文章编号:1671-4598(2022)04-0229-08 DOI:10.16526/j.cnki.11—4762/tp.2022.04.038 中图分类号:TP399 文献标识码:A

基于双单向安全传输的移动警务请求服务总线平台的设计与实现

张 雷[1],樊志杰[2,3],张 冰[1],张丹丹[1],曹志威[2,3]
(1.黑龙江省鹤岗市公安局 科技信通支队,黑龙江 鹤岗 154103;
2.上海辰锐信息科技公司 研发中心,上海 200031;
3.公安部第三研究所 信息安全技术部,上海 200031)

摘要:对泛政府行业内网与其他网络间的跨网域的请求服务进行了研究,提出了泛政府行业信息化数据跨域共享服务总线平台的设计方案,底层硬件设计上基于单向光传输方式,实现不同网域间数据的安全隔离传输;上层系统软件通过服务总线(ESB)体系架构和定义统一请求调用接口,实现跨区域、跨网域间服务授权访问、资源授权调用和数据安全转发;整个系统由请求协议转换、安全检控组件、健康度评估、MQ数据服务、节点资源调度、限流熔断管理、通道任务管理、资源监控上报等模块组成,可实现请求服务、设备状态上报、通道任务管理、安全访问控制等功能,并根据不同业务量级设定不同应用模式,可满足跨网域移动警务请求服务数据资源的安全、高效传输需求。

关键词:移动警务;服务总线;泛政府行业;单向光传输;ESB体系架构

Design and Implementation of Mobile Police Request Service Bus Platform Based on Bi-directional Secure Transmission

ZHANG Lei[1], FAN Zhijie[2,3], ZHANG Bing[1], ZHANG Dandan[1], CAO Zhiwei[2,3]
(1. Science and Technology Ict Detachment, Hegang Public Security Bureau of Heilongjiang Province, Hegang 154103, China;
2. Research and Development Center, Shanghai Chenrui Information Technology Company, Shanghai 200031, China;
3. Department of Information Security Technology, The Third Research Institute of the Ministry of Public Security, Shanghai 200031, China)

Abstract: The request service of cross domain between intranet and other networks in the pan-government industry is investigated. The design of a service bus platform for cross-domain sharing of information data in the pan-government industry is proposed. The underlying hardware is designed based on the one-way optical transmission, the secure isolated transmission of data between different network domains is achieved. The upper software of the system realizes cross-regional, cross-domain service authorization access, resource authorization invocation and data security forwarding through the architecture of the ESB service bus and the definition of a unified request invocation interface. The whole system is composed of request protocol conversion, security inspection and control components, health assessment, MQ data services, node resource scheduling, flow restriction and fuse management, channel task management, resource monitoring and reporting modules, which can realize request services, equipment status reporting, channel task management, security access control and other functions, and the different application modes is set according to the different business levels. The proposed platform can meet the safe and efficient transmission of the request services of cross-domain mobile police.

Keywords: mobile police; service bus; pan-government; unidirectional optical transmission; ESB architecture

0 引言

当前,出于信息安全防护的需求,政府行业的内部网络必然需要和互联网等外部网络进行物理隔离,这样必然会造成内外网间数据交换的不便。在当下大数据和“互联网+”战略的趋势下,以及一系列惠民便民政策的驱动下,各级政府机关急需要与其他企事业单位之间进行数据交换,其中与互联网之间进行数据交换必不可少。同时,为了全

收稿日期:2021-12-15; **修回日期**:2022-02-25。
基金项目:上海市人才发展资金项目(2020016);中国博士后科学基金项目(2020M670998);上海市自然科学基金项目(21ZR1422000);四川省科技计划项目项目(2021YFS0310)。
作者简介:张 雷(1978-),男,吉林东丰人,硕士,高级工程师,主要从事软件工程及大数据应用方向的研究。
通讯作者:樊志杰(1982-),男,山西朔州人,博士,研究员,主要从事信息与网络安全方向的研究。
引用格式:张 雷,樊志杰,张 冰,等.基于双单向安全传输的移动警务请求服务总线平台的设计与实现[J].计算机测量与控制,2022,30(4):229-236.

