

基于参数测量的园区网可靠性分析系统的实现

李崇东,肖晓强,李 达,徐 明,赖建文

(国防科学技术大学 计算机学院,湖南 长沙 410073)

摘 要:随着园区网的快速发展,网络运行状况及关键业务的服务质量已经成为园区网管理与维护必须要考虑的重要因素,通过对网络流量与性能参数的分析来评价网络性能已经成为网络可靠性研究的重要手段。从研究网络可靠性入手,运用 SNMP 流量监控技术,提出了基于宏观流量分析的园区网可靠性分析策略。系统采用集中式控制、分布式测量的体系结构,运用监测服务器逻辑分层的方法和区域代理监测技术进行网络可靠性监测,实现了网络设备信息显示、宏观流量监控和异常流量预测与报警等功能。实验表明,所设计的系统能较好地分析网络可靠程度,及时了解网络的负载状况、快速发现网络性能瓶颈,并能根据分析结果找到可靠度下降的原因。

关键词:宏观流量监测;SNMP;可靠性分析;异常报警

中图分类号:TP393.18

文献标识码:A

文章编号:1673-629X(2010)10-0021-05

Implementation of Reliability Analysis System on Campus Network Based on Parameters Measurement

LI Chong-dong, XIAO Xiao-qiang, LI Da, XU Ming, LAI Jian-wen

(College of Computer, National University of Defence and Technology, Changsha 410073, China)

Abstract: With the rapid development of campus networks, operation status of network and service quality of key business must be considered as important factors for management and maintenance of the campus network, evaluating the network performance by analyzing network traffic and performance parameters has become an important means of network reliability research. Studying the reliability of campus network to start, with SNMP traffic monitoring technique, a campus network reliability analysis strategy is proposed based on macro-traffic analysis. A monitoring architecture which is centralized control and distributed measurement is implemented in this system. The whole network is monitored by applying the measure of server logical layering and the technology of regional agency monitoring. The functions of network equipment information display, macro-flow monitoring, abnormal traffic prediction and alarm are achieved. The experimental results show that the proposed system can analyze the reliability of the network more effectively, keep abreast of the network load conditions, rapidly discover the bottleneck of network performance and find out the reasons of the decline of reliability according to the analysis results.

Key words: macro-traffic monitoring; SNMP; reliability analysis; abnormal alarm

0 引 言

随着社会信息化进程的加速,大量企业、事业及政府部门都建立了园区网。但是,随着 IP 网络承载业务类型和关键业务越来越多,对网络可用性的要求越来越高。如何设计高可靠性的园区网以及如何快速、准确地对园区网进行可靠性评价已成为热点问题。文中首先分析了网络可靠性分析的研究状况,接着根据实际需求设计了一个基于宏观流量分析的园区网可靠性

分析系统。实验结果表明,该系统能较好地满足园区网可靠性分析需求。

1 相关技术概述

1.1 网络可靠性分析概述

如今网络对人们工作和生活的作用日趋重要,网络可靠性作为衡量网络性能的重要指标日益引起人们的重视。网络可靠性描述了网络在规定时间内和一定环境下完成目标任务的能力^[1]。对网络可靠性的研究,大都以不同的研究目标为牵引,规定了不同的可靠性测度,并引入了各种判定网络可靠性的标准,这些标准可分为生存性(Survivability)^[2]、抗毁性(Invulnerability)^[3]、完成性(Performability)^[4,5]以及可用性(Avail-

收稿日期:2010-01-28;修回日期:2010-04-20

作者简介:李崇东(1983-),男,硕士研究生,研究方向为网络测量、网络可靠性分析;肖晓强,副教授,硕士生导师,研究方向为性能分析、网络测量、计算机仿真等;徐 明,教授,博士生导师,研究方向为无线网络与移动计算。

ability)^[6]四类。

其中,网络的生存性和抗毁性是从网络连通性角度分别描述了网络拓扑结构和网络节点、路径对网络可靠性的影响,主要用于军用网络研究。网络的完成性是指任务初始化后,在规定的完成时限内,系统按客户需求稳定运行或满足服务质量的能力。网络的可用性是指产品或服务处于工作状态时所期望达到的连接时间的平均值。可用性有助于用户理解某一特定网络可用程度是多少,对于直接要为网络中断付出代价的业务来说,这是非常关键的因素。如今,视频点播、远程会议、电子商务等多媒体业务的快速发展对园区网的性能稳定性提出了更高要求,网络可靠性的监测也日趋重要。文中研究的内容主要是针对园区网可靠性中的可用性研究的。

