

基于 SNMP 和 AHP 的网络设备安全态势分析系统

汪涛, 石润华, 罗斌, 汤进

(安徽大学 计算机科学与技术学院, 安徽 合肥 230039)

摘要:为了解决日益严峻的网络设备安全形势,设计并实现了一种网络设备安全态势分析的综合分析方法和分析系统。首先,引入了运筹学中经典的决策方法—AHP,并且提出了一种网络设备安全态势分析的综合分析方法;然后,设计了一个网络设备安全态势分析的模型与框架;最后,基于 SNMP 协议,实现了该分析系统。实验结果表明该系统能够实时、有效地分析网络设备的安全态势,并且对异常的安全态势进行实时地报警,从而达到了对网络设备的实时监控和管理。

关键词:简单网络管理协议;层次分析法;网络设备;安全态势分析;方差

中图分类号:TP393

文献标识码:A

文章编号:1673-629X(2012)01-0238-04

Analysis System of Network Device Security Situation Based on SNMP and AHP

WANG Tao, SHI Run-hua, LUO Bin, TANG Jin

(School of Computer Science & Technology, Anhui University, Hefei 230039, China)

Abstract: To solve the insecurity of network devices, it is necessary to design a system about the analysis of network device security situation. Firstly, import the classical decision-making approach in operational research—AHP, and propose an integrated approach about the analysis of network security situation. Then, design a model and framework about network device security situation. Finally, based on SNMP protocol, realize this system. The experimental results show that the system can real-time and effectively analyze network device security situation, and also alarm the abnormal security situation, so as to achieve real-time monitoring of network equipment and management.

Key words: SNMP; AHP; network device; security situational awareness; variance

0 引言

随着网络系统及其应用日趋复杂,传统网络安全工程的理论和方法受到了挑战,单一的检测方法或检测系统难以有效地检测出复杂的网络安全事件。尽管目前出现一些采用中心管理控制平台和检测引擎组成的分布式结构的网络入侵检测系统,但它们大多只解决了大规模网络环境下检测任务的分布问题求解,没有做到安全信息高层知识融合^[1],也没能实现对系统整体安全态势的有效分析^[2]和评估^[3]。因此,面向大规模复杂网络环境,在更大范围内融合更多的信息,提高系统对安全事件的检测以及对网络系统的整体安全

态势进行估计的能力,是下一代网络安全事件检测评估的发展趋势。目前对网络设备安全态势分析^[4]的研究成果并不多,理论体系和方法也还不完善。所以,文中就是在这样的前提下,提出了一套网络设备安全态势分析理论,并使用该理论完成了一套基于 SNMP^[5](简单网络管理协议)和 AHP^[6,7](层次分析法)的网络设备安全态势分析系统的设计与实现。

1 背景知识介绍

SNMP 协议定义在 IP 协议上,使用无连接的 UDP 进行通信。其定义了使用到的传输层协议、支持的操作与 PDU 结构、操作的时序、角色、实例取值、共同体、管理信息结构 SMI,管理信息库 MIB 等。SNMP 支持 5 种基本操作^[8],即 GetRequest、GetNextRequest、SetRequest、GetResponse 和 Trap,这 5 种操作有各自的 PDU 结构。SNMP 采用的是一个请求对应一个应答的通信方式,但 Trap 除外,Trap 不需要应答。因为

收稿日期:2011-06-01;修回日期:2011-09-19

基金项目:国家自然科学基金(61073116);安徽高校省级重点自然科学基金项目(KJ2010A009, KJ2010A006)

作者简介:汪涛(1989-),男,安徽合肥人,硕士研究生,主要从事图像处理与模式识别研究;罗斌,教授,博导,主要从事图像处理与模式识别研究。

Trap 的发送方向是从代理发送到管理站。

层次分析法 (AHP) 是由美国运筹学家匹茨堡大学教授萨蒂于 20 世纪 70 年代初,提出的一种层次权重决策分析方法。这种方法的特点是在对复杂的决策问题的本质、影响因素及其内在关系等进行深入分析的基础上,利用较少的定量信息使决策的思维过程数学化,从而为多目标、多准则或无结构特性的复杂决策问题提供简便的决策方法。

