网络应用软件监控系统通讯协议设计①

Design of Communication Protocol in Network Monitoring System for Application Software

匡巧艳　徐　成　(湖南大学 计算机与通信学院 湖南 长沙 410083)

摘　要：对简单网络管理协议的协议数据单元进行扩充，设计并实现面向应用软件的网络监控系统。研究管理站点和管理代理监控信息的交换方式，详细地设计了系统中通信协议栈及各组成部分的通讯协议并进行验证，实现了管理站点和管理代理间监控信息实时、准确的交换。达到了管理站点对受控站点上运行的应用程序类中成员变量和成员函数进行有效监控和管理的目的。

关键词：网络应用软件 监控系统 协议栈 协议类型 通讯协议

随着网络规模增大，网络结构及网络应用日渐复杂，传统的物理安全技术和措施已经不足以保证信息系统的安全了，因此网络管理系统作为网络安全运行的保证，其重要性越来越突出。为了提高计算机网络信息安全，许多相关的网络安全产品被开发，但大多是基于网络硬件设备，如路由器，集线器，交换机等，而对网络应用软件的研究和开发相对较少[1]。为了保证网络环境中的应用程序正常高效地运行，笔者设计了基于简单网络管理协议的 ASNMS(Network Monitoring System for Application Software，网络应用软件监控系统)，该系统选择运行于网络环境中的应用程序为研究对象，对简单网络管理协议中管理信息和协议数据单元进行扩充，实现了对网络中运行的应用程序类中成员变量和成员函数的有效监控。本文详细介绍该监控系统中管理站点和管理代理通信协议的设计与验证。

1　网络应用软件监控系统(ASNMS)

网络应用软件监控系统(ASNMS)的主要监控目标是网络中的应用软件，通过及时获取软件中重要变量值(如系统配置、状态指示等)，从而及时了解整个网络中应用程序的状态[2]，并且还可以通过管理站点对各受控站点中的应用程序进行控制操作，提高整个网络和应用系统的安全性。

该网络应用软件监控系统主要有三个模块：

a. 管理站点主程序。该程序在管理站点上运行。通过该程序，管理站点可以使用 UDP/IP 协议与管理范围内的所有受控站点进行通信，收集网络应用程序的监控信息，并下发各种控制命令。

b. 管理代理。每一个受控站点上运行一个管理代理程序(有且仅有一个)。管理代理是系统的通信中心。一方面，通过内存映射文件与受控站点上的各应用程序实例进行通信，收集各应用程序实例的监控信息[3]。另一方面，通过 UDP 协议与管理站点通信，发送受控站点的管理信息以及转发管理站点的控制信息。

c. 监控模块。监控模块是供软件开发人员使用的一个通用接口模块。它负责从受控应用程序中获取监控信息，发送到管理站点，并且也能接收从管理代理转发的管理站点命令，对受控应用程序执行一定的控制操作。从结构上来看，监控模块附属于受控应用程序，但它以单独的线程形式存在。

2　协议数据单元的定义

2.1 ASNMS 协议栈

由于 ASNMS 系统提供给管理站点一个整个监控范围内管理信息树的直观映射，同时采用 UDP 协议作

① 基金项目:湖南省自然科学基金项目(04JJ6036)
收稿时间:2008-09-10

为监控系统传输协议的下一层协议，这不像 TCP 协议那样能保证数据传输的正确性和顺序性，因此需要对简单网络管理协议中的协议数据单元加以扩充[4]。ASNMS 系统的协议栈如图 1 所示。其中：MCSP 为 Monitor & Control System Protocol；RRP 为 Register Request Protocol；GDP 为 Get Data Protocol；SDP 为 Set Data Protocol；SSP 为 Set Setting Protocol；REP 为 Response Protocol；TRP 为 Trap Protocol；INP 为 Inform Protocol。

RRP	GDP	SDP	SSP	REP	TRP	INP
MCSP						
UDP						

图 1　ASNMS 的协议栈

MCSP 的报文格式如图 2 所示，其中：协议标识字段为 MCSP，版本号为 1。报文序列号、包数、包号、包长度、标志 5 个字段是为完成报文的分解、重组及正确传送所设。数据字段内部包含的是 MCSP 的上层协议内容。协议类型字段用于区分上层协议的类型，具体含义如表 1 所示。

