基于中间件的多源数据交换系统

李伟伟,张 涛,马媛媛,周 诚
(国网智能电网研究院,江苏 南京 210003)

摘 要:随着智能电网互动化的发展,信息内外网边界交互数据种类呈现多样化趋势,除了传统的各种数据库等结构化数据以外,一些以电子文档数据为代表的非结构化数据也将频繁地在信息内外网之间进行交互。为更好地应对电力系统业务系统数据交换的多源化、文件过滤复杂化的需求,文中详细设计了一种基于中间件的插件调度和管理体系,各种定制安全中间件实现不同的解析和过滤功能,并由中间件调度器调度形成统一、高效、安全的过滤能力。采用该方法实现的基于中间件的数据交换系统可在确保电力信息内网安全的前提下,满足业务系统多源数据交换的需求。系统测试结果表明,通过该方法可以实现多源数据交换,文件接收和标签过滤等各项功能和性能满足电力系统数据交换要求。

关键词:中间件;安全;数据交换;隔离
中图分类号:TP393 **文献标识码**:A **文章编号**:1673-629X(2016)05-0095-04
doi:10.3969/j.issn.1673-629X.2016.05.020

Multi-data Exchange System Based on Middleware Technology

LI Wei-wei,ZHANG Tao,MA Yuan-yuan,ZHOU Cheng
(China Smart Grid Research Institute,Nanjing 210003,China)

Abstract:With the development of smart grid interactive,the data which interacts network boundary becomes diversified. In addition to the various databases and other traditional structured data,some of non-structured data like the electronic document data for representation begin to interact frequently between the internal and external of electronic information network. To solve the complexity and diversity of data exchange in grid system,a plug schedule and management system based on middleware technology is designed in detail,which realizes different parsing and filtering,and forms the unified,efficient and safe filtering capabilities by middleware. The system realized by the method proposed can meet the need of data exchange on the premise that network security can be guaranteed. The test results show that functionality and performance of the system meet the requirements of data isolation and exchange.

Key words:middleware;safety;data exchange;isolation

0 引 言

随着病毒和黑客攻击造成的危害越来越大,网络安全成为人们关注的焦点。Internet 为电力系统的数据交换提供了方便快捷的途径,同时也带来了安全威胁。电力系统中许多重要的内部网络都采取了与 Internet 隔离[1-3]的方式,避免了来自 Internet 的各类侵扰,也阻断了必需的信息交换。

数据交换系统[4-8]可以在安全内网与非信任外网在物理隔离的前提下,安全完成两网之间的信息交换功能。在对非法网络通路进行安全网络隔离的同时,还能保证正常、合法的网络应用,从而实现既保证正常、合法的网络应用,又保证关键网络资源的安全网络隔离的理想目标。

1 电力系统数据交换面临的问题

随着智能电网互动化的发展,信息外网展现的内容越来越丰富,除了传统的各种数据库等结构化数据以外,一些以电子文档数据为代表的非结构化数据也将频繁地在信息内外网之间进行交互。电子商务平台、财务管控系统、基建管控中的现场管理系统、统计系统及综合管理系统等各种业务信息系统中均涉及到多种类型的电子文档,迫切需要对多源数据交换技术进行研究,使之在不降低公司原有信息安全“三道防线”隔离强度与效率的情况下,满足智能电网的“互动”业务需求,将成为坚强智能电网信息安全保障体系建设过程中迫切需要思考和解决的问题。

在信息内外网间交换多源数据是现实且迫切的需

收稿日期:2014-12-12 **修回日期**:2015-04-08 **网络出版时间**:2016-05-05
基金项目:国家电网公司科技项目(EPRIXXKJ[2014]2244)
作者简介:李伟伟(1985-),女,工程师,硕士,研究方向为信息安全;张 涛,硕士,高级工程师,研究方向为信息安全。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20160505.0814.018.html

求。然而,多源数据格式各异、数据量极大,同时包含大量敏感信息,是病毒、木马的理想载体。因此多源数据交换既有迫切需求,又蕴含安全风险。如何构建一个交换体系,在确保信息安全的前提下,适应各种多源数据格式,满足大数据量的交换需求,以合理的性能提供信息内外网间的多源数据交换功能。

2 基于中间件的多源数据交换系统

多源数据交换功能涉及的过滤技术更加复杂和多元化,因管理要求的变化、文件格式的不同都可能会产生新的过滤需求。为了更好地应对这些过滤需求,文中引入基于中间件[9-10]的插件调度和管理体系,各种安全中间件实现不同的解析和过滤功能,并由调度器调度形成统一的安全过滤能力。

通过中间件技术,可灵活扩展多种协议、多种数据格式、多种过滤算法。研究基于标准中间件的多种安全过滤方法组合技术,可灵活组合基于等级标签的过滤、基于协议的过滤、基于特征的过滤和基于内容识别的过滤等多种安全过滤技术[11-14]。