1.2 网络可靠性监测技术

网络流量的采集是进行网络可靠性分析的基础,是衡量网络运行负荷和状态的重要参数。根据不同的流量监测粒度,可将可靠性监测方法分为数据包级监测、链路级监测和业务流级监测三种。

数据包级监测主要通过捕获数据包,用协议分析方法解析所关心的协议流量^[7]。这种方法可以了解深层网络流量特征,如数据包大小分布、各层协议流量分布与速率变化情况等,并由此建立网络流量模型。但是,单纯基于数据包级的流量监测没有考虑到流量的聚合特性,不能刻画网络的宏观流量特征。但数据包级监测方法原理简单,实现环境要求低,而且能够得到各种形式的流量统计信息,可以分析网络各业务应用的分布情况,提供发现网络性能下降或故障根源的途径。

链路级监测主要通过 SNMP 协议实现^[8,9]。目前 SNMP 协议发展迅速,绝大多数网络设备都支持 SNMP,它已经成为事实上的网络管理规范,SNMP RMON 方法便于在网络中大量布置流量监测点,达到对整个网络区域同时进行监测的目的,并且在流量监测点中完成大量流量分析统计工作,减轻了流量监测系统管理者的负担。采用该监测方法具有以下优点:可以在任何时候收集任何地点的网络流量,能够收集到某个网络中大量设备的同步流量信息,并获得流量间的相互关系。该方法不受底层网络物理类型的限制,需要的试验设备及试验人员少,普遍适用于大型局域网网络行为的测量,其主要缺点是缺乏安全机制,但可通过一定的手段进行预防。

业务流级监测是一种新型的网络可靠性监测方法。近年来,以 NetFlow^[10]为代表的业务流级监测技术得到了越来越多的应用,NetFlow 流信息丰富,可以

为流量分布、业务分布等性能分析提供充足的数据。但目前业务流测量技术有很大的局限性:一是消耗网络设备的资源,不能实时捕捉数据包;二是在大中型网络上的各个节点全面部署会产生大量数据,及时准确处理这些数据非常困难。因此 NetFlow 一般比较适合于边缘路由器的单独部署。

2 可靠性分析系统设计

2.1 可靠性分析系统总体结构设计

通过对比可靠性监测方式的适用范围和优缺点,文中设计的园区网可靠性分析系统采用基于 SNMP 的链路级监测方式对原始流量数据进行采集,并运用宏观流量分析策略实时监测网络性能和各种主要业务服务质量。系统主要由四个功能层次组成,分别是:数据采集层、数据管理层、数据分析层和数据展示层。系统功能结构如图 1 所示。

数据采集层从各个被管对象处采集数据,接收陷阱事件,向被管对象发布命令。数据管理层负责各种数据的格式化和数据存储,包括数据的整合、备份以及数据预处理工作,其中预处理工作主要用数据库的存储过程完成。数据分析层对数据采集层采集的数据进行处理分析,形成可靠性参数数据,并负责各类数据的查询、告警和可视化处理。数据展示层按照需求以多种表现形式展示网络性能数据,采用图形用户界面 GUI,以直方图、多维坐标曲线和报表等形式显示目标网络的性能状况,从而为优化和改善网络状况提供合理的依据。

2.2 网络拓扑发现模块

准确发现网络拓扑是实施网络监测与管理的基础,全面、动态地反映网络运行的拓扑状况能够为监测网络性能、排除物理故障、优化网络配置提供支持,也为网络技术人员监视整个网络的可靠性提供有力手段。文中采用基于 SNMP 和 UDP 协议来自动搜索、发现园区网中的所有网络设备以及它们之间的连接关系,从而监测出整个网络的拓扑结构信息。系统要求网内设备支持 SNMP 协议。

(1) 骨干网络拓扑发现。

骨干网络搜索主要是根据查询路由设备的路由表来实现的。SNMP 协议的 MIB 库中存放着网络设备的重要信息,并且 MIB 信息库总能随着网络运行状况自动更新,可以通过获取 MIB 库的信息发现网络节点设备,并绘制网络拓扑图。需要解析的相关路由信息如表 1 所示。