协议标识(1)	版本号(1)	协议类型(1)	报文序列号(2)	包数(2)	包号(2)	包长度(2)	标志(1)	数据(≥0)

括号中数字为字节

图 2　MCSP 的报文格式

表 1　协议类型及作用

字段值	协议类型	协议作用
1	RRP	管理站点要求管理代理向其注册
2	GDP	管理站点向管理代理搜集管理信息子树中被管对象的值
3	SDP	管理站点向管理代理设置管理信息子树中被管对象的值
4	SSP	管理站点对管理代理的管理信息子树进行配置
5	REP	管理代理对管理站点各项请求的回应
6	TRP	管理代理对管理站点设置的陷阱做出回应
7	INP	管理代理向管理站点通知管理信息子树的最新变化

2.2 通讯协议

2.2.1 注册请求协议（RRP）

管理站点要求管理代理注册的报文有 3 种：强制注册(广播)、中途注册(广播)、出错后的强制注册[5]。注册请求报文的报文格式如图 3 所示，其中：NAME 为管理站点的名字；IP 为管理站点的 IP 地址；TYPE 为注册请求的类型，0 表示强制注册，1 表示中途注册；TIMER 为系统缺省的定时时间间隔，单位为秒。

NAME(16)	IP(16)	TYPE(1)	TIMER(2)

括号中数字为字节

图 3　注册请求报文格式

2.2.2 数据请求协议(GDP)

数据请求报文的报文格式如图 4 所示，其中：IP 为管理站点的 IP 地址；PATH 为请求数据的管理信息树分支的根节点的管理对象路径；NAME 为请求数据的管理信息树分支的根节点的名字，即 PATH 所表示节点的名字；NUM 为数据项号，可选字段，表示所请求的数据是表格中的第几项。

IP(16)	PATH(16)	NAME(20)	NUM(2)

括号中数字为字节

图 4　数据请求报文的报文格式

2.2.3 数据设置协议(SDP)

数据设置协议与数据请求报文的报文格式相似，只是多一个 VALUE 字段，表示所要设置的值。

2.2.4 配置设置协议(SSP)

ASNMS 的一个重要特点是可以对管理代理上的管理信息树进行配置。这将大大提高监控系统的工作效率及其灵活性和及时性。配置报文分 4 类：

a．定时设置：设置注册请求协议报文的 TIMER 字段。

b．阈值设置：设置那些有着明显值域又有比较敏感要求的被管对象值的范围[6]，当被管对象的值超出阈值时，管理代理将马上以 Trap 报文的形式向管理站点报告。

c．阈值失效设置：当管理站点收到管理代理发来的第一个 Trap 报文后，应马上向该代理发送阈值失效设置报文，使设置在该被管对象上的阈值无效[7]。

d．取消设置：管理站点退出前，在管理范围内的网段上发送一个取消设置的广播。

2.2.5 响应请求协议(REP)

对于管理站点发来的各个请求报文，管理代理都要作出回应，向管理站点回送响应请求报文。根据管理站点发来的不同的请求报文，管理代理回送不同的响应报文。响应请求报文有以下 5 种：注册请求响应报文；数据请求响应报文；数据设置响应报文；配置设置响应报文和出错响应报文。

2.2.6 陷阱响应协议(TRP)

陷阱响应是指当管理代理的管理信息树发生特定事件时，管理代理主动向负责的管理站点报告，而不必等待管理站点的请求，以保证管理站点能及时得知这些事件并加以处理。目前 ASNMS 系统定义了下述特殊事件：添加节点事件、删除节点事件、管理代理退出事件和阈值突破事件。

陷阱响应的协议报文格式如图 5 所示，IP 为发生事件的管理代理的 IP 地址；TYPE 为事件类型；DATA 为所传送的数据。

IP(16)	TYPE(1)	DATA(n)

括号中数字为字节

图 5　陷阱响应报文的报文格式

2.2.7 通知响应协议(INP)

管理代理根据管理站点定时设置启动定时器，当定时时间到时，向管理站点发送通知响应报文，将本地管理信息树中所有发生值变化的管理对象节点的新值反映到管理站点上，使管理站点上的管理信息树映射能够反映被管理区域内的管理信息树的最新变化。