面支撑便捷化的社会服务与各类政府的实战业务，实现专业化、智能化、精准化的警务应用，亟需构建集“通道单向无反馈、协议高效稳定、资产智能调度、策略集中管控”等服务能力为一体的平台。

政府行业信息化建设历经多年，仍不断暴露出“传输效率低、管控力度弱、监控能力差”等问题，影响便民服务效率的同时，还存在数据安全不可控的风险。此外，技术上不同网络间的数据传输主要采用 FTP 协议，该协议本身存在效率低下和传输模式不合理的问题，其默认的 ASCII 传输模式甚至会造成文件损坏，需探索新模式的传输协议规避此类问题的再次发生；传统信息化平台建设多采用分布式部署、分布式管理，导致服务资源数据流转情况不清晰、安全策略不统一、节点资源使用率未知，处于失联状态，因此需寻求技术手段，定义标准接口实现对服务资源和节点资源的统一管理和有效调度；传统业务模式存在数据垄断情况，为打破这一壁垒，实现服务资源目录的公开化、服务资源使用的可授权化，需要定义安全可靠的统一请求调用接口，将对接能力服务化[1-5]。

鉴于此，本文提出泛政府行业信息化数据资源跨域共享的服务总线技术并研制系统，其主要采用双单向安全传输模式，实现数据的物理单向无反馈安全传输；采用融合云计算和微服务的总线型技术架构，实现资源及服务统一管理、策略统一下发、日志统一上报；设计一种资源健康度评估模型，实现对资源通道的合理调度；基于限流熔断机制，确保高峰期重要业务及服务能力的持续支撑；定义标准统一请求接口，实现不同网络、不同区域间服务资源的授权访问、调用和执行；采用 MQ 协议，实现服务数据的高效传输；基于证书的安全架构，保障任务配置、日志传输以及数据传输过程的安全管控。

1 系统结构及原理

本文研制的泛政府行业信息化数据互联互通服务总线平台[6]，软件层面主要包括：外总线子系统、单向安全传输系统和内总线子系统，如图 1 所示。

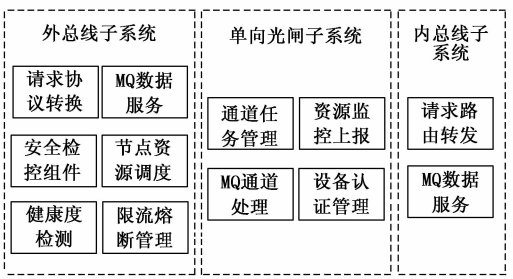

图 1 系统结构图

本系统通过双单向安全传输子系统将外总线子系统与内总线子系统分隔两端。外总线和内总线子系统分别实现对应用请求的接收和响应，单向安全传输系统实现对通道任务的管理和数据资源的监控。

本文所提服务总线主要采用单向安全传输技术和 ESB（enterprise service bus）技术，并通过两台单向安全传输系统实现服务总线数据的通道交换。

1）单向安全传输技术：单向安全传输从硬件层面提供了数据的单向传输，其采用双主机硬件结构，内外端主机各采用一个光口收发不同方向信号，其中外端机光口作为发送端只能发送数据，内端机光口作为接收端则只能接收数据[7-10]。

2）ESB 技术：本文所提系统内外总线主要基于 ESB 技术，解决多个应用系统互联所面临的复杂性，减低集成和维护成本[11-16]。

2 系统软件设计

本文所设计的服务总线主要由“外总线子系统”、“单向安全传输子系统”和“内总线子系统”组成，其中“外、内总线子系统”包含的模块和实现的功能相似，在软件设计层面的思路相似。

