

家庭网络设备远程管理协议的研究

王 芳,孙运强,姚爱琴

(中北大学 信息与通信工程学院,山西 太原 030051)

摘 要: 针对家庭网络终端设备的复杂性和业务的多样性引发的终端管理问题,在研究各网络管理协议的基础上,着重介绍了管理体系协议 TR069 规定的网管构架、网管功能及其安全性。

关键词: 家庭网络;远程管理;协议

中图分类号: TP393

文献标识码: A

Research of equipment remote management protocol in home networks

WANG Fang, SUN Yun Qiang, YAO Ai Qin

(Institute of Information and Communication Engineering, North University of China, Taiyuan 030051, China)

Abstract: The complexity of customer premises equipment (CPE) and the diversity of services indicate the problems of the terminal device management for home networks. Based on further study of network management protocols, the paper presents emphatically the protocol TR-069, involving the framework of network management, the function of network management and the sake of security.

Key words: home networks; remote management; protocol

随着宽带市场的高速发展、宽带用户的增多和宽带接入网络的增大,宽带业务的开户、管理和维护问题也越来越突出,越来越迫切。作为宽带网络接入设备的用户端设备,由于数量众多、布放分散,它的放号、维护、诊断和升级都需要运营商的维护工程师上门服务,使其成为宽带接入网络运维问题中的最突出问题。为了有效降低运维成本,提高用户满意度,在传统的电信网络设备的管理框架、商业模式和业务流程内,构建一个低成本、高效率的宽带运营管理系统,已经成为宽带接入市场的重要问题。而对数量最多、故障最为集中的用户端设备的远程集中管理维护系统,则成为重中之重的问题。可见,终端设备的远程管理和维护是非常必要的^[1]。

从目前运营商的需求来看,家庭网络管理的任务包括:状态管理,监视联网家电运行状态;设备控制,通过家庭网络远程控制联网家电;服务管理,自动发现和配置联网家电提供的服务;名字管理,在家庭网络中维护一个可以唯一标志联网家电的名字空间。下面将对家庭网络设备远程管理的相关技术进行介绍。

1 家庭网络设备远程管理的相关协议

家庭网络设备远程管理需要解决的技术问题主要是管理通道和管理协议。远程管理的信息承载在 IP 包上,管理通道问题主要是解决如何传送承载管理信息的 IP 包,这主要与具体的接入技术相关。如何保证管理通道的可用性和管理通道的带宽是目前相关接入技术需要解决的问题。管理协议主要是指 IP 层之上的管理内容传送协议。管理协议的选择主要需要权衡安全性和协议复杂性。目前主要是 DSL FORUM 制定的 TR-069。

1.1 简单网络管理协议 SNMP

1987 年 11 月发布的简单网关监控协议 SGMP (Simple Gateway Monitoring Protocol), 成为第一个专门为网络管理提出的协议。该协议提出了直接监控网关的方法。简单网络管理协议 SNMP (Simple Network Management Protocol) 建立在 SGMP 的基础上, SNMP 最初只是作为一种临时解决方案被提出,但如今已经成为了事实标准,而且是目前最常用的环境管理协议,它最重要的思想是要尽可能简单。SNMP 首先是由 Internet 工程任务组

网络与通信 Network and Communication

织 IETF 的研究小组为了解决 Internet 上的路由器管理问题而提出的。SNMP 提供了一种从运行网络管理软件的中央计算机来管理网络设备的方法,并提供了一种从网络上的设备中收集网络管理信息的方法,也为设备向网络管理工作站报告问题和错误提供了一种方法。

随着未来的网络管理智能化趋势,网络规模日趋加大、设备种类更加复杂、需要更强大功能,网络管理协议也会随之作相应变动,这些都需要更多的安全作保障。然而,在 SNMP 的整个应用过程中,出现了许多安全方面的问题。SNM-Pv1 和 SNM-Pv2 协议仍存在内容被篡改等漏洞,虽然 SNM-Pv3 协议就安全方面做了很大的努力,但由于复杂性使其推广受到限制^[2]。