2.1 系统架构

多源数据交换系统框架包括驱动、接收模块、安全过滤中间件、配置管理和监控页面等模块。多源数据经过驱动预处理后,使用私有协议,添加标签信息,经加密通道送至隔离服务接收模块,在经过安全过滤中间件过滤后,交换至目标文件服务器。

该系统架构可在业务系统和文件服务器之间实现安全的数据交换。业务系统作为交换的发起方,文件服务器作为数据的接收方。该体系可实现双向数据交换,且内外网均可发起数据交换请求。所不同的是,自内而外的数据交换主要关注的是数据防泄漏,而自外而内的数据交换则更关注对恶意文件的过滤。

基于中间件插件的多源数据交换系统设计架构如图 1 所示。

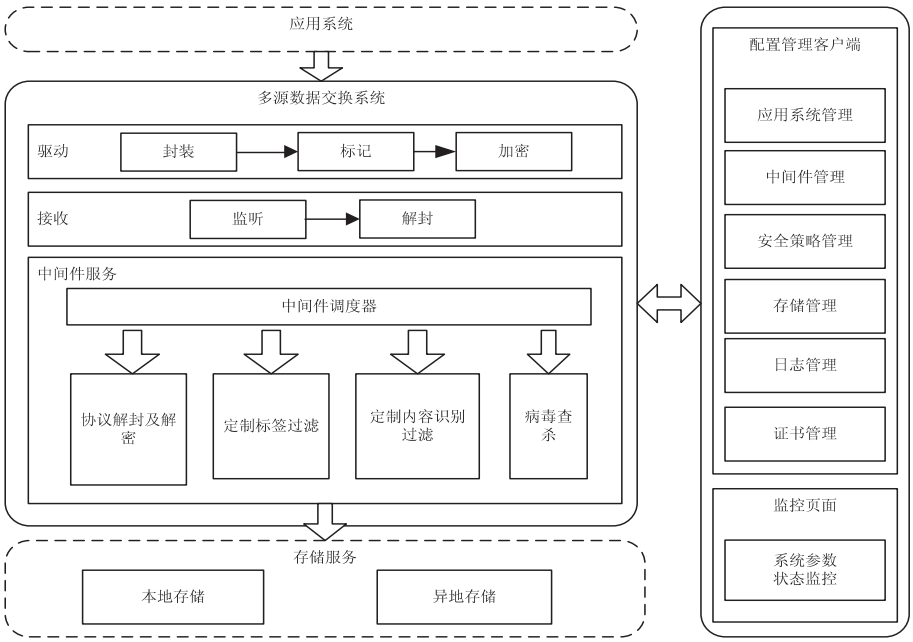

图 1 基于中间件插件的多源数据交换系统设计架构

2.2 处理流程

业务系统通过代理驱动提交文件交换请求,服务端的文件接收进程接收文件交换请求,将文件缓存在本地文件缓冲区,同时在进程内部的任务队列中生成文件交换任务,然后向客户端报告文件交换请求已受理。服务端可同时存在多个过滤和执行进程,每个过滤和执行进程可独立完成文件的过滤和交换任务。过滤和执行进程向文件接收进程请求任务列表,并依次处理列表中的每个任务。过滤和执行进程的核心是中间件调度线程,该线程按照配置文件的要求依次调用各过滤插件执行各项过滤任务,最后将通过过滤的文件提交给文件存储线程,并完成交换。

2.3 功能模块

基于中间件插件的多源数据交换系统主要包含安全驱动、文件接收模块、过滤中间件调度、存储适配器、配置管理和状态监控模块。

2.3.1 安全驱动

文件安全代理驱动部分的作用是给用户提供创建文件对象和发送文件的接口。用户可以调用这些接口来实现文件交换,接口内部预处理包括了系统对文件对象和标签对象的创建和维护,其中标签对象包含了数据的属性信息,文件接收进程可通过标签信息进行报文的过滤,最后将数据封装成统一的安全交换数据,经过 SSL 加密隧道进行传输。

2.3.2　文件接收模块

文件接收模块位于服务端,此模块的功能是监听客户端请求,接收客户端发送的文件,进行格式解析和标签过滤,最后存放到数据缓存中。

文件接收模块从数据监听开始,客户端有文件上传后开始接收文件,文件接收完毕后生成待处理任务,并在中间件模块请求任务时执行任务分发,任务分发完毕后文件接收模块流程结束。

2.3.3　中间件调度

中间件调度器的主要功能是根据配置文件生成中间件调度序列,并且在多源数据过滤的过程中根据配置项调用指定的中间件。多源数据中的每个具体的应用对应不同的中间件调度序列,该调度序列在配置文件中配置。

