息基础设备安全与公共信息安全的总和，安全的最终目标是确保信息的机密性、完整性、可用性、可审计性和抗抵赖性，以及信息系统主体(包括用户、团体、社会和国家等)对信息资源的控制。本文讨论的重点是网络安全[4−5]。安全服务(安全机制)作 X 轴，协议层作 Y 轴，信息系统构成单元作 Z 轴(见图 1)。本三维体系不涉及定量的数值表达式。在 X 轴中，安全机制并不直接配置在协议层上，也不直接作用在系统单元上，而是必须通过提供安全服务来发挥作用。

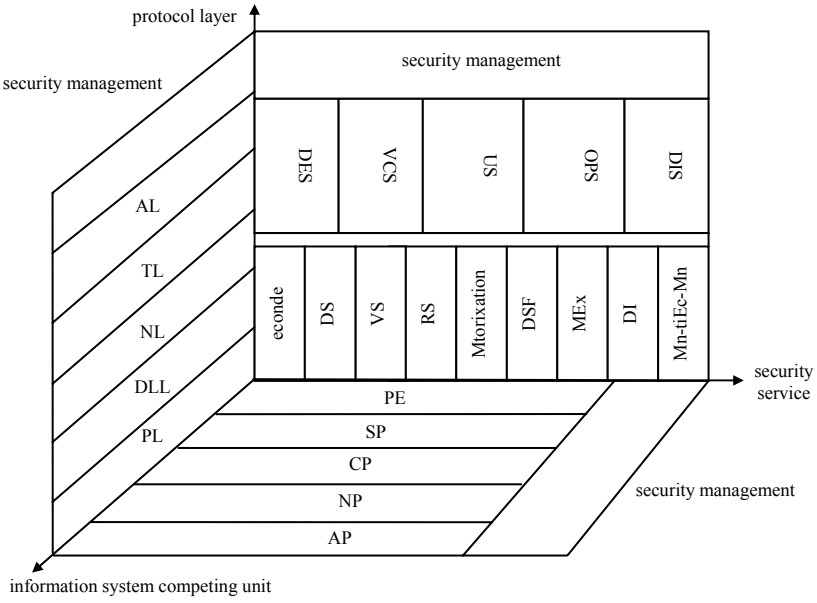

Fig.1 3-D figure of safety technology system
图 1　安全技术体系三维图

为便于从三维图中全面地概览信息系统安全体系中的相互关系，将安全机制作为安全服务的底层支撑(示意)放在图 1 中；在安全机制中，将开放式通信系统互联参考模型(Open System Interconnection，OSI)安全体系中的 8 种机制与物理安全中的电磁辐射安全机制放在一起，可使安全服务中的数据保密性和可靠性、可用性功能赋有更为广泛的安全意义；协议层以 OSI 七层模型为参考，只选取可适宜配置安全服务的 5 个层次；每个维中的“安全管理”是一种概念，它是纯粹基于标准(或协议)的各种技术管理。

3　网络安全技术应用

为了实现供电局电力数据网的安全运行，在设计中应全面地考虑安全保障措施，主要采用：1) 在每个功能区域内部进行详细的虚拟局域网(Virtual Local Area Network，VLAN)划分；2) 在功能区域之间使用防火墙进行隔离；3) 采用入侵检测系统(Intrusion Detection System，IDS)；4) 采用先进的网络安全监控、分析、响应技术，形成网络自防御体系；5) 在电力生产系统和电力管理信息系统之间通过物理隔离装置进行通信；6) 采用多协议标签交换(Multi-Protocol Label Switching，MPLS)虚拟私有网(Virtual Private Network，VPN)技术对不同安全级别的区域进行隔离；7) 病毒防范技术。

3.1 虚拟网络 VLAN 技术

对于核心交换机和接入交换机之间的互相连接的端口，将其设为 VLAN Trunking，这样它将传递所有的 VLAN

信息和数据给 VLAN 中继协议或虚拟局域网干道协议(VLAN Trunking Protocol，VTP)域的其他交换机，VLAN Trunking 技术采用 802.1Q 标准协议[6-7]。为了提高整个网络骨干的带宽，同时提高网络连接的可靠性，在 2 台交换机之间配备多条千兆连接，这多条连接可以同时工作和负载均衡，又互为备份。在方案中，2 台交换机之间的多条千兆连接采用千兆捆绑(GE Channel)技术互连，提高交换机之间的带宽，既可以实现交换机之间 VLAN Trunk，又使整个系统具有较高的可靠性。