1.2 家庭网络管理协议 HNMP

针对家庭网络的特定结构以及 SNMP 的简单性,有人提出了一个新的家庭网络管理协议 HNMP (Home Network Management Protocol),它把 SNMP 协议延伸到家庭网络。HNMP 模型对家庭内部网络进行管理,不仅可以描述各种各样的家电设备参数,并对其进行管理,而且具有简单、无需用户自己配置的特点,可以达到即插即用的效果,为远程控制家庭信息设备打下了基础。它的主要功能是管理联网家电的运行状态,并且和 SNMP 模型兼容。但是对于网络接入和网络服务分离的接入网模型(目前国外一般都属于这种模型),SNMP 这种集中式的网络管理协议并不能满足要求,这就需要一种新的管理模型^[3]。

1.3 改进的家庭网络管理协议 EXHNMP

与一般的网络管理相比,家庭网络管理不仅是对联网家电的状态和行为进行管理,还要对联网家电能提供的服务进行管理。在家庭网络中,不同的联网家电提供五花八门的服务,这些服务之间可能还有复杂的依赖关系,同时,家庭网络中的服务的配置必须是自动完成的,不需要人为干预,需要是家庭网络的管理协议能够自动发现和配置家庭网络上的这些服务。HNMP 考虑了联网家电的运行状态的管理,并没有考虑家庭网络上服务的管理。针对此局限性,对 HNMP 协议进行了改进和扩展得出 EXHNMP。

EXHNMP 是一个分布式的家庭网络管理协议,联网家电可以对等地直接控制网络上的其他联网家电;EXHNMP 还引入了简单的服务管理,联网家电可以根据任务自动选择适当的服务;EXHNMP 是对家庭通过由管理信息库(MIB)中扩展的管理对象描述的服务,EXHNMP 使得联网家电对家庭网络上的服务进行检索和匹配并根据要完成的任务查找适当的服务及其提供者。事实上,EXHNMP 中对 MIB 的服务对象的描述还相对简单,不能精确地定义

服务的细节,因此服务的匹配不能非常准确^[4]。

1.4 CPE 广域网管理协议

TR-069 协议是当今宽带领域最受关注的管理体系协议,其全称为“CPE 广域网管理协议”。它在 2004 年 5 月由 DSL Forum 提出,并且还在不断地更新中。它规定了家庭网关进行远程管理配置时的通用框架和协议,用于从网络侧对家庭网关进行远程集中管理。该协议支持对设备的自动配置,软件和固件的升级管理,以及监测设备的状态和性能,并能对设备故障进行诊断。TR-069 协议可以认为是 DSL Forum 关于家庭网络一系列设备远程管理的基础,在支持设备远程管理方面具有很大的优势。该协议正成为各设备运营商在采购设备时,要求设备必须支持的管理协议。因此,为使各种家庭设备特别是家庭网关设备支持远程管理的功能,TR-069 协议采用了成熟的通信协议,开放的面向对象的管理信息架构,具有强大的灵活性和可扩充能力^[5]。

2 TR-069 协议

TR-069 广域网网络自动管理协议是 DSL 论坛定义的终端管理框架的一部分,TR-069 CPE 广域网网络自动管理协议负责三层以上复杂业务的配置过程。它的核心思想是通过定义一套 ACS 和 CPE 之间自动协商交互协议,实现终端的自动配置的过程。TR-069 规范主要由自动配置管理服务器(ACS)、用户驻地设备(CPE,即被管终端)、业务配置管理服务器以及一些必要的管理接口组成。它通过定义一套 ACS 和 CPE 之间自动协商交互协议,实现终端的自动配置和动态的业务发放,软件/固件映像管理与升级,状态、性能监视以及诊断功能^[6]。

基于 TR-069 的网管构架如图 1 所示,宏观上主要有 2 个接口,一个是完成从业务或服务提供商向 ACS 下发业务配置的北向接口(ACS Northbound Interface),另外一个完成从 ACS 到 CPE 配置管理的南向接口(ACS Southbound Interface)。