中间件调度器根据配置文件配置的中间件信息生成中间件调度序列。当需要使用中间件时,首先从中间件调度序列中获取对应中间件的信息,然后根据中间件信息中的中间存放路径,以及中间件对外提供的接口名调用中间件。

(1)生成中间件调度序列。

中间件调度器在系统中采用链表的方式实现,序列链表生成过程如图 2 所示。

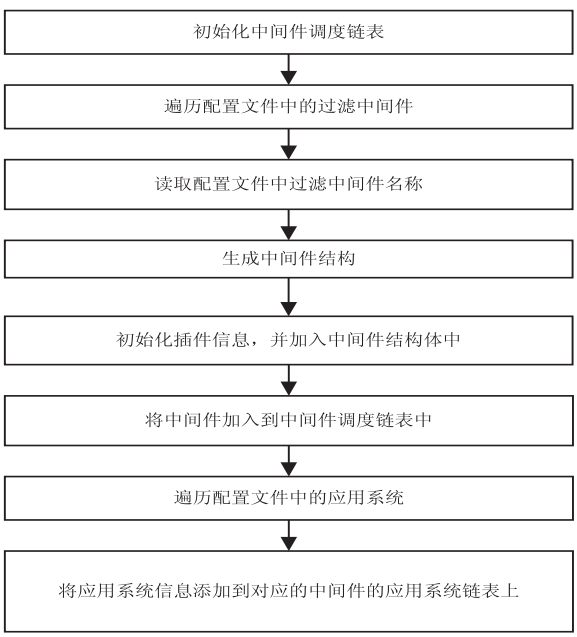

图 2　中间件调度器生成流程图

生成的中间件调度序列结构如图 3 所示。

(2)获取中间件。

当收到多源交换任务时,根据任务对应的应用系统,遍历中间件调度器,查找应用系统对应的所有中间件,获取中间件。

(3)调用中间件。

存储中间件以动态链接库的形式存在。只有当需要调用某个存储中间件时,才加载该中间件对应的动态链接库。调用动态链接库提供的函数时需要知道动态链接库的位置,同时还要知道动态链接库对外提供的函数的名称。这些信息在获取存储中间件时已经得到。

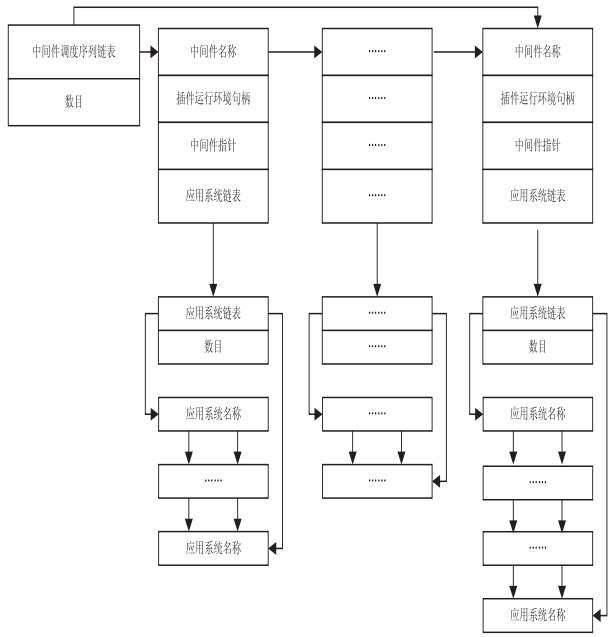

图 3　中间件调度器结构图

2.3.4　存储适配器

存储中间件的功能是将过滤完成的多源数据转存到其他位置。由于存在多种存储方式,因此相应地也存在多个存储中间件。存储适配器完成对所有存储中间件的维护和调用。

存储适配器采用与中间件调度器相似的实现方式,即存储中间件以动态链接库的形式存在,存储适配器维护存储中间件链表,并且在需要调用存储中间件时从存储中间件链表中读取存储中间件信息,完成存储多源数据的操作。

2.3.5　配置管理和监控页面

配置管理模块需要的配置内容包括系统基础配置、系统运行参数配置和策略配置。系统基础配置是配置系统的一些基本信息,如日志数据库地址、文件上传地址等;系统运行参数配置是针对系统运行参数的配置,如临时文件队列的清理时间;策略配置是对文件的过滤策略配置,如限定文件的上传时间等。