3.2 防火墙技术

目前实现防火墙的主要技术有：数据包过滤，应用网关，代理服务等。数据包过滤技术和应用网关是通过特定的逻辑判断来决定是否允许特定的数据通过，其优点是速度快，实现方便，缺点是审计功能差；代理服务技术既能进行安全控制，又可以加速访问，但实现比较困难。在实际应用当中，构筑防火墙的真正解决方案很少采用单一的技术，网络的安全性研究通常都是解决各种问题的不同技术的有机组合。防火墙的 3 种技术都各有各自的优点和缺点，单独使用一种技术不能完全满足网络的要求，应根据网络所提供的服务、网络的开放程度以及网络的带宽等实际情况采用不同的组合方式。同时，单纯的防火墙防卫方式无法满足电力数据网络对安全性的要求，需结合其他安全技术如入侵检测技术、物理隔离等来共同达到保护电力数据网络安全的目的。

3.3 IDS 入侵检测系统

IDS 就是对网络或操作系统上可疑行为做出策略反应，比如及时切断入侵源，记录并通过各种途径通知网络管理员等措施，以求最大幅度地保障系统安全。目前应用于不同操作系统平台的几种典型入侵检测系统，通常都采用异常检测模型和滥用检测模型来检测入侵。入侵检测方法主要有基于规则的入侵检测方法和基于行为的入侵检测方法，又分别被称为滥用检测和异常检测[8]。通用的入侵检测模型见图 2，它可以涵盖这 2 种入侵检测方法。

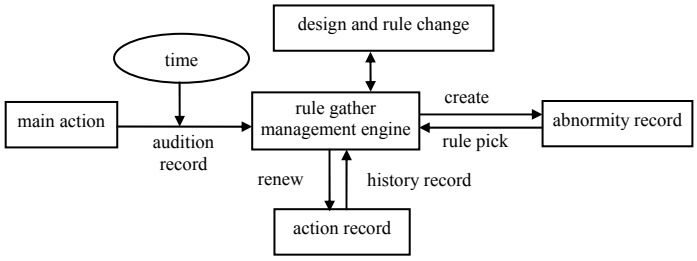

Fig.2 General intrusion detection model
图 2 通用入侵检测模型

目前采用的是东软入侵检测系统 IDS，与东软防火墙相得益彰。它以实时性、活动检测和主动防御为特点，有效弥补了其他静态防御工具的不足。

3.4 网络安全监控、分析、响应技术

以监控—思科安全监控、分析和响应系统(Cisco-Monitoring Analysis and Response System，CS-MARS)为例对网络安全管理系统进行说明，该系统是一个软硬件一体化的产品，可以关联网络和安全设备配置信息、NetFlow、应用日志和安全事件，提供图形化界面让 IT 人员可以从一个集中的地点实时发现、跟踪、分析、防御、报告和存储整个企业网络中的安全事件和攻击[9]。主要功能有：集中管理和控制网络上的安全设备；集成网络智能，进行网络异常事件和安全事件的先进关联；察看校正后的事件并自动执行调查；通过全面充分利用网络和安全基础设施来防御攻击。

3.5 物理隔离装置

物理隔离装置是电力系统专用安全产品。物理隔离的作用在于要保证内外网在任意时刻都保持物理传导和物理辐射意义上的断开。一般来说，物理隔离装置主要由内网处理单元、外网处理单元和控制处理单元这 3 部分构成。外网处理单元与外网(安全级别低的网络)相连，内网处理单元与内网(安全级别高的网络)连接，控制处理单元中的转换开关，在同一时刻只能与内网或外网处理单元中的一个闭合，另一端是断开的，从而使内、外 2 个通信网络实现了物理上的隔离。

3.6 MPLS VPN 安全传输技术

VPN 实现在公用网络上构建私人专用网络。VPN 按隧道所属的协议层次划分，分为基于二层隧道协议的 VPN 和基于三层隧道协议的 VPN。MPLS VPN 属于基于三层隧道协议的 VPN，是一种基于 MPLS 技术的 IP VPN。它在网络路由和交换设备上应用 MPLS 技术，简化核心路由器的路由选择方式，是结合传统路由技术的标记交换实现的 IP 虚拟专用网络(IP VPN)，可用来构造宽带的 Intranet 和 Extranet，满足多种灵活的业务需求。图 3 显示了