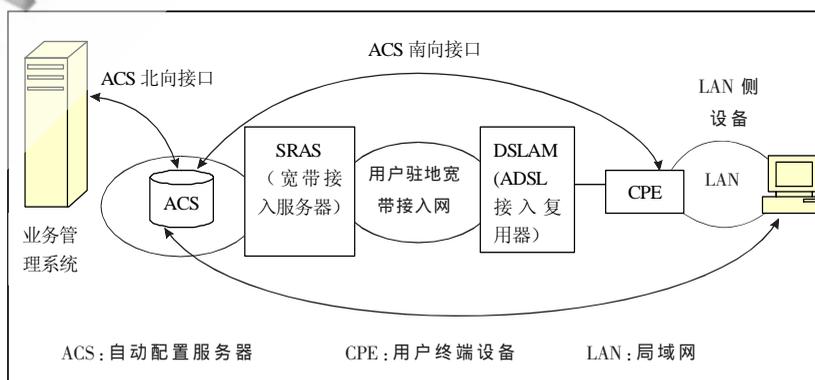


图 1 基于 TR-069 的网管构架

TR-069 设备广域网配置管理框架是一种被动式的管理模型,与 SNMP 主动管理模式不一样,它不要求设

网络与通信 Network and Communication

备一直在线,也不需要检测终端设备是否在线,所有的请求都由终端设备发起,服务器只是被动地处理请求,能够适应终端设备数量巨大、地域分散的特点,具有更好的鲁棒性和适应性。

2.1 TR-069 协议栈结构

TR-069 协议采用了许多现存的、标准的协议以获得最广泛的设备支持。采用 IP 协议来保证 TR-069 协议独立于网络传输的物理介质,采用 SOAP 协议来保证 TR-069 设备具有互操作能力,采用 XML 来对设备和服务进行统一的描述,采用 HTTP 协议来进行 TR-069 设备的信息交互,采用 RPC 方法实现 CPE 与 ACS 之间的交互,采用 SSL/TLS 增加网络传输的安全。采用这些现存的、广泛应用的协议能减少开发 TR-069 设备的工作量,使 TR-069 设备更好地融入现有网络。CPE WAN 管理协议中定义的协议栈如表 1 所示。

表 1 TR-069 协议层次

协议层次	描述
CPE/ACS 管理应用	CPE/ACS 使用此协议的应用程序
RPC 方法	远程过程调用方法
SOAP	简单对象访问协议
HTTP	超文本传输协议
SSL/TLS	传输层安全协议
TCP/IP	传输控制协议/网间协议

TR-069 协议中使用的这些成熟层次之间有非常紧密的联系。TR-069 协议的最终目的是建立一个可用的设备管理应用协议,它是一个多层协议构成的框架体系,每一层都以相邻的下层为基础,同时又是相邻上层的基础。TCP/IP 是通用的互联网传输协议,SSL/TLS 则是出于安全的考虑,属于可选的协议层次,HTTP 则是标准的传输会话协议,用于客户端与服务器的会话管理,而 SOAP 则是用于对上层应用协议内容的编码。由此可见这些协议层次是一个完整的网络应用协议的典型结构,功能完善,结构简洁明了,它们是缺一不可的整体。

2.2 基于 TR-069 实现的网管功能

TR-069 协议的管理内容包括设备的自动配置及动态业务发放、软件/固件升级、状态和性能监测以及故障诊断。

(1) 设备的自动配置及业务动态发放

CPE 在与 ACS 利用 TR-069 协议进行交互过程中对自己做出标识(例如型号、版本等),而 ACS 则根据这些特定的标识设定特定的规则,对某个特定的用户或者某类特定的设备进行配置信息的更新或者业务的发放。在该协议中,CPE 在开机后自动请求 ACS 中的配置信息,而 ACS 也可在任意需要的时刻主动进行配置或者业务下发。通过这样的设置,用户可以实现对设备的“零配置安装”,而 ACS 可以从 WAN 侧动态地监控设备参数的