矩阵归一化^[9]是一种简化计算的方法,将矩阵中的有量纲的表达式转化成无量纲的表达式。通过归一化可以给矩阵的每个元素配一个权值,然后计算出加权平均值,那么这个值就可以作为综合评价的一个很客观的指标。

2 网络设备安全态势的分析方法

在这部分,提出了一种网络设备安全态势分析的综合方法。其具体的描述如下。

2.1 指标的确定

通过咨询网络系统管理员以及通过其他渠道查询影响设备健康指数的因素,确定了健康指数 S 包含下列指标,见公式(1)。

指标

代号

CPU 利用率

X_1

内存使用率

X_2

输入带宽利用率

X_3

输出带宽利用率

X_4

S

(1)

2.2 指标的同趋势化处理

指标的同趋势化变换的思想是:把反向指标化为正向指标,对绝对值反向指标 X 使用倒数 $1/X$,对相反数反向指标使用差值法 $(1 - X)$ 。在处理的过程中,CPU 利用率可以直接从设备的 MIB 库中获得,而内存使用率可以通过获得的内存使用情况除以设备的总内存得到。同时,用 Input 表示设备输入的实时流量,用 $\Delta \text{IfInOctets}$ 表示两次取回的输入字节计数器值的差。

假设取数据时间间隔为 60 秒,那么,这一分钟内的平均实时数据流量就是:

$$\text{Input} = \frac{\Delta \text{IfInOctets} * 8}{60}$$

(2)

如果要获得整个网络设备的流量信息,那么就需要将该设备的所有端口流量加在一起,所以,输入的带宽利用率为:

$$X_3 = \frac{\text{Input} * 100}{65535}$$

(3)

按照同样的计算方式,可计算设备的输出带宽利用率 X_4 。

2.3 数据归一化处理

为了消除不同量纲对评价结果的影响,使得评价的多指标在同一个量纲体系下进行比较,需要对取得的数据进行归一化处理,方法为:

$$Z_i = X_i / \sqrt{\sum_{i=1}^4 X_i^2}, i = 1, \dots, 4$$

(4)

2.4 比较矩阵 A 的确定

在层次分析法中,建议计算比较矩阵的方法是“成对比较法”,即每次只比较两个指标重要性的比值: $a_i/a_j, i, j = 1, \dots, n$ 。另外,AHP 还建议估计 a_i/a_j 时,采用九级计分法,即:总是取其中小的一个为 1,大的一个只在前 9 个正整数中取值。其尺度定义及含义说明如表 1 所示:

表 1 尺度定义表

尺度	9	7	5	3	1
含义	绝对强	很强	强	稍强	相同

为了计算权向量,需要根据九级计分法构造一个比较矩阵。在处理该系统时,广泛征求网络管理专家的意见,在深入分析的基础上,建立了如下比较矩阵 A :

$$A = \begin{bmatrix} 1 & 3/4 & 7/4 & 3/2 \\ 4/3 & 1 & 7/3 & 2 \\ 4/7 & 3/7 & 1 & 6/7 \\ 2/3 & 1/2 & 7/6 & 1 \end{bmatrix}$$

(5)

由于理想的比较矩阵应该满足一致性条件: $\forall i, j, k, a_{ik} = a_{ij}a_{jk}$ 。所以,需要对上述得到的比较矩阵进行一致性检验。检验的步骤如下:

- ① 计算一致性指标: $CI = |r - n| / (n - 1)$
- ② 计算可靠性指标: $CR = CI / RI$
- ③ 检验规则:比较矩阵为可靠,当且仅当 $CR < 0.1$ (相当于小 10 倍以上,可根据重要性调整)。

其中 CI 是比较矩阵 A 的最大特征值 r 相对于同阶一致性矩阵最大特征值的相对偏差,其值越小越好。 $RI(n)$ 称为随机一致性指标,AHP 中给出的一致性指标如表 2 所示:

表 2 一致性指标表

n	2	3	4	5	6
RI	0	0.58	0.90	1.12	1.24
n	7	8	9	10	11
RI	1.32	1.41	1.45	1.49	1.51

对上述比较矩阵进行一致性检验,发现其通过了一致性检验。所以,决定用公式(5)中的比较矩阵 A 作为最终的比较矩阵。

2.5 权向量 $W^T = [\alpha_1, \alpha_2, \alpha_3, \alpha_4]$ 的确定

通过上述操作,已经得到通过一致性检验的比较

矩阵 A , 现在可由它近似决定权向量 W^T , AHP 给出计算公式:

$$W^T(\alpha_1, \dots, \alpha_n) = (1/n)(\beta_1 + \dots + \beta_n) \quad (6)$$

其中, β_j 为 A 的第 j 列的归一化。

$$\beta_j = (1/(a_{1j} + \dots + a_{nj})) \begin{bmatrix} a_{1j} \\ \dots \\ a_{nj} \end{bmatrix} \quad (7)$$

根据上述理论分析, 利用公式(6)和(7)得出与矩阵 A 对应的权向量为:

$$W^T = [0.20, 0.15, 0.35, 0.30] \quad (8)$$

2.6 设备的健康指数 S 的确定

为了获得设备的健康指数, 需要对归一化后的指标矩阵 X 进行处理, 处理方法为:

$$S = X * W \quad (9)$$

2.7 设备的安全态势曲线图绘制

根据采集到的数据, 用上述步骤处理, 可得到在采样点处的设备健康指数, 进而可绘制出设备的安全态势曲线图。

2.8 设备的异常安全态势报警

因为设备的健康指数是一个独立的随机变量, 根据中心极限定理, 如果随机变量 S 可表示成多个独立的随机变量 S_i 之和, 只要每个 S_i 对 S 只起微小的作用, 在 n 较大时, 可认为 S 服从正态分布。对于 n 个数据, 样本方差为:

$$F_n^2 = \frac{1}{n-1} \sum_{i=1}^n (S_i - \bar{S}_n)^2 = \frac{1}{n-1} (\sum_{i=1}^n S_i^2 - n \bar{S}_n^2) \quad (10)$$

样本的标准差为:

$$F_n = \sqrt{\frac{1}{n-1} (\sum_{i=1}^n S_i^2 - n \bar{S}_n^2)} \quad (11)$$

利用样本均值和标准差, 可以为健康指数的总体均值构造一个置信区间。即置信度为 $1 - \alpha$ 的置信区间为:

$$(\bar{S}_n - Z_{\frac{\alpha}{2}} \frac{F_n}{\sqrt{n}}, \bar{S}_n + Z_{\frac{\alpha}{2}} \frac{F_n}{\sqrt{n}}) \quad (12)$$

公式(12)中, $Z_{\frac{\alpha}{2}}$ 可以根据正态分布表获得。通过确定置信度为 95%, 可以求得总体均值的置信区间。那么, 如果测量值在置信区间内, 则认为健康指数正常; 如果不在置信区间内, 则认为出现了异常, 需要及时地给出异常报警。

3 网络设备安全态势分析系统设计与实现

3.1 系统模块设计与分析

根据 SNMP 运行环境^[10], 设计了基于 C/S 架构的网络设备安全态势分析系统, 其可分为 6 个模块, 如图 1 所示。

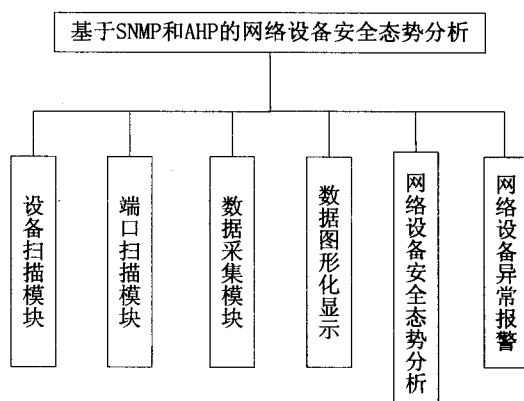


图 1 系统功能模块图

在下面的篇幅, 将对以上 6 个模块逐一展开说明。

1) 设备扫描模块分析。

此模块完成的功能是管理站根据网络的连接情况, 找到管理员所管理的所有 SNMP 代理, 取回代理的 IP 地址等。

2) 端口扫描模块分析。

此模块实现当用户选择监视某个网络设备后, 为了对端口的流量进行监控, 需要获得该网络设备的所有端口信息。

3) 数据采集模块分析。

利用 SNMP 协议与代理设备进行通信, 完成对代理设备 MIB 库的数据采集和处理, 以获得最终图形化显示的数据。

4) 数据图形化显示模块分析。

实现对网络中的某个代理设备的 CPU 使用情况和内存使用情况以及设备的所有端口的流入和流出流量的显示。

5) 网络设备安全态势分析。

利用第 2 节中提出的分析方法对网络设备的安全态势进行分析, 通过处理 2.1 ~ 2.7, 得出在取样点处的设备健康指数 S , 根据 S 可以绘出网络设备的安全态势分析图。