监控页面用于对系统的运行状态进行监控,监控数据由各个模块中的监控线程收集,并反映到监控界面。

3　系统应用

业务系统要提交数据或文件等到内网都要经过多源数据交换系统。基于中间件的多源数据交换系统与

业务系统的接口关系如图 4 所示。

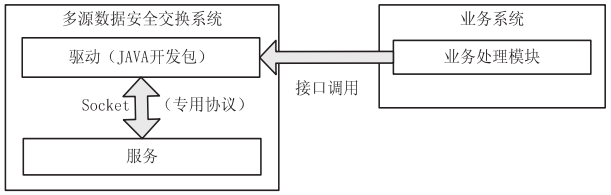

图 4 多源数据交换系统与应用服务的接口关系

应用系统通过调用驱动接口函数发送文件，驱动与服务通过 socket 进行通信，并使用专有协议封装标签和加密信息，通过服务的中间件调度序列过滤和存储适配器将文件保存的内网的目的地并返回文件操作结果信息，实现多源数据的隔离交换功能。

4 系统测试

4.1 测试环境

实验设备硬件环境为 Intel 5500+ICH10R 芯片组，2 路 4 核 CPU。操作系统是 32 位凝思定制安全操作系统。测试采用的是 LoadRunner 性能测试工具。

4.2 测试结果

4.2.1 文件接收性能测试

测试步骤如下：

(1)启动多源数据交换服务，开启文件接收进程；

(2)上传文件(单个文件大小 90 MB)；

(3)统计文件接收进程处理时间。

测试过程中，在上传总文档大小为 4 050 MB 的情况下，平均处理速率为 425.456 Mbps，具体测试结果见表 1。

表 1 文件接收性能测试结果

处理文件大小/MB	处理速率（最大值）/Mbps	处理速率（最小值）/Mbps	处理速率（平均值）/Mbps	失败个数
4 050	500.345	364.216	425.456	0

4.2.2 标签过滤插件测试

测试步骤如下：

(1)启动多源数据交换服务，开启插件过滤进程；

(2)上传文件(单个文件大小 90 MB)；

(3)统计标签过滤插件处理时间。

测试过程中，在过滤总文件大小为 4 050 MB 情况下，平均处理速率为 4 385.324 Mbps，具体测试结果见表 2。

表 2 标签过滤插件性能测试结果

处理文件大小/MB	处理速率（最大值）/Mbps	处理速率（最小值）/Mbps	处理速率（平均值）/Mbps	失败个数
4 050	3 594.234	3 215.422	4 385.324	0

4.3 测试结论

系统处理文件速率满足性能要求。测试过程中，服务器 CPU、内存和硬盘各项指标检测正常。

5 结束语

通过基于安全过滤中间件的多源数据交换系统，可以解决电力系统业务系统多源数据发送内网的安全问题。各种安全中间件实现不同的解析和过滤功能，并由调度器调度形成统一的安全过滤能力，有效实现了多源数据交换功能，保证了内网的安全。

参考文献：

[1] 孙学军. 隔离网络数据安全交换系统的设计与实现[J]. 网络与信息，2011，25(4)：60-61.

[2] 林朝爱，傅 鹂. 网络物理隔离体系结构的研究[J]. 现代计算机，2007(7)：105-107.

[3] 夏汉民. 一种网络隔离技术的实现方案[J]. 计算机安全，2009(6)：57-59.

[4] 王亚玲，郝 赫，曹占峰，等. 数据交换平台在国家电网公司信息化建设中的应用[J]. 电力信息化，2011，9(2)：116-120.

[5] 邱丽丽，俞 烽. 异构数据动态交互平台设计与实现[J]. 计算机应用与软件，2013，30(3)：182-185.

[6] 石彦华，李蜀瑜. 动态服务的数据交换模型研究[J]. 计算机应用研究，2011，28(12)：4576-4580.

[7] 周红波，孙宇达，王继霞，等. 基于 XML 的数据交换及其参照完整性研究[J]. 计算机工程与设计，2006，27(14)：2611-2613.

[8] 何 慧，孙 芙，李 遂. 异构数据库数据类型转换模型[J]. 计算机工程与设计，2005，26(9)：2461-2463.

[9] 刘 海，陈启买. 基于角色的数据交换中间件的研究与实现[J]. 计算机应用，2009，29(1)：326-327.

[10] 曾小宁，黎 明. 基于 XML 的数据交换中间件的研究与实现[J]. 计算机工程与设计，2007，28(12)：2999-3002.

[11] Kiriansky V，Bruening D，Amarasinghe S. Secure execution via program shepherding[C]//Proceedings of the 11th USENIX security symposium. [s. l.]：USENIX，2002：191-206.

[12] Abadi M，Budiu M，Erlingsson U，et al. Control-flow integrity principles，implementations，and applications[J]. ACM Transactions on Information and System Security，2009，13(1)：1-40.

[13] Shu G，Rana O F，Avis N J，et al. Ontology-based semantic matchmaking approach[J]. Advances in Engineering Software，2007，38(1)：59-67.

[14] Afrati F，Li Chen，Mitra P. Rewriting queries using views in the presence of arithmetic comparisons[J]. Theoretical Computer Science，2006，368(1-2)：88-123.