改变。

(2) 设备的软件或固件升级

由于 ACS 可以识别 CPE 的设备标志以及其软件的版本号,所以 ACS 一旦发现 CPE 的软件或者固件需要升级时,就会要求 CPE 远程更新其软件或固件。由于在 TR-069 协议中提供了文件下载的功能,因此 ACS 指定新的软件或者固件文件的地址,让 CPE 到指定位置下载文件即可,CPE 在文件下载结束后会通告 ACS 文件下载的结果。

(3) 设备的状态和性能监测

ACS 通过协议规定的 RPC 方法读取 CPE 中参数的值,从而可以监控设备的当前状态,以判定设备当前是否处于正常工作状态。同时 ACS 通过对一些反应 CPE 性能状态的参数的检测,也可以知道 CPE 性能是否变坏。

(4) 故障诊断

TR-069 中定义了一系列的参数用于设备故障的诊断,当设备发生故障后,可以读取相应的参数来诊断故障的发生。ACS 也可以通过要求 CPE 上传设备的日志文件来分析 CPE 的历史状态和操作等,以更好地找到故障发生的原因,从而能对设备做有针对性的修复,降低设备的故障率。

2.3 TR-069 协议的安全性

由于 TR-069 是一个远程设备管理协议,所以 CPE 和 ACS 间通信的安全性是很重要的。因此,TR-069 推荐使用 SSL/TLS 安全套接口层协议。SSL 是一种安全通信协议,它提供了 2 台计算机之间的安全连接,对整个会话进行了加密,从而保证了安全传输。SSL 协议建立在可靠的 TCP 传输控制协议之上,与上层协议无关,各种应用层协议(如:HTTP、FTP、TELNET 等)能通过 SSL 协议进行透明传输。在 TR-069 协议中采用 SSL/TLS 和 TCP 有以下一些限制:SSL/TLS 的版本必须是 SSL3.0 或者 TLS1.0,并且加密算法长度要大于或等于 128 位;CPE 必须用 ACS 提供的证书认证 ACS;ACS 可以接收一个有效的 CPE 提供的证书来认证 CPE,但是如果 CPE 不提供证书,ACS 必须允许 SSL/TLS 连接建立。

采用 SSL/TLS 的方法虽然可以解决通信安全性的问题,但是在 TR-069 中却将此协议作为可选而不是必须的。这是因为 SSL 在实现时需要的代码量比较大,增大了整个协议的复杂度,需要更大的存储器容量,而这对一般的数字家庭设备来说是很宝贵的资源。因此,TR-069 采用 HTTP 的摘要认证来作为 SSL 的补充,即:如果不使用 SSL 来保证通信安全性,ACS 必须对 CPE 采用 HTTP 的摘要认证方式进行认证。

本文通过对设备远程管理相关协议的优劣做了详细的研究后,从协议栈结构、实现的网管功能及其安全性,重点介绍了目前宽带领域最受关注的管理体系协议

(下转第 54 页)

技术与方法 Technique and Method

5 改进的算法例证

使用参考文献[6]中的决策表,分别采用本文算法与基于差别矩阵的属性约简算法(老算法)进行比较。表1为所用决策表,表2为其对应的特征矩阵,表3为本文算法所对应的辨识集。

表1 决策表^[6]

U/C	O	T	H	W	D
1	sunny	hot	high	false	N
2	sunny	hot	high	true	N
3	overcast	hot	high	false	P
4	rain	mild	high	false	P
5	rain	cool	normal	false	P
6	rain	cool	normal	true	N
7	overcast	cool	normal	true	P
8	sunny	mild	high	false	N
9	sunny	cool	normal	false	P
10	rain	mild	normal	false	P
11	sunny	mild	normal	true	P
12	overcast	mild	high	true	P
13	overcast	hot	normal	false	P
14	rain	mild	high	true	N

表2 对应的特征矩阵

O	OT	OTH	OTHW	TH	OTH	THW	OTW	OH
OW	OTW	OTHW	OTW	THW	OTHW	TH	OT	OHW
OTHW	THW	W	O	OW	TW	OT	OTH	OTW
OT	OT	THW	OTHW	TH	OH	HW	OW	OTH
OTW	W	THW	OTH	OTHW	HW	TH	OW	OTHW