VPN 的可见地址空间，没有 P 路由器或者其他 VPN 的地址对这个 VPN 是可见的。用户网络边缘设备(Customer Edge，CE)和运营商边缘路由器(Provider Edge，PE)之间的链路，包括 PE 上的端口地址，属于 VPN 的地址空间。所有 PE 路由器上的其他地址，包括 loopback 端口，都不属于 VPN 的地址空间。

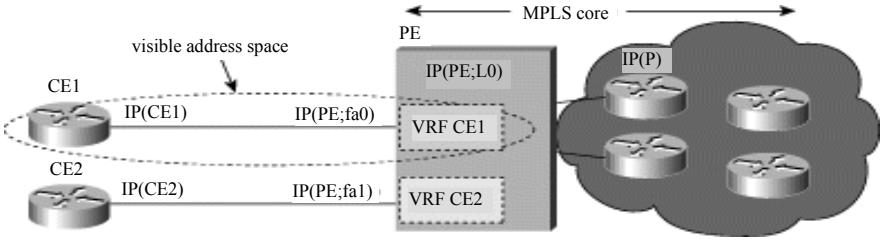

Fig.3 Concealing core network structure
图 3　核心网络结构的隐藏

可以看出，从安全性来看，在 IP 网上提供 MPLS VPN 服务也可以达到甚至超过在 ATM 网络上模拟电路方式的二层隔离技术，采用 MPLS VPN 实现业务的隔离能够满足各自业务系统安全性的需求。

3.7 防病毒技术

趋势防毒墙网络版 officescan 采用可集中管理的桌面防毒策略，为企业中的本地和远程办公人员提供最新的病毒保护，趋势病毒库每 1~2 天升级 1 次。officescan 利用驻留在 PC 中的防病毒客户端程序向中央服务器报告所有的病毒事件，同时使管理员能够实时查看可能会发生的所有病毒活动，并提供统计分析报告。

4　应用实例方案设计

遵循网络拓扑结构模块化、层次化的总体设计，网络拓扑结构主要由核心层、分布层和接入层组成；在上述网络拓扑结构层次化的基础上，根据数据中心各业务功能分区的不同，把网络分为多个功能模块化分区，每个功能模块主要有分布层和接入层组成，统一接入到局域网的核心区域[10]。每个功能模块的分布层交换机负责各业务功能模块到核心交换机和提供各种网络控制，如安全、服务质量(Quality of Service，QoS)和内容交换等，兼做接入层功能。

结合上述网络要求，并针对都匀电网的要求和应用特点,都匀供电局网络分为:1) 核心交换区域；2) 核心数据服务器区域；3) 楼层和下属部门接入区域；4) 合作伙伴和外包区域；5) 外联网区域；6) 网络和安全管理区域；7) 区县局、变电站、供电所的接入；8) 互联网接入。见图 4。