2.1 外、内总线子系统

外、内总线子系统主要实现业务请求的传输与转换，以及限流熔断等功能。

2.1.1 请求协议转换

服务总线接收到来自请求方的请求后，通过请求方登记的注册信息，按登记的请求方式和协议对请求内容重新组织，向目标服务发起请求，其过程如图 2 所示。

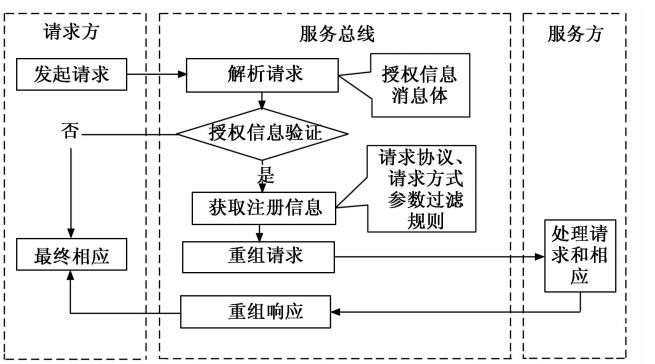

图 2 请求协议转换转发图

2.1.2 节点资源调度

资源调度管理作为系统内部整体统筹管理模块。其结构如图 3 所示。

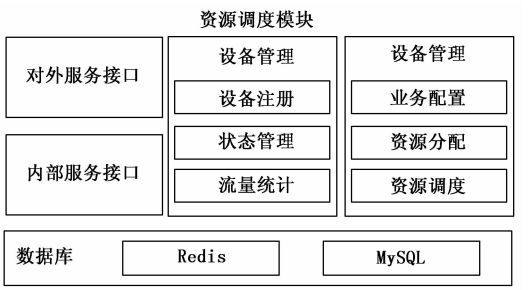

图 3 资源调度模块结构图

通道资源池根据其物理通道上带宽资源的分配方式不

同，可以分为如图 4 所示的 6 种类型。

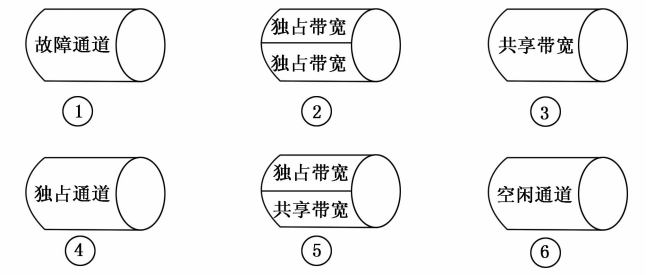

图 4　通道资源池

本文提出的通道资源分配模型根据其通道占用方式不同，可以分为独占通道、独占带宽、共享带宽 3 种类型。

1）独占通道：该通道为故障通道，无法对外提供数据传输服务。

2）独占带宽：该通道上承载了一个或多个独占带宽方式的数据传输业务。该类物理通道需要根据业务分配的带宽容量，进行限流控制。

3）共享带宽：该通道作为共享带宽资源使用，为多个业务提供数据传输服务。该类物理通道以系统最大能力运行，并为多个业务动态分配资源，不做限流控制。

2.1.3　健康度评估

外端服务总线通过模拟请求的方式，请求内端服务总线。通过响应速度和两端服务总线的设备状态，分析系统的健康度，并上报日志，其过程如图 5 所示。

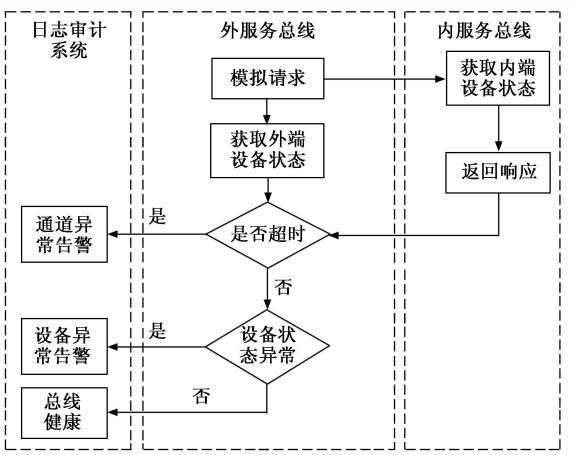

图 5　健康度评估流程图

2.1.4　限流熔断管理

为了保证业务的高效、稳定运行，本文所研究的服务总线提出了“限流熔断管理”模块，主要从边界的入口和出口两个方向切入，基于“一个策略＋两个机制”实现相关保护。

通过对边界上运行各业务的重要性等级进行标定，指导拥塞保护机制对各业务执行不同等级的处置和取舍。

业务的优先等级，对应于业务的重要性，从高到低划分为：

1）最高：最重要业务，在各种场景下都应予以保障，在系统异常时，应调集资源优先保障，尽一切可能使其运行不受影响。

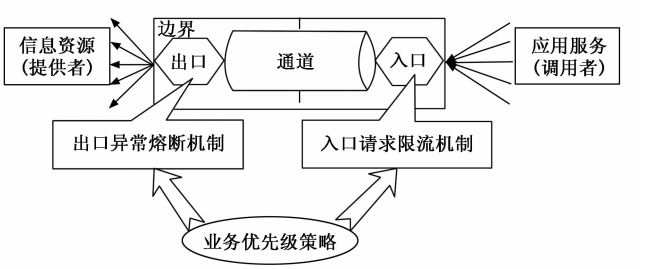

图 6　限流熔断示意图

