文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

基于 MSA 无线网络安全系统的设计

樊静
中国联合网络通信有限公司软件研究院
DOI:10.12238/acair.v2i3.8591

[摘　要] 无线Mesh网络作为无线通信技术的主要接入方式,主要特点为带宽高、健壮性良好,被广泛应用到各场景中,使互联网终端接入问题得到解决。在移动互联网不断发展的背景下,网络安全问题也逐渐凸显出来,影响了无线Mesh网络部署和商用。所以,研究设计基于MSA协议的无线网络安全系统,实现系统模块化管理,使系统设计复杂度降低,方便系统的维护升级和二次开发。
[关键词] 无线网络；网络系统；网络安全
中图分类号：TN915.08　文献标识码：A

Design of MSA based wireless network security system

Jing Fan
China United Network Communication Co., Ltd. Software Research Institute,Anqing City
[Abstract] As the main access method of wireless communication technology, wireless mesh network is characterized by high bandwidth and good robustness, and has been widely used in various scenarios to solve the problem of Internet terminal access. In the context of the continuous development of mobile Internet, network security issues have gradually emerged, affecting the deployment and commercial use of wireless mesh networks. So, research and design a wireless network security system based on MSA protocol, achieve modular management of the system, reduce system design complexity, facilitate system maintenance, upgrading, and secondary development.
[Key words] Wireless network; Network system; network security

在大数据背景下,基于云计算的云社交、云存储等智能应用也在不断发展,方便了人们的日常生活和生产,但是也存在部分安全隐患。常见网络安全包括计算机崩溃、用户数据泄露、网络病毒等,影响了企业或者用户的生产、生活。在信息技术发展的过程中,网络病毒种类也在不断增加。传统安全系统中的自动追踪、预警和智能处理技术已经无法对病毒进行识别,要求对其进行改进、优化。基于此,本文就对无线网络安全系统的优化设计进行分析[1]。

1 无线网络安全系统的总体架构

在现代社会下,大数据技术不断发展,网络安全检测系统的设计要求以网络非法入侵为基础,主要包括检测引擎、报文解码、报文捕获、预处理、日志报警等功能,图1为无线网络安全系统的架构。在系统设计过程中,要求系统具备高可靠性、可扩展性、高安全性和开放性的需求,系统运行稳定,能够全天不间断运行。另外,以设计应用需求方便系统扩充,使系统使用需求得到满足。并且支持各高速网络技术,使网络带宽进行拓展。利用国际标准协议进行设计,比如基于SNMP的网络管理等。

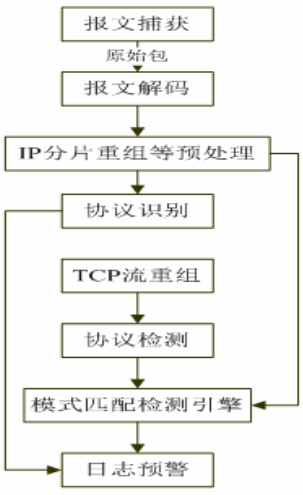

图1　无线网络安全系统的架构

系统能够利用大数据环境收集数据,并且对数据的非法入侵检测行为进行检查,所以报文捕获为系统设计的基本模块。全面处理所收集的数据,使非法入侵检测速度和精准度得到提高。报文解码的基础为网络协议所定义的格式,利用解码函数分析

所捕获的数据,对网络协议信息解析后在Packet结构中存储,方便系统的分析和处理。利用可扩展插件体系结构,能够对报文解密数据进行有效处理,要文件对相应的插件进行选择,使模块有效性、可扩展性得到提高。为了提高非法入侵检测的精准性,可以使用协议分析模块根据类型实现数据报文分流,使系统网络安全检测的性能得到提高[2]。

2 基于MSA无线网络安全系统的硬件设计

2.1滤波器设计。滤波器指的是滤波电路设备,主要包括电阻、电感和电容。利用滤波器处理滤波,以不同网络的频率和频点使网络监测效率提高。

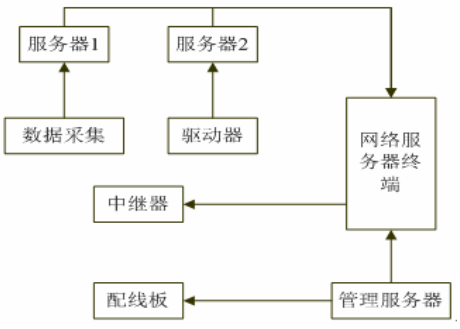

图2　滤波器的结构

2.2处理器设计。在处理器功能设计过程中,要求具备网络安全功能,提高系统硬件设备的能力。本文使用英特尔I5 9400F处理,处理模式为6内核12线程方式,能够额外设置4个1.5GHz的基本频率模块,从而提高处理器的速率和网络安全性。为了使网络扩展性得到满足,处理器自身内存有128G,并且设置多个插槽,如果处理器空间无法满足需求,可以将处理器缓存冗余清理,使处理器使用率得到提高[3]。