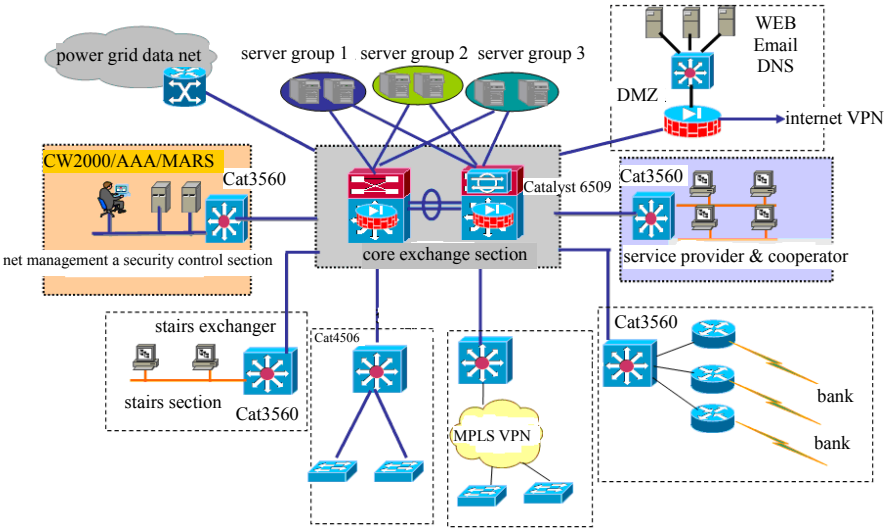

Fig.4 Network partition
图 4　网络区域划分

4.1 核心交换区域设计

4.1.1 网络设计

核心层设备应该是高性能的交换机，可实现线速度的交换传输[11]。同时，核心层设备必须非常可靠，能实现不间断工作，并具备多层交换功能，要求具备高带宽、高可靠性、高安全性等先进功能。用 2 台高性能多层交换机 Catalyst 6509 作为整个大楼局域网的核心交换机，核心交换机 Catalyst 6509 的配置采用双电源，双机配置采用单 720G 交换矩阵处理器。双机配置时 Catalyst 6509 核心交换机之间采用多个千兆以太网通道技术，这样做的好处是不仅可以平衡多个千兆链路的负载，形成一个逻辑传输连接，而且可以在其中任何一条或多条千兆链路出现故障时，使网络快速收敛，保证业务的高可靠运行。

4.1.2 安全设计

Cisco Catalyst 6500 交换机将一套先进的安全模块集成在一起，以便进一步增强网络安全性。Catalyst 6500

交换机可以提供新型思科高级安全模块包括防火墙服务模块(Firewall Service Module，FWSM)[12]、安全插接层(Secure Sockets Layer，SSL)、IP 安全虚拟专用网(IPSec VPN)服务模块、防范分布式拒绝服务攻击(Distributed Denial of Service，DDOS)的模块(Anomaly Detection Module)、入侵检测系统模块(Intrusion Detection System Module，IDSM)和网络分析模块(Net Analysis Module，NAM)。客户将能够在交换机上部署综合安全性，这种方式可以大大提高性能、可管理性和整个系统的性价比。在本次改造中部署以下安全模块和功能，见表 1。

表 1 核心交换机 Cisco6509 安全模块及其功能

Table1 Safe module in core switching exchange—Cisco6509 and its function

name of module	features
FWSM	CiscoFWSM is completely integrated inside Cisco Catalyst 6500 serials exchangers. For each module, the throughput can be extended to the size over 5 GB. With more modules, the bandwidth can reach 20 GB. It can support VLAN and provide dynamic router.
NAM	To supply the practical level of visibility, and to realize the update fluency analysis, functional surveillance and fault handle, being extremely adaptable to the data center, enterprise edge and distributed layers.
IPSec VPN	Supporting IPsec encryption throughput of 2 G, and providing the IPsec VPN converge with power supplier

4.2 核心数据服务器区域及业务系统接入设计

4.2.1 网络设计

供电局主要有以下服务器系统：办公自动化系统(Office Automation，OA)服务器、管理信息系统(Management Information System，MIS)服务器、营销服务器、财务服务器、95598 服务器、地理信息系统(Geographic Information Systems，GIS)服务器、WEB 服务器、邮件服务器等等。为了适应财务、营销等数据大集中的发展趋势和存储中心的发展趋势，适应电力未来业务的发展，该局将在下一步的工程中逐步建设核心数据服务器区域，这里只作初步方案设计。

核心数据服务器区采用 2 台独立的具有安全控制能力的局域网交换机，采用千兆双链路和服务器群连接，并采用多个千兆捆绑或万兆和大楼核心交换机 Catalyst6509 连接，能满足大负荷网络运行需求。核心服务器区拓扑见图 5。

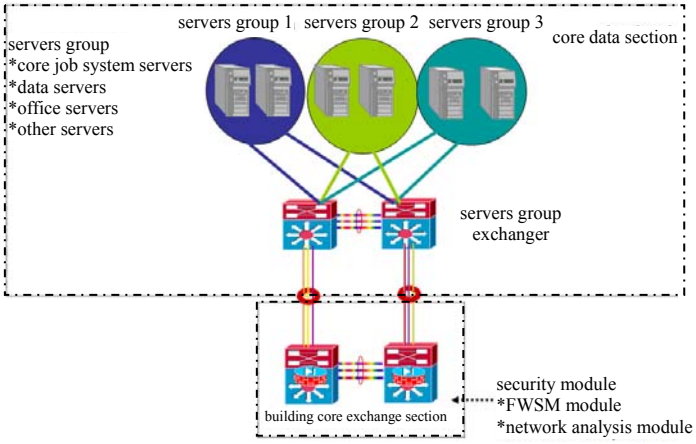

Fig.5 Core server partition

图 5 核心服务器区

4.2.2 安全设计

对于服务器群的安全控制，可以在服务器群交换机上对不同业务的服务器划分 VLAN，将 VLAN 通过 Trunk 联结到核心交换机 Catalyst6509 的防火墙模块 FWSM 上，这样通过 FWSM 可以隔离不同安全级别的服务器。不同的 VLAN 在 FWSM 上可以分配不同的安全级别，实现隔离安全域；在供电局的服务器群可划分为：营销业务服务器 VLAN、财务业务服务器 VLAN、OA 服务器 VLAN、95598 服务器 VLAN、生产服务器 VLAN、数据库系统 VLAN、连接大楼交换机 VLAN 和其他 VLAN，拓扑连接见图 6。