2）高：重要业务，大部分场景下应予以保障，在系统异常时，应调集资源保障，尽可能使其运行不受影响。

3）中：普通业务，默认级别，正常情况下应得到服务保障，但在异常情况（特别是为保障重点业务需要牺牲时），可容忍一定程度的服务受限。

4）低：可受限业务，在正常情况下一般都能得到服务，但在异常情况（特别是为保障重点业务需要牺牲时），可容忍较大程度的服务受限。

5）最低：可忽略业务，在正常情况下一般都能得到服务，但在异常情况下，将首先被牺牲，以让出资源保障高优先级业务。

2.2　单向安全传输子系统

2.2.1　通道任务管理

通道任务对外提供服务。供外、内服务区的资源调度模块调用，实现通道任务的创建、修改、删除、启停。其流程如图 7 所示。

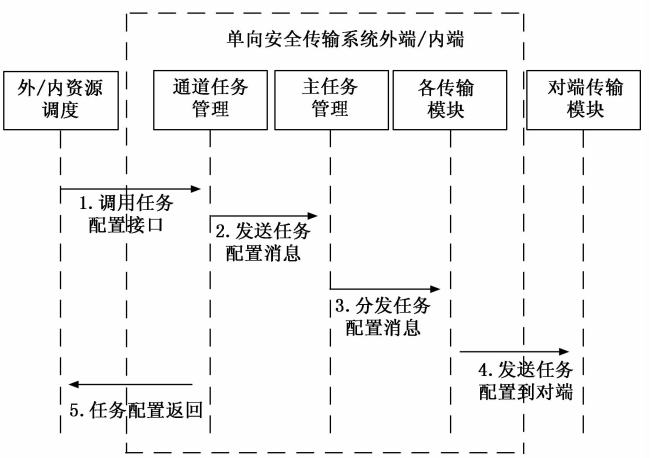

图 7　通道任务管理流程图

具体流程说明如下：

1）外、内资源调度模块调用通道任务管理模块对外提供的任务配置接口。

2）通道任务管理模块收到任务数据信息后，封装任务配置消息报文发送到主任务管理模块。

3）主任务管理模块根据业务类型分发任务配置消息报

文到各传输模块。

4）各传输模块根据任务配置报文类型更新数据库，执行相应动作。同时发送任务配置到对端。

5）通道任务管理模块返回资源调度模块调用信息。

2.2.2 资源监控上报

资源监控上报模块提供单向安全传输系统的硬件信息实时上报总线，总线根据单向安全传输系统状态进行分发，具体流程如图 8 和图 9 所示。

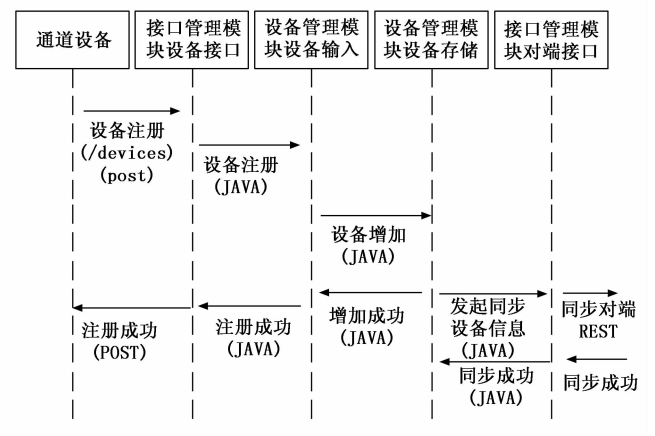

图 8 设备资源注册流程图

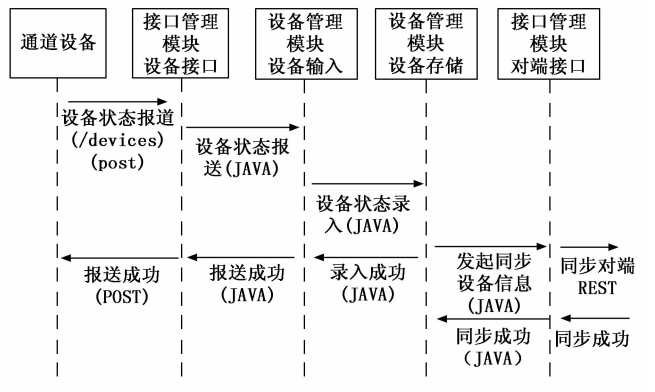

图 9 设备资源报送流程图

2.2.3 MQ 通道处理

MQ 服务作为内、外总线传输的中间协议，起到协议解耦、设备解耦作用。MQ 通道处理流程如图 10 所示。

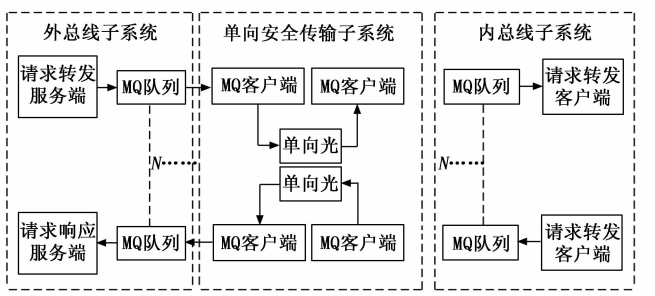

图 10 MQ 通道处理流程图

具体流程说明如下：

1）请求数据进入请求转发服务端，服务端进行协议转换并发送至 MQ 队列。

2）单向安全传输系统的 MQ 客户端获取外总线 MQ 队列数据，并摆渡至内总线 MQ 队列。

3）内总线请求转发客户端从 MQ 队列获取数据，并对真实服务器发起请求。