2.3数据采集器。对网络运行中全部网络数据包进行收集,对监控器和处理器的数据处理。本文使用YUH75-1系列数据采集器,其中包括大量卡扩充卡槽、type接口等,提高数据采集器的采集速度,从而使系统的网络监测效率提高。

2.4监测器。监测器为系统对网络安全监测的核心硬件设备,可以通过滤波器、数据收集器和处理器监测网络运行状态。假如网络运行中出现入侵行为,要将IP信息或者地址发送到网络管理中心,利用相应的算法处理信息。

SICCDF0-92芯片是一种双核四通道芯片,使用此芯片设计监测器,提高了识别网络行为效率。利用3840*2160高清屏幕设计监测器,根据双协议、超高频的网络数据筛查模块,使监测器数据运行速率得到提高,从而进一步的提高监测器在工作过程中的效率。

3 基于MSA无线网络安全系统的软件设计

3.1网络入侵检测模块。(1)网络数据捕获。在系统设计过程中,能够收集无线网络中各关键节点数据并且处理。利用网络入侵方式对数据进行过滤,根据敏感属性字段对其进行出具。通过转变接收器预处理数据包之后,能够使其成为被识别的方式,之后进行检测和学习。在收集数据包时,可以利用以太网广播特征实现,图3为网络入侵检测的流程。(2)特征提取和处理。在无线网络入侵攻击方面,入侵行为特征和方式各有不同,无法对其开展表面检测和处理。部分行为模式并没有特定的规则,但是存在一样的本质。所以,要对入侵的本质特征进行提取,从而对网络行为进行全面分析,充分展现入侵行为信息。在对数据特征进行处理的过程中,要求转变网络数据,使其能够成为被神经网络进行识别的方式,有效分析特征向量。(3)报警机制。主要包括两种报警机制,比如主动、被动的报警。在主动报警中,用户能够改变入侵的攻击进程;在被动报警中,要求拦截入侵信息,之后进行其他操作。但是,不管是什么操作方式,用户应用屏幕报警的方式比较多。假如存在非法入侵或者病毒时,利用弹窗等方式提醒给用户。如果使用不同的报警方式,那么也存在不同的行为和数据,比如攻击行为、目标等。另外,要求以用户自身实际情况对针对性报警的内容进行设置。(4)攻击样本库。是指对数据库进行入侵检测,利用数据库能够存储入侵模型和相应的数据,一般可以在应用过程中成为神经网络的自主学习对象。根据日志记录等功能记录系统在检测过程中存在攻击事件,能够方便系统用户查看。

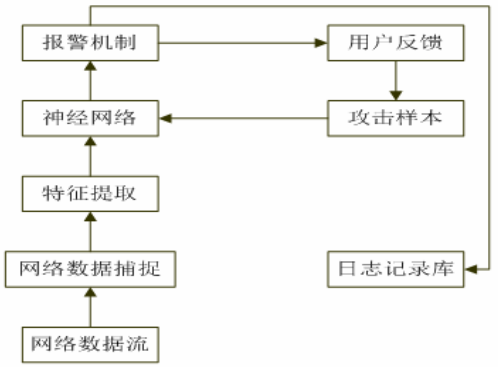

图3　网络入侵检测的流程

3.2网络管理服务运行控制。网络服务生命周期监控运行主要包括服务需求、分析、实现、规格、部署等,属于反复迭代的过程,主要阶段为:

(1)初始阶段。使系统网络服务得到实现,根据网络管理的需求更新规格说明,在校验后部署服务;(2)创建阶段。根据初始阶段的需求创建服务,以实际需求更新规格说明,从而对服务进行设置;(3)运行阶段。实时监控系统运行过程中的实际情况,检验运行中的异常和问题。比如在对服务执行时通过改善实际情况升级服务,从而有效实现。

通过网络管理服务的安全访问功能能够有效控制无线网络服务,从而解决服务自组织存在的安全问题。利用网管服务安全访问控制的主要功能包括用户权限管理、传输信息、用户认证等,如果用户没有授权,就无法应用系统,授权用户能够正常使用。用户权限管理和相应服务权限一一对应,根据实际需求调整用户的等级。另外,非授权的第三方是无法识别传输过程中的机密信息的。