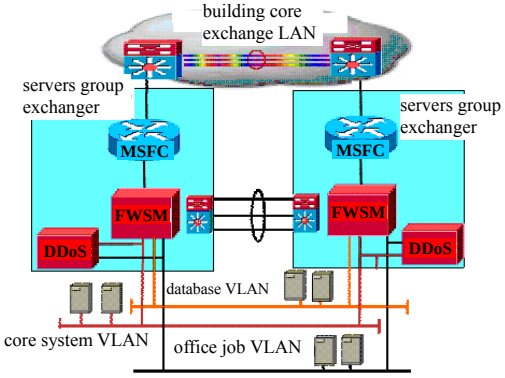

Fig.6 Topological relationship between VLANs

图 6 VLAN 间的拓扑关系

防火墙采用路由模式运行，MSFC 在防火墙模块中起路由网关作用，隔离 VLAN 间不授权的访问。通过定义不同的安全层次和安全接口实现对关键业务资源的深层次保护(例如定义公用服务器组中的数据库 VLAN、核心系统 VLAN 等属于防火墙 Inside 区，安全级别为 100；其余用户 VLAN 属于 outside 区，安全级别为 0；安全级别越高代表受保护程度越高)。对于同层次内 VLAN 间互相访问的控制，例如属于 outside 区域的 VLAN 间访问控制，仍将采用包过滤(定制访问控制列表 Acl，即在 sup720(MSFC)模块上的访问控制列表)的方式实现。

5 结论

本系统的研发和实施，较为全面地解决了电力企业数据网络由于历史原因而造成的安全防范措施的缺失问

题，能够有效发现安全隐患，并及时提供解决手段，对于未来可能发生的病毒与恶意攻击，以及其他的计算机犯罪等突发性事件，提供了提前预防和即时升级的能力，是较为高效的电力系统数据网络安全系统。

参考文献:

[1] 徐超汉. 计算机网络安全与数据完整技术[M]. 北京:人民邮电出版社, 1999:50-75.
[2] 林晓鹏,郭东辉. 基于经济机制的网格资源调度分析[J]. 信息与电子工程, 2010,8(4):495-499.
[3] 谭伟贤,杨力平. 计算机网络安全教程[M]. 北京:国防工业出版社, 2001.
[4] (美)CHRIS HARE KARANJIT SIYAN. Internet 防火墙与网络安全[M]. 刘成勇,刘明刚,王明举,等译. 北京:机械工业出版社, 1998.
[5] (美)MARCUS GONCALVES. 防火墙技术指南[M]. 宋书民,朱智强,徐开勇,等译. 北京:机械工业出版社, 2000.
[6] 黄允聪,严望佳. 防火墙的选型、配置、安装和维护[M]. 北京:清华大学出版社, 1999.
[7] 段海新. 防火墙规则的动态分配和散列表匹配算法[J]. 清华大学学报, 2001,41(1):96-98.
[8] 胡华平,陈海涛,黄辰林. 入侵检测技术的研究现状与发展趋势[J]. 计算机工程与科学, 2001,23(2):20-25.
[9] 陈硕,安常青,李学农. 分步式入侵检测系统及其认知能力[J]. 软件学报, 2001,12(2):225-232.
[10] White G B,Fisch E A,Pooch U W. Cooperating Security Managers:A Peer-based Intrusion Detection System[J]. IEEE Network, 1996,10(1):20-23.
[11] LING Jun. A Novel Immune System Model and Its Application to Network Intrusion Detection[J]. WuHan University Journal of Natural Sciences, 2003,8(2A):393-398.
[12] YONG Xiang. On the defense of the distributed denial of service attacks:An on-off feedback control approach[J]. IEEE Trans. On System,Man,and Cybernetics-part A:Systems and Humans, 2001,31(4):282-293.

作者简介:

张冀晛(1984-)，男，太原市人，助理工程师，研究方向为测控技术、数字通信技术、数字信号处理技术. email:873647602@qq.com.

吴中川(1973-)，男，沈阳市人，本科，从事核电子方面的研究工作.