6) 网络设备异常报警。

根据网络的健康指数曲线图, 通过确定置信度为 95% 的置信区间, 处理第 2 节中的 2.8, 从而对网络设备的安全态势进行异常判定, 对异常的网络设备给出异常报警。

3.2 系统运行效果展示

本系统利用实验室中五台 PC 机构建一个小的局域网, 把每台 PC 机的 SNMP 服务开通, 搭建了如下的一个网络拓扑(见图 2)。

1) CPU 利用率、内存使用情况效果图见图 3。

2) 设备总输入、输出流量效果图见图 4。

3) 设备安全态势分析图见图 5。

通过上面指标的图形化显示和实际观察, 可以看

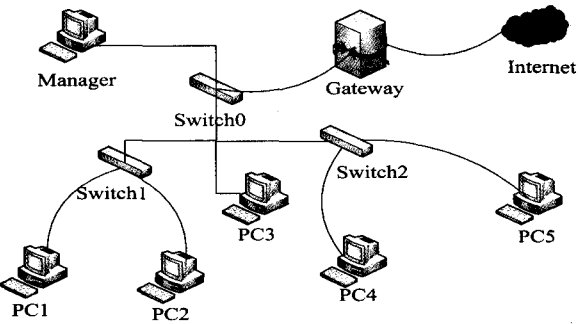


图 2 网络拓扑图

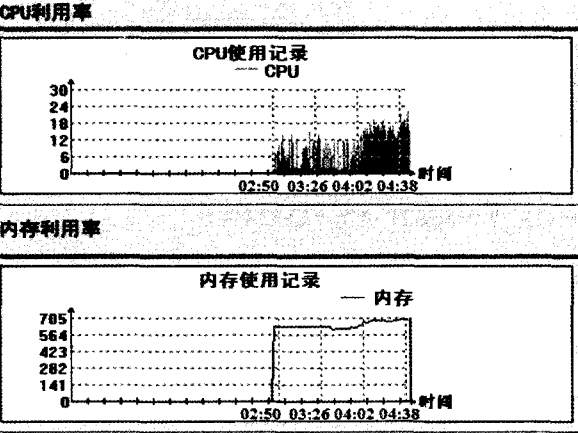


图 3 CPU、内存使用情况效果图

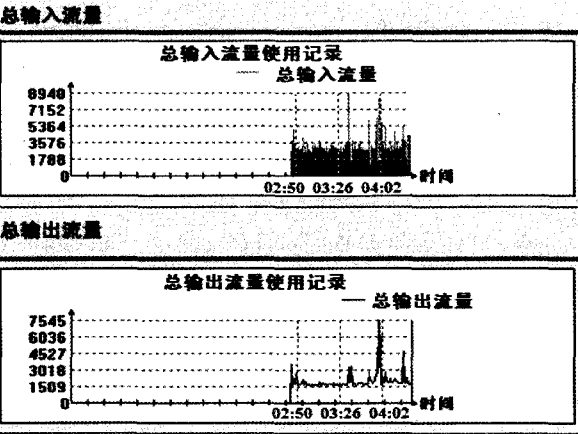


图 4 总输入、输出流量效果图

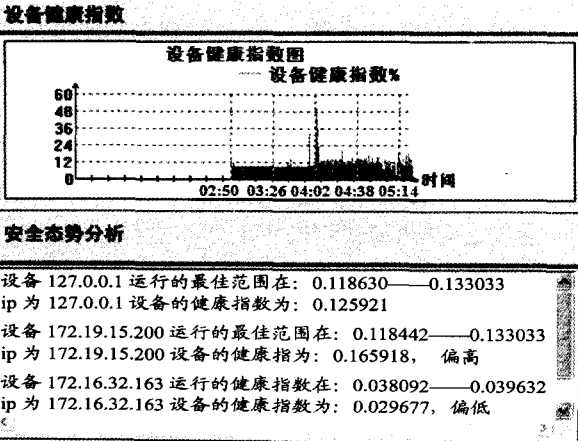


图 5 设备安全态势分析图

出采集到的数据和实际的数据相互吻合,所以上述数据的获取是正确的。同时,还能看到对于图 5,得出了代理设备的健康指数曲线分析图,对图中的健康指数进行分析,可以得出一个正常的指标区间。通过对健康指数与指标区间的对比,能得出设备的安全态势,对异常的代理设备进行了报警处理。例如,图中显示设备 172.16.15.200 的健康指数较高,因为对该台代理设备进行了实时的攻击。设备 172.16.32.163 (PC4)的健康指数较低,而实际情况下这台设备所执行的任务很少。所以,这些实验的成功测试证明了系统是十分可行的,是正确的!

4 结束语

文中以 SNMP 为基础,选择 C/S 架构模式,使用了 Visual C++^[11]和 SNMP++^[12]作为开发环境。通过构建网络设备安全性能指标体系,使用指标同趋势法和归一化法对采样得到的指标粗糙数据进行处理。然后,基于层次分析法,构建了一种网络设备安全态势分析的综合分析方法。通过实施这个方法,得到网络设备的健康指数。根据设备的健康指数,利用方差进行计算,使用中心极限定理,确定置信度为 95% 的置信区间。根据测量值是否在置信区间内,判定网络设备是否处于正常,从而达到对网络设备的实时监控和管理。