表3 本文算法的辨识集

$O, OT, OTH, OTHW, TH, THW, OTW, OH, OW, OHW, W, TH, HW$

采用本文算法生成 $D(U, C) = \{O, OT, OTH, OTHW, TH, THW, OTW, OH, OW, OHW, W, TH, HW\}$, 需要比较的次数为: $(9+9+3 \times 3+6+2+5+5) \times 5 = 45 \times 5 = 225$ 。选择核时 $D(U, C)$ 内部比较的次数为 13 次, 各个核生成 $\{d | m \in d, d \in D(V, C)\}$ 时需比较 $13 \times 2 = 26$ 次(有 2 个核), 核选择

后, $B = \{W, O\}$ $D(U, C) = \{TH\}$; 下一步选择 T 或 H 只需要比较 1 次即可, $B = \{T, W, O\}$ 或 $B = \{H, W, O\}$, $D(U, C) = \{\}$, 算法结束。因此本文算法总的比较次数为: $225 + 13 + 26 + 1 = 265$ 次。每个属性元素存储时占 1 个存储单元, 则本文算法只需要 30 个存储单元。而在参考文献[7]中分析的老算法的比较次数为 447 次, 存储单元需 116 个。性能对比如表 4 所示。可见本文改进的属性约简算法大大提高了算法的效率。

表4 新老算法性能比较

	本文改进算法	老算法
比较次数	265	447
所需存储单元数	30	116

本文在分析传统基于辨识矩阵属性约简的基础上, 提出了一种基于辨识集的属性约简算法, 该算法无论在空间使用上还是在时间性能上都优于传统的基于辨识矩阵的属性约简算法, 例证证明了本算法的优点, 在属性约简中有一定的实用价值。

参考文献

- [1] PAWLAK Z. Rough sets[J]. International Journal of Information and Computer Sciences, 1982, 11(5): 341-383.
- [2] LIANG J Y, CHIN K S, DANG C Y, et al. A new method for measuring uncertainty and fuzziness in rough set theory[J]. International Journal of General Systems, 2002, 31(4): 331-342.
- [3] 徐章艳, 杨炳儒, 宋威, 等. 一种快速计算 HU 差别矩阵的属性约简算法[J]. 小型微型计算机系统, 2008, 29(10): 1820-1827.
- [4] 杨明, 杨萍. 基于广义差别矩阵的核和属性约简算法[J]. 控制与决策, 2008(29): 1049-1054.
- [5] 王柯, 朱启兵. 一种基于差别矩阵的启发式属性约简算法[J]. 计算机工程与科学, 2008, 30(6): 73-75.
- [6] 赵卫东, 戴伟辉. 基于特征矩阵的决策表约简研究[J]. 系统工程理论与实践, 2003, 23(3): 65-69.
- [7] 曾黄麟. 智能计算[M]. 重庆: 重庆大学出版社, 2004.

(收稿日期: 2009-06-04)

(上接第 51 页)

TR-069。虽然通过部署基于 TR-069 的网管系统, 可以在很大程度上减少用户的配置和管理工作, 提高设备的易用性和可管理性, 便于家庭网络中设备的快速部署和业务的迅速开展。但从协议目前的发展情况来看, TR-069 仍然处于一个不断完善的过程中, 在业务参数模型上还需要加入对更多的终端业务和特性的支持。

参考文献

- [1] 宋臣. 终端自动配置管理研究[D]. 成都: 西南交通大学, 2006.

- [2] 彭淑静. SNMP 网络管理系统技术. 甘肃科技纵横, 2008, 38(2).
- [3] LIU Yun Xin, ZHANG Yao Xue. HNMP: a digital home network management model. ACTA Electronica Sinica, 2001.
- [4] 王勇, 张尧学, 方存好. 一种改进的家庭网络管理协议—ExHNMP. 小型计算机微型系统, 2004, 25(7).
- [5] DSL Forum. CPE WAN management protocol [S]. Tech. rep. 069, May 2004.
- [6] 王远波. 家庭网关远程管理功能模块的设计与实现[D]. 武汉: 华中科技大学, 2009.

(收稿日期: 2009-06-04)