由于路由表中的下一跳地址 ipRouteNextHop 所标识的必然是具有路由功能的网络节点,所以可以从

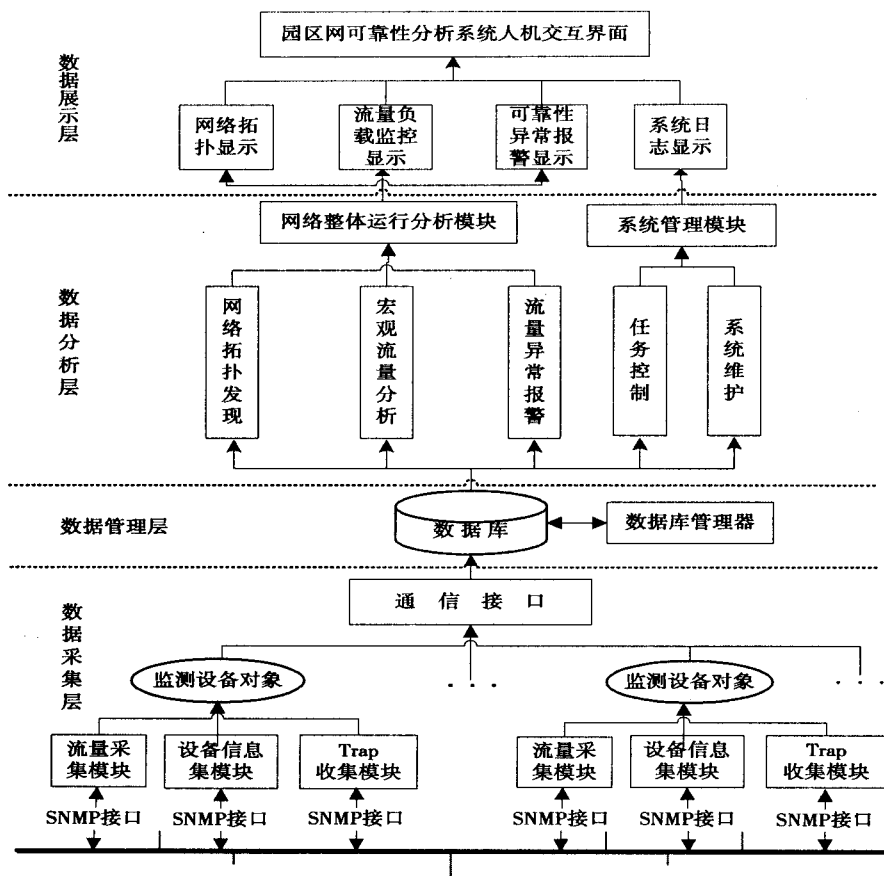


图 1 园区网可靠性分析系统总体功能结构图

表 1 路由 MIB 相关信息

MIB 对象	功能	ASN.1 编码	类型	备注
ipRouteDest	路由的目的地址	1.3.6.1.2.1.4.21.1.1	IpAddress	列对象
ipRouteIfIndex	网关的接口号	1.3.6.1.2.1.4.21.1.2	Integer	列对象
ipRouteNextHop	下一跳路由的 IP 地址	1.3.6.1.2.1.4.21.1.7	IpAddress	列对象
ipRouteType	记录 ipRouteNextHop 表示的地址与连接关系	1.3.6.1.2.1.4.21.1.8	Integer	列对象
ipRouteMask	路由目的地址的子网掩码	1.3.6.1.2.1.4.21.1.11	IpAddress	列对象
ipAdEntAddr	接口的 IP 地址	1.3.6.1.2.1.4.20.1.1	IpAddress	列对象

监控中心的默认网关开始,通过读取路由设备的路由表下一跳信息,由内向外发现网络中的所有具有路由功能的网络节点及其连接关系。从 ipRouteType 的值可以知道该网关连接哪些子网,通过接口表得到的接口类型可以了解子网类型。因此,从起始搜索节点开始,采用广度优先遍历无向图的算法对整个网络系统的路由设备进行遍历,并综合分析路由信息表,就可以发现目标网络的主干拓扑结构,得到网络的主拓扑关系。

相应的拓扑发现算法流程描述如下:

①指定 IP 地址作为拓扑发现的起始节点,同时指定搜索深度,本算法搜索深度为 20。

②从配置文件读取拓扑发现配置信息,初始化如下对象:

seedRouter、communitySnmp ReadList 和 outBoundAddressSets, seedRouter 加入到空队列 nexthopQueue 中。如果 nexthopQueue 为空队列,则转为⑥,否则调用 SnmpPing 测试响应的协议版本号 and 通信口令字。

③如果②中没有找出响应的通信口令字,则分两种情况处理:被测试设备地址为 seedRouter,转为⑧,否则转为④。

④用②中测试成功的协议版本、通信口令字和设备地址作输入参数,调用 GatherRouterInfoAll 采集路由器地址信息 info_ipAd 和路由表信息 info_ipRo;并分析路由表数据,若 ipRouteType 值为 4,记录 ipRouteNextHop 值所代表的设备;若 ipRouteType 值为 3,记录该路由器与子网直接相连。

⑤重复②~④的操作。

⑥分析 info_ipAd:如果两个接口 IP 地址与对应掩码做与运算后得到的网络地址相等,则它们是直接连接或是同一子网间相连。

⑦判断是否达到搜索深度,如果没有,则从②继续执行;若达到搜索深度,根据设备地址表读出设备所有 IP 地址,计算所辖网络中所有可能存在的主机地址集合,为子网拓扑发现做准备。

⑧算法结束。

(2)子网内活动主机的发现。

获取子网内活动主机的传统方法是 Ping 方法,但是目前有些园区网的主机出于安全性考虑关闭了 Ping 响应功能。文中使用如下算法获得子网内活动主机:首先根据骨干网络拓扑发现算法和子网掩码得到各个子网 IP 地址的范围,然后向该子网内所有主机发送 UDP 包,同时指定一个冷僻端口,只要子网内的主机处于运行状态,就会向监测主机返回一条目的端口不可达的 ICMP 报文,监测主机收到 ICMP 后就可以确定活动主机的位置了。园区网网络设备拓扑发现结果如图 2 所示。

2.3 宏观流量分析模块

在发现了园区网拓扑信息之后,就可以从各个网络设备获取流量信息来进行宏观流量采集和监测了。

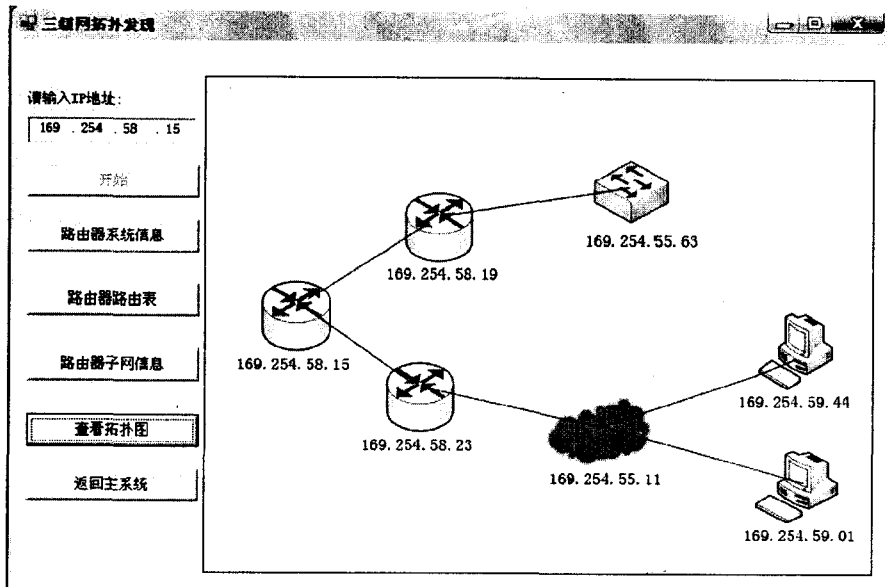


图 2 园区网拓扑发现结果图

文中的宏观流量采集是基于 RMON 的。RMON 是一个标准监测规范,在 RMON 中,网络监测数据包含了一组数据统计、数据分析和数据诊断的性能指标,可以在同步的远程监测器和监测管理站之间进行交换。在流量监测中使用较多的是 Statistics 组和 History 组,表 2 显示了它们所提供的监测子网流量统计信息。

具体的流量分析方法如下。

①接口错误包率和丢包率:

输入错误百分率 = $\text{ifInErrors} / (\text{ifInUcastPkts} + \text{ifInNUcastPkts})$

输出错误百分率 = $\text{ifOutErrors} / (\text{ifOutUcastPkts} + \text{ifOutNUcastPkts})$

输入丢包率 = $\text{ifInDiscards} / (\text{ifInUcastPkts} + \text{ifInNUcastPkts})$

输出丢包率 = $\text{ifOutDiscards} / (\text{ifOutUcastPkts} + \text{ifOutNUcastPkts})$

Get - Request 类型的 SNMP 数据包,在收到这些数据包后,Agent 设备将监控端所请求查询的 MIB 变量值封装到 Get - Response 类型的 SNMP 数据包中,返回给流量采集进程,整个传输过程承载在 UDP 协议之上。所定义的接口信息结构变量名称为表 2 所列的 MIB 对象,数据类型为 unsigned int 型;另外,还要定义代理信息结构和性能管理信息结构。

2.4 流量预测与报警模块

流量分析在某种程度上可以说是统计学意义上的时间序列分析。时间序列分析^[11,12]是根据系统观测得到的动态数据,通过曲线拟和和参数估计来建立数学模型的理论和方法。它一般采用曲线拟和和参数估计方法进行。对于平衡时间序列,可用通用的 ARMA (自回归滑动平均模型)模型拟合。但是,经过对园区骨干网大量流量的测量,从实际采集到的数据序列可以看出,所有流量在正常状态下都不满足平稳性要求,

表 2 需监测的流量 MIB 相关信息

MIB 对象	功能	单位	ASN.1 编码	类型	备注
ifNumber	接口数目	个	1.3.6.1.2.1.2.1	Integer	标题对象
ifIndex	接口索引	无	1.3.6.1.2.1.2.2.1.1	Integer	列对象
ifDescr	接口描述	无	1.3.6.1.2.1.2.2.1.2	DisplayString	列对象
sysUpTime	设备运行时间	秒	1.3.6.1.2.1.1.3	TimeTicks	列对象
ifSpeed	接口带宽	Bit/s	1.3.6.1.2.1.2.2.1.5	Gauge	列对象
ifInOctets	接口接收的字节数	字节	1.3.6.1.2.1.2.2.1.10	Counter	列对象
ifOutOctets	接口发送的字节数	字节	1.3.6.1.2.1.2.2.1.16	Counter	列对象
ifInUcastPkts	接口输入的单播包数	包数	1.3.6.1.2.1.2.2.1.11	Counter	列对象
ifOutUcastPkts	接口发送的单播包数	包数	1.3.6.1.2.1.2.2.1.17	Counter	列对象
ifInNUcastPkts	接口输入的非单播包数	包数	1.3.6.1.2.1.2.2.1.12	Counter	列对象
ifOutNUcastPkts	接口发送的非单播包数	包数	1.3.6.1.2.1.2.2.1.18	Counter	列对象
ifInDiscards	丢弃的输入包数	包数	1.3.6.1.2.1.2.2.1.13	Counter	列对象
ifOutDiscards	丢弃的输出包数	包数	1.3.6.1.2.1.2.2.1.19	Counter	列对象
ifInErrors	错误的输入包数	包数	1.3.6.1.2.1.2.2.1.14	Counter	列对象
ifOutErrors	错误的输出包数	包数	1.3.6.1.2.1.2.2.1.20	Counter	列对象

②接口利用率:

接口每秒通过的字节数 = $((\text{ifInOctets}_y - \text{ifInOctets}_x) + (\text{ifOutOctets}_y - \text{ifOutOctets}_x)) / (y - x)$

然后计算接口的利用率:

利用率 = $(\text{接口每秒通过的字节数} * 8) / \text{ifSpeed}$

③接口输入、输出流量:

接口输入流量 = $\text{ifInOctets} * 8 / (\text{sysUpTime} * 0.01)$

接口输出流量 = $\text{ifOutOctets} * 8 / (\text{sysUpTime} * 0.01)$

进行流量采集时,流量采集进程向路由器或交换机发送

而是呈现出明显的趋势性或周期性,无法直接利用 ARMA 模型对其进行模拟,需要用其它的时间序列模型进行流量预测与报警。文中构建了既有确定性又有随机性流量特点的基于时间因素的组合模型描述设备接口的流量并加以预测和报警。