4）请求响应客户端收到数据后，转存至 MQ 队列。

5）单向安全传输系统的 MQ 客户端获取内总线 MQ 队列数据，并摆渡至外总线 MQ 队列。

6）外总线请求响应服务端从 MQ 队列获取响应数据，并最终返回请求方。

2.3 业务交互流程

2.3.1 数据交换业务

2.3.1.1 FTP 协议数据交换业务注册

FTP 协议数据交互业务注册流程如图 11 所示，具体说明如下：

1）接口服务向通道资源调度模块发送业务注册请求；

2）通道资源调度模块根据申请的业务类型查找匹配的通道资源；

3）通道资源调度模块根据申请的通道资源类型和带宽要求等，从可用通道里分配该业务使用的通道资源；

4）通道资源调度模块判断设备是否支持任务动态配置接口，如果不支持则表示需要手工配置交换设备上的传输任务，跳过步骤 5；

5）通道资源调度模块向数据交换设备发送创建 FTP 传输任务请求；

6）通道资源调度模块保存任务相关信息；

7）通道资源调度模块向接口服务返回业务注册成功响应。

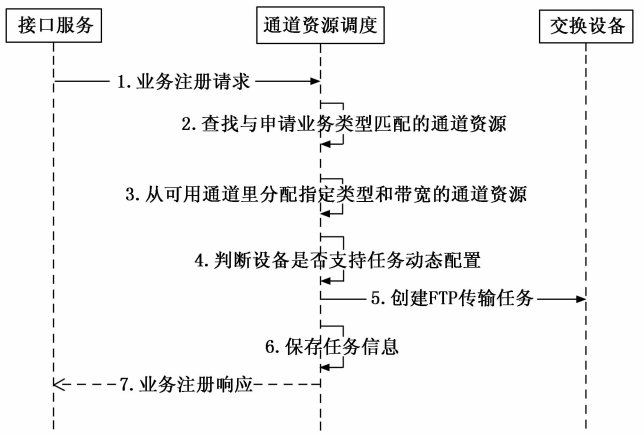

图 11 FTP 协议数据交互业务注册流程图

2.3.1.2 FTP 协议数据交换业务注销

FTP 协议数据交换业务注销流程如图 12 所示，具体说明如下：

1）接口服务向通道资源调度模块发送业务注销请求；

2）通道资源调度模块查找该业务相关的所有任务信息；

3）通道资源调度模块向数据交换设备发送删除任务请求；

4）通道资源调度模块保存任务相关信息；

5）通道资源调度模块向接口服务返回业务注销成功响应。

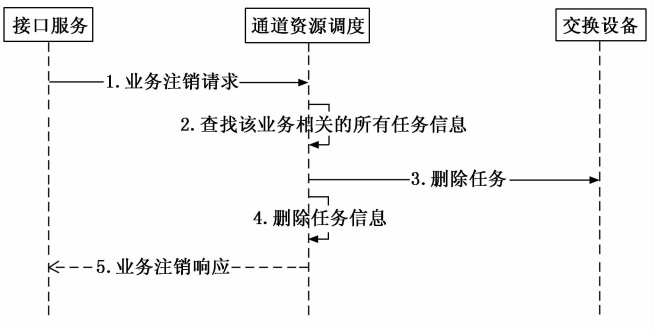

图 12　FTP 协议数据交换业务注销流程图

2.3.1.3　FTP 协议数据交换业务执行

对于双向数据交换按照两个单向数据交换任务分别独立执行，二者的流程完全一样，只是方向相反，因此这里只介绍单向数据交换的具体流程，如图 13 所示。

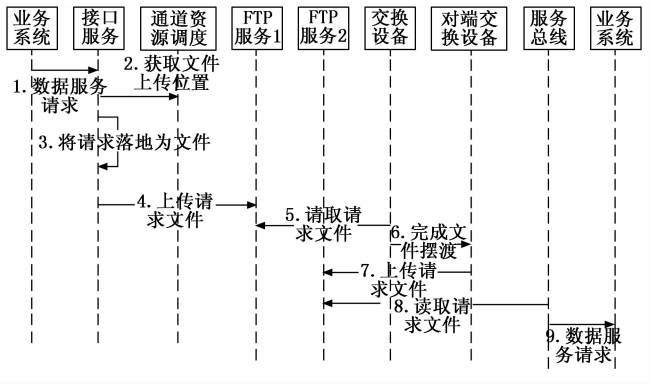

图 13　FTP 协议数据交换业务执行流程图

1）业务系统向接口服务发送数据服务请求；

2）接口服务调用通道资源调度模块获取文件上传位置；

3）接口服务将请求消息落地为文件；

4）接口服务将请求文件上传到指定的 FTP 服务器；

5）数据交换设备从 FTP 服务器获取请求文件；