将网络管理服务能够结合安全模型,根据不同的网络层协议应用安全技术。通过内过滤技术能够提高信息的安全性,根据

IP协议、端口过滤技术和ICMP协议能够避免端口没有授权的入侵。以生命周期、安全访问等模型,能够利用wbe技术对网络管理服务进行编程。有效管理运行平台中的用户和服务,以实际的需求使管理功能得到实现。服务库的管理语义关系主要包括时序关系、数量关系、等价关系等,通过服务安全实现消息安全模型的创建,主要功能为安全策略、机制等；根据服务实时监控技术有效展现服务的监控状态和结果。

以生命周期对系统无线网的安全服务流程进行管理,验证服务设计方案是否合理,将结果反馈到服务设计部门中。在部署方案时,要求通过系统能够控制网管服务的运行策略,并且设置服务周期性或者长期的运行起止时间。其中周期性的起止时间是每天、每周的时间,运行起止时间是在服务全生命周期中。能够同时设置两种策略,在网络管理服务运行过程中,系统监控服务能够根据用户投诉和实际运行情况生成自动化方案,或者对技术人员通知。另外,要求和网管系统创建通信,使用SOAP语言或者XML文件格式实现系统的相互连通。

4 系统的性能测试

为了对系统网络安全入侵检测的性能进行测试,使用C语言编程软件测试,具体测试过程为：

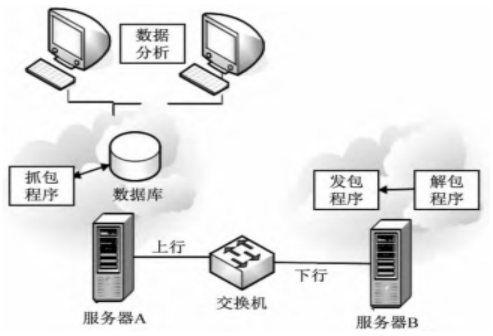

图4　测试硬件环境

表1　误报率数据表

入侵程序	误报率/%	
	现有系统	设计系统
pad	23.15	19.52
smurf	24.52	20.16
teardrop	25.65	18.65
neptune	30.25	17.54
land	32.11	15.44
satam	29.54	15
protsweep	28.65	15.26
syn	26.15	15.15
icmp	26.44	10.21
dos	23.65	10.14
平均数值	26.67	15.22

4.1创建测试环境。测试环境能够保证顺利开展系统测试,图4为测试硬件环境,主要包括计算机、服务器、数据库和交换机。使用麻省理工实验室DARPA数据集进行测试,并且提取十种网络安全入侵程序。

4.2测试结果。根据以上的测试环境实现入侵程序开展测试,利用检测率和误报率对系统测试结果展现出来,表1为误报率数据表,表2为检测率数据表。通过表1和表2可以看出来,入侵程序在测试过程中以实验数据对检测率和误报率分析,系统误报率比较低,检测率高,表示系统网络安全入侵的检测效果良好,能够保证无线网络的安全运行。

5 结束语

在计算机网络技术不断发展和普及的背景下,管理工作信息化使人们工作效率得到提高,但是会导致出现安全风险与管理问题。无线网络安全监测系统能够强化内部网络安全审计,对内部信息安全进行保证。通过本文研究,设计的系统能够保证无线网安全可靠的运行,使用多种技术设计安全监测和防御系统使无线网安全防护能力得到提高,并且提高入侵检测报警工作效率,能够为网络安全防御相关行业提供借鉴和参考。

表2　检测率数据表

入侵程序	检测率/%	
	现有系统	设计系统
pad	56.21	75.91
smurf	59.11	80.65
teardrop	49.54	75.41
neptune	56.25	81.65
land	59.11	79.88
satam	56.21	82.65
protsweep	42.22	80.14
syn	35.65	75.11
icmp	15.11	80.65
dos	50.26	81.25
平均数值	51.26	79.52

[参考文献]

[1]梁广荣.基于MSA无线网络安全系统设计和实现[J].信息记录材料,2023,24(9):133-135.

[2]杨琦,熊志金,陈永丰.基于无线传感器网络的地铁隧道安全监测系统设计[J].南方职业教育学刊,2022,12(2):103-109.

[3]刘雯雯.基于云计算环境下的计算机网络安全存储系统的设计与实现[J].电脑知识与技术,2022,18(12):38-40.

作者简介：

樊静(1992--),女,汉族,安徽省安庆市人,硕士研究生,中级,中国联合网络通信有限公司软件研究院,研究方向：通信方向。