3 系统体系结构设计

园区网的拓扑结构特点决定了其核心层到汇聚层的链路带宽是整个网络的性能瓶颈。在具有这种拓扑特点的网络中采用集中式的可靠性监测体系结构,采集数据的传输将占用很多瓶颈链路带宽,从而导致网络负载严重不均而降低整体网络的性能,而分布式体系结构有部署复杂的特点。为避免这些缺点,采用监测服务器逻辑分层的概念,将可靠性监测中心分为顶级监测中心和区域代理监测中心。在汇聚层和接入层建立区域代理监测中心,其功能是部分处理本区域的性能采集数据,并把分析结果传送到顶级监测中心。每个区域代理监测中心都运行一个 RMON 代理, RMON 代理在子网内自动收集统计信息供顶级可靠性分析中心查询,并接受其配置, RMON 也能按照管理站的配置自动发送告警信息。

系统采用分布式测量、集中式控制的体系结构和 Client/Server 工作方式,具有较强的灵活性,可有效降低网络负载。

4 结束语

通过对园区网拓扑结构发现、宏观流量监测的分析与研究,设计并实现了基于参数测量的园区网可靠性分析系统。该系统对硬件的要求不高,配置较为简单,只要各网络设备支持 SNMP 协议即可实施,目前绝大多数园区网都满足这个要求。利用所设计的可靠性分析系统,可以很好地对所辖范围内的网络流量数据进行有效监控,为网络管理人员优化网络配置、提高

网络服务质量提供了科学的决策依据。

参考文献:

- [1] 王云光. 浅议计算机网络中的可靠性设计[J]. 微型电脑应用, 2004(7): 29-34.
- [2] Frank H, Frisch I. Analysis and Design of Survivable Network [J]. IEEE Trans. on Communication Technology, 1970, 18(5): 55-60.
- [3] Sawionek B, Wojciechowski J, Arabas J. Synthesis of reliable networks in the presence of line failures[C]//Proceedings of the 2000 IEEE International Symposium on Circuits and Systems. Geneva: [s. n.], 2000: 649-653.
- [4] Aggarwal K K, Chopra Y C, Bajwaj S. Capacity consideration in reliability analysis of communication systems[J]. IEEE Trans. Reliability, 1982, 31(2): 177-188.
- [5] 潘勇. 通信网可靠性指标研究[J]. 电子产品可靠性与环境试验, 2006, 24(1): 1-5.
- [6] Kyandoghere K. Survivability Performance Analysis of Rerouting Strategies in an ATM/VP DCS Survivable Mesh Network [J]. Computer Communication Review, 1998, 28(5): 22-30.
- [7] 杨建华, 谢高岗, 李忠诚. 基于 Linux 内核的流量分析方法[J]. 计算机工程, 2006, 32(8): 67-69.
- [8] IPPM. The Internet Engineering Task Force[EB/OL]. 1990-05. <http://www.ietf.org>.
- [9] McCloghrie K, Rose M. Management information base for network management of TCP/IP-based internets; MIB-II [S]. RFC1213. [s. l.]: Network Working Group, 1991.
- [10] Cisco Systems. Cisco Netflow Introduction [EB/OL]. 2005. <http://www.cisco.com/warp/public/732/Tech/nmp/netflow/index.shtml>.
- [11] 杨叔子, 吴雅, 轩建平, 等. 时间序列分析的工程应用[M]. 第2版. 武汉: 华中科技大学出版社, 2007.
- [12] 武伟, 刘希玉, 杨怡, 等. 时间序列分析方法及 ARMA, GARCH 两种常用模型[J]. 计算机技术与发展, 2010, 20(1): 247-249.

全国“IEEE 标准电脑鼠(智能机器人)走迷宫”决赛

为了培养大学生的科技创新意识和动手设计能力,中国计算机学会微机(嵌入式系统)专业委员会将于11月在北京举办2010全国“IEEE 标准电脑鼠(智能机器人)走迷宫”决赛。

本次比赛规则采用国际最流行的 IEEE 标准电脑鼠走迷宫竞赛规则。在全国各省市建立分赛区,各赛区的一等奖获得者参加北京的总决赛。国际电工和电子工程学会(IEEE)每年都要举办一次国际性的电脑鼠走迷宫竞赛,此次全国决赛优胜者将代表中国参加国际赛事。