6）数据交换设备负责将文件摆渡到对端；

7）对端数据交换设备将摆渡过来的文件上传到接口服务指定的 FTP 服务器；

8）接口服务从 FTP 服务器下载请求文件；

9）接口服务调用业务系统接口提交数据服务请求。

2.3.1.4　FTP 协议任务分发

FTP 协议任务发布流程如图 14 所示，具体说明如下：

1）接口服务向通道资源调度模块发送查询 FTP 任务分发通道请求；

2）通道资源调度模块查找该业务对应的通道配置，从已按照通道负载系数排好序的队列中取出第一个可用的通道；

3）通道资源调度模块获取该通道上对应该业务的 FTP 账号信息；

4）通道资源调度模块向接口服务返回成功响应，为了减少接口服务调用该接口的频度，提高系统性能，一次查询结果允许接口服务用于传输后续的多个文件。

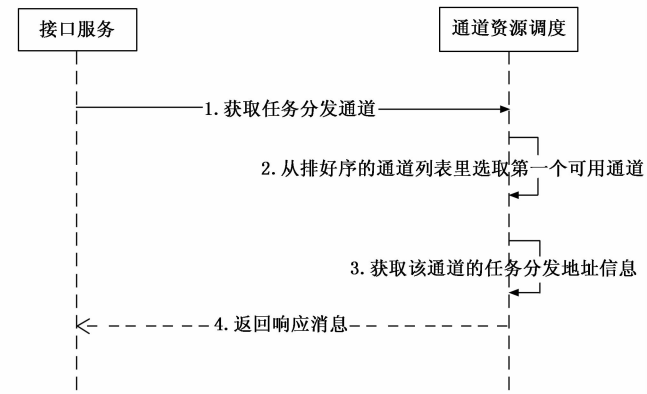

图 14　FTP 协议任务发布流程图

2.3.1.5　流模式数据交换业务注册

流模式数据交换业务注册流程如图 15 所示，具体说明如下：

1）接口服务向通道资源调度模块发送业务注册请求；

2）通道资源调度模块根据申请的业务类型查找匹配的通道资源，分配的数据交换设备应支持流模式；

3）通道资源调度模块根据申请的通道资源类型和带宽要求，从可用通道里分配该业务使用的通道资源；

4）通道资源调度模块向数据交换设备发送创建流代理任务请求；

5）通道资源调度模块保存任务相关信息；

6）通道资源调度模块向接口服务返回业务注册成功响应。

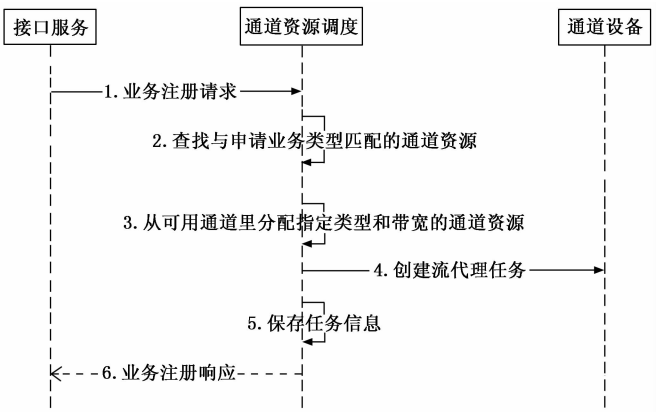

图 15　流模式数据交换业务注册流程图

2.3.1.6　流模式数据交换业务注销

流模式数据交换业务注销流程如图 16 所示，具体说明

如下：

1）接口服务向通道资源调度模块发送业务注销请求；

2）通道资源调度模块查找该业务相关的所有任务信息；

3）通道资源调度模块向数据交换设备发送删除流代理任务请求；

4）通道资源调度模块保存任务相关信息；

5）通道资源调度模块向接口服务返回业务注销成功响应。

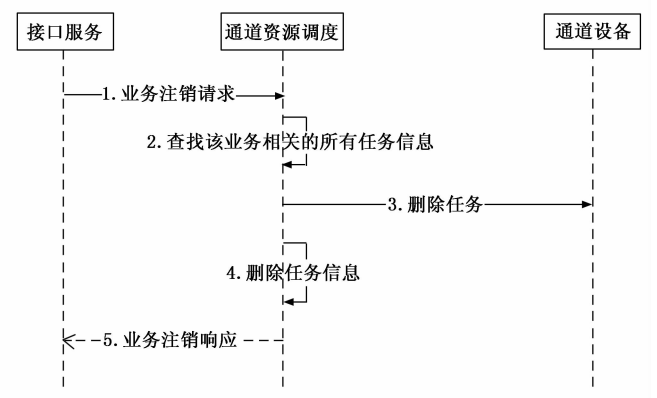

图 16 流模式数据交换业务注销流程图

2.3.1.7 流模式数据交换业务执行