通知响应的协议报文格式如图 6 所示，IP 为发送通知响应的管理代理的 IP 地址；NUM 为所传送的管理对象节点的个数；DATA 为该字段为管理代理上值发生变化的管理对象节点的信息的集合。

IP(16)	NUM(2)	DATA(n)

括号中数字为字节

图 6　通知响应报文的报文格式

3　协议验证

以 VisualC++作开发工具，采用 SOCKET 编程技术和客户机/服务器通信方式在 ASNMS 系统中实现了 MCSP 协议的验证。实现中通过对套接字类 CSocket 进行派生，生成 CSecSocket 类实现 MCSP 中 RRP、GDP、SDP、SSP、REP、TRP 和 INP 等 7 个协议。借助 WinSNMP API 函数库在 ASNMS 系统管理站点和管理代理间的通信过程中完成了对 MCSP 协议的验证。管理站点和管理代理间的通信步骤及程序中用到的主要函数如下：

第 1 步：应用函数 Snmpstartup()，SnmpSetTranslateMode()和 SnmpSetRetmusmitMode()进行 WinSNMP 通信的初始化。

第 2 步：应用函数 SnmpCreateSession()生成 WinSNMP 会话句柄。

第 3 步：根据设定的 IP 地址，应用函数 SnmpStrToEntity()将源和目标机器的 IP 地址转换为实体句柄。

第 4 步：调用函数 SnmpStrToContext()将设定的团体名转换为安全控制的上下文通信句柄。

第 5 步：调用函数 SnmpCreateVb()和 SnmpSet-Vb()生成并绑定待访问的管理信息库中管理对象标识符。

第 6 步：调用函数 SnmpCreatePdu()生成 SNMP 通信协议数据单元。

第 7 步：发送请求访问报文 SnmpSendMsg()。

第 8 步：接收从代理返回的请求响应报文 Snmp-RecvMsg()。

第 9 步：从接收到的响应数据中分析欲获得的结果值。

第 10 步：关闭通信过程中生成变量所占用的内存空间。

4　小结

对 ASNMS 系统中通信协议栈及各组成部分通讯协议的具体报文格式进行了设计，它具有以下特点：

a. 管理代理向管理站点注册的类型不同，发送数据类型的标志就会不同，管理站点可以很方便地知道某个数据包来自于哪个管理代理。此外，管理站点要求管理代理先向其注册才能够发送数据，大大提高了数据传输的安全性。

b. 管理站点可以向管理代理指明所要查询数据的 MIB 路径，而不是笼统的 get-next 操作，大大提高了管理站点的工作效率。

c. 配置设置协议使得 ASNMS 系统可以对管理代理上的 MIB 树进行配置，大大提高了监控系统的工作

(下转第 160 页)

(上接第 78 页)
效率及其灵活性。

d. 当管理代理发生特定事件时，管理站点可以实时知道所发生的事件，对其做出响应。此外，管理站点还可以设置定时器，当定时时间到时，管理代理会主动向管理站点发送通知响应报文，大大提高了监控系统的实时性。

参考文献

1 王娜,王亚弟,汪斌强.一个适用于分布式入侵检测系统的安全通信协议.计算机工程, 2006, 32(12): 157－159.

2 林立新,蒋新华,陈特放.网络监控原理及实现.计算机工程, 2004,30(7):92－94.

3 Hunter P. Integrated security and network management remain elusive. Network Security, 2004,10(6):15－16.

4 Bhutani, Kiran R, Khan, Bilal. Optimal distribution of a hierarchy of network management agents. Information Sciences, 2003,149(4):235－248.

5 Comer DE, Stevens DL. Internetworking With TCP/IP Vol II：Design, Implementation, and Interanls. 北京:清华大学出版社, 1998.

6 Lety E, Turletti T, Baccelli F. SCORE: a scalable communication protocol for large-scale virtual environments. IEEE/ACM Transactions on Networking, 2004,12(2):247－260.

7 Gambiroza V, Yuan P, Balzano L, et al. Design, analysis, and implementation of DVSR: a fair high-performance protocol for packet rings. IEEE/ACM Transactions on Networking, 2004,12(1):85－102.