与已有的系统相比,文中的分析系统有以下方面优点:

- ① 构建了网络设备安全性能指标体系,建立了一种网络设备安全态势分析的综合方法。
- ② 基于 SNMP 协议进行开发也是一大创新。
- ③ 系统界面的图形化显示方便了专业人员和非专业人员对于系统的了解。

下一步的目标是进一步完善和细化文中的分析方法和系统。例如,通过得到网络设备的安全态势,来分析整个网络的安全态势和考虑更多影响网络设备性能的指标等。

参考文献:

[1] 韦 勇,连一峰,冯登国. 基于信息融合的网络安全态势评估模型[J]. 计算机研究与发展,2009,46(3):353-362.
[2] 肖道举,杨素娟,周开锋. 网络安全评估模型研究[J]. 华中科技大学学报(自然科学版),2002,30(4):37-39.
[3] 冯登国,张 阳,张玉清. 信息安全风险评估综述[J]. 通信学报,2004,25(7):10-18.
[4] 王慧强,赖积保,朱 亮. 网络态势感知系统研究综述[J]. 计算机科学,2006,33(10):5-10.
[5] 李明江. SNMP 简单网络管理协议[M]. 北京:电子工业出版社,2007.

离 LMA 成反比。当 PMIPv6 域的大小一定时,即 LMA 和 MAG 的距离一定, LMA 失效的概率越大则该机制的信令开销越大。当 LMA 失效的概率一定时,机制的信令开销将随着 LMA 和 MAG 的距离增加而增大。以上分析表明,该机制在 LMA 失效概率小, PMIPv6 域小的场景下能保持最小的开销。

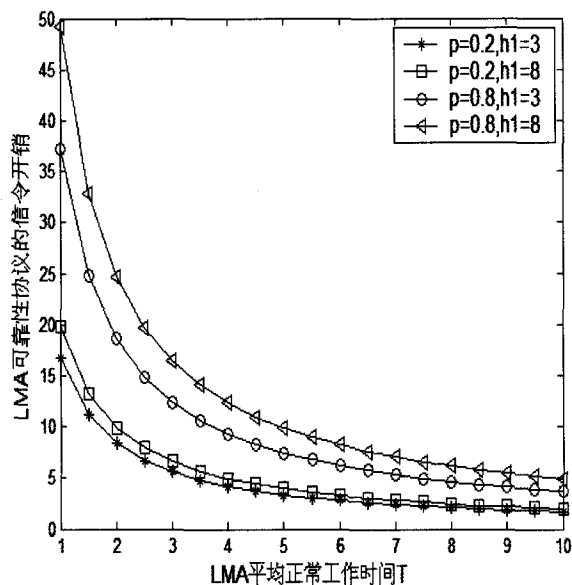


图3 机制信令开销

4 结束语

文中所提出的保证 LMA 可靠性的机制,可以有效地应对 LMA 失效的情形,通过保证网络中 LMA 功能的可靠性,实现了其移动性管理功能的延续性和服务状态的一致性,从而有效地提高了 PMIPv6 网络的稳定性。另外,该机制的实现不需要移动终端的参与,因而也不会给终端带来额外的开销,进而更加保证了该机制的可行性。