对于双向数据交换按照两个单向数据交换任务分别独立执行，二者的流程完全一样，只是方向相反，因此这里只介绍单向数据交换的具体流程，如图 17 所示。

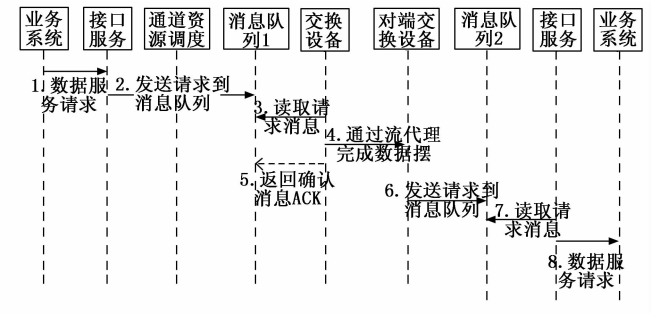

图 17 流模式数据交换业务执行流程图

具体流程说明如下：

1）业务系统向接口服务发送数据服务请求；

2）接口服务将请求消息发布到消息队列 1 中；

3）数据交换设备从消息队列 1 中读取请求消息；

4）数据交换设备通过流代理将数据摆渡到对端；

5）数据交换设备向消息队列 1 返回确认消息；

6）对端数据交换设备将摆渡过来的请求消息发布到消息队列 2 中；

7）接口服务从消息队列 2 中读取请求消息；

8）接口服务调用业务系统接口提交数据服务请求。

3 系统主要功能

本文所研究服务总线的主要功能模块包括：请求业务传输功能、限流熔断功能、安全控制功能[17-21]。

3.1 请求业务传输功能

将请求方的请求数据进行解析和转换，生成符合标准的请求报文文件，传输至服务方；接收服务方响应报文文件并解析，将反馈结果返回至请求方。

接受请求：接收服务节点回传的请求报文，解析报文，根据资源服务目录，审核请求权限，调用已授权的服务方接口，发起资源使用请求并获取数据。

响应请求：接收服务节点回传的响应报文，根据请求方标识，调用请求方接口，向请求方反馈响应报文。

1）支持 HTTP 请求转发，支持 Restful、Webservice 接口方式并提供统一入口。

2）支持参数格式检查。

3.2 限流熔断功能

在接入请求并发量高于边界处理能力时，通过限制请求接入量的方式，降低系统负载，避免边界拥塞。

3.3 安全控制功能

为了保障运行的安全性和稳定性，本系统建立了安全防护体系，具体的安全控制功能包括：

1）身份认证：管理员访问基于泛政府行业信息化数据跨域共享服务总线的管理系统时需采用硬件数字证书登陆。

2）角色三权分立：提供业务管理员、系统审计员、系统管理员三类角色权限。

3）访问控制：设置安全策略对服务调用进行访问控制，包括时间段控制、访问资源的 IP 地址黑白名单控制、请求频率或流量控制、请求参数检测与过滤、服务响应关键字过滤。

4）全流程监控审计：提供访问接入、服务交换、路由调度、服务响应等全流程的运行监控、日志采集和审计功能，提供 FTP、JDBC、JMS、SYSLOG 等协议的日志推送接口支持，支持第三方审计系统的无缝对接。