参考文献:

- [1] Johnson D, Perkins C, Arkko J. Mobility Support in IPv6[S]. RFC3775, 2004.
- [2] Koodli R. Fast Handovers for Mobile IPv6[S]. RFC4068, 2005.
- [3] Soliman H, Castelluccia C, Malki K E, et al. Hierarchical Mobile IPv6 Mobility Management (HMIPv6) [S]. RFC4140, 2005.
- [4] 李庆,曾志纯. IPv6 协议对移动性的支持[J]. 微机发展(现更名:计算机技术与发展), 2003, 13(11): 90-92.
- [5] Gundavelli S. Proxy Mobile IPv6[S]. RFC5213, 2008.
- [6] 周华春,张宏科,秦雅娟. 一种基于代理移动 IPv6 的全局移动性管理结构和协议[J]. 电子与信息学报, 2008, 30(12): 3000-3004.
- [7] 韩卫占,张思东,孙玉. 通信网络管理控制系统可靠性及其评价研究[J]. 西安电子科技大学学报, 2008, 35(1): 133-139.
- [8] 郑龙,刘敬军,罗鹏程,等. C3I 系统的网络可靠性综述[J]. 计算机技术与发展, 2006, 16(4): 11-16.
- [9] 张玉军,张翰文,自文曙,等. 移动 IPv6 网络家乡代理容错方法研究[J]. 软件学报, 2008, 19(6): 1491-1498.
- [10] Wakikawa R. Home Agent Reliability Protocol (HARP) [S]. IETF, 2010.
- [11] Korhonen J, Gundavelli S, Yokota H, et al. Runtime LMA Assignment Support for Proxy Mobile IPv6[S]. IETF, 2010.
- [12] Kwon T. Mobility Management for VoIP Service: Mobile IP vs SIP[J]. IEEE Wireless Commun, 2002, 9(5): 66-75.
- [13] Woo M. Performance Analysis of Mobile IP Regional Registration[J]. IEICE Trans Commun, 2003, E86-B(2): 472-478.
- [14] Xie Jiang, Akyildiz I F. A Novel Distributed Dynamic Location Management Scheme for Minimizing Signaling Costs in Mobile IP[J]. IEEE Transactions on Mobile Computing, 2002, 1(3): 163-175.
- [15] 刘银龙,曾志民,夏海轮,等. 代理移动 IPv6 的开销分析与自适应优化[J]. 北京邮电大学学报, 2010, 33(5): 56-60.
- [16] 裴珂,李建东,郭峰. 移动 IP 路由优化性能分析及仿真[J]. 电子学报, 2002, 30(4): 484-487.
- [1] Johnson D, Perkins C, Arkko J. Mobility Support in IPv6[S].

(上接第 241 页)

- [6] 杨尚俊. 数学建模简明教程[M]. 合肥:安徽大学出版社, 2006.
- [7] 陈秀真,郑庆华,管晓宏,等. 层次化网络安全态势威胁态势量化评估方法[J]. 软件学报, 2006, 17(4): 885-897.
- [8] RFC1905. Protocol Operations for Version 2 of the Simple Network Management Protocol[S]. 1996.
- [9] 王军,雄伟,肖德宝. 基于 SNMP 的入侵检测系统的设计与实现[J]. 计算机工程与应用, 2003, 17(2): 55-59.
- [10] 秦海龙. 基于 SNMP 的网络设备性能监控系统的研究与实现[D]. 呼和浩特:内蒙古大学, 2008.
- [11] 武孟军,任相臣. Visual C++ 开发基于 SNMP 的网络管理软件[M]. 第 2 版. 北京:人民邮电出版社, 2009.
- [12] 周志成,王卓,汪秉文,等. 基于 SNMP++ 类库的简单网络管理平台的实现[J]. 计算机技术与发展, 2006, 16(3): 158-160.