5）高安全交换控制：提供高安全的服务访问的控制功能，支持对 IP 地址信息的认证验证；支持通过设置安全策略对服务调用进行访问控制，包括时间段控制、IP 地址黑白名单控制、请求频率或流量控制、请求参数检测与过滤、服务响应关键字过滤等。

6）数据加解密：外部提供 HTTPS 加密请求接口，保证请求数据安全。

7）上报基座：系统运行日志、业务访问日志等实时上报基座，并由基座运算实时预警。

4 实施方式与应用案例

4.1 实施方式

本系统使用双单向安全传输系统将外总线模块与内总线模块分隔两端。外总线模块接收应用系统请求后进行 JSON-RPC 协议转换后发布请求消息，外端单向安全传输系统接收消息并将消息发布到内端消息服务器，内总线模块接收消息后进行协议转换并向信息资源系统发送请求，待获得服务响应消息后协议转换发布响应消息，内端单向

安全传输系统接收消息并将消息发布到外端消息服务器，外总线模块收到消息后进行协议转换向应用系统发送响应消息。本系统根据不同业务量级可采用不同应用模式，具体实施方案如下：

4.1.1　总线与单向安全传输系统一对一部署

当业务场景请求和响应流量均衡，且并发均衡没有达到总线性能极限时，单向安全传输系统及总线资源消耗相当，一对一的部署模式合理有效。具体部署方式如图 18 所示。

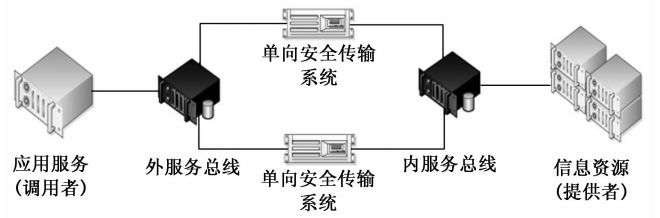

图 18　一对一部署方式

4.1.2　总线与单向安全传输系统多对一部署

当业务场景请求和响应流量比较大时，外总线接收应用服务请求、内总线路由资源消耗资源较大，同时向应用服务响应消息性能降低，此时单向安全传输系统资源占用率低，可部署多套总线通过负载均衡分配资源，实现资源利用最大化。具体部署方式如图 19 所示。

4.1.3　总线与单向安全传输系统一对多部署

当业务并发较大但是流量较小时，总线处理时间较短，单向安全传输系统性能达到极限，可部署多套单向安全传输系统加速传输消息，使整体性能发挥极致。具体部署方式如图 20 所示。

4.2　应用案例

本文所设计系统已在某市相关部门进行实际验证，并

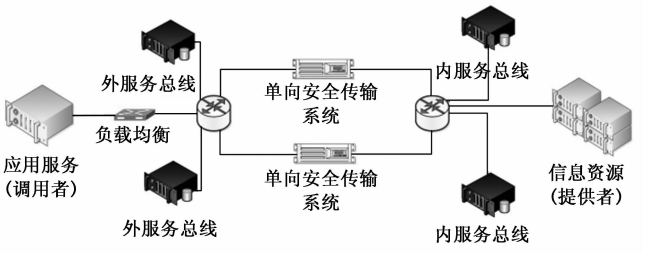

图 19　多对一部署方式

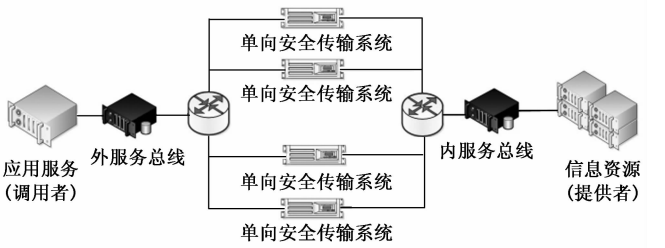

图 20　一对多部署方式

取得较好效果。具体部署方式如图 21 所示。

某市社企专网与某部门信息内网间需实现跨网请求信息共享，特通过本文设计的服务总线平台实现信息的高效交互。其中，分别在应用服务区和部门信息内网中部署了外服务总线系统和内服务总线系统，通过二者相互配合的形式实现对服务方请求接口的代理。同时支持接收中心服务推送的同步信息，包括：请求方/服务方的注册信息、授权信息以及服务目录和授权目录等资源。当社企专网侧请求方发起请求时，应用服务区外服务总线在接收到来自请求方的请求后，将通过请求方登记的注册信息，按登记的请求方式和协议对请求内容进行重新组织，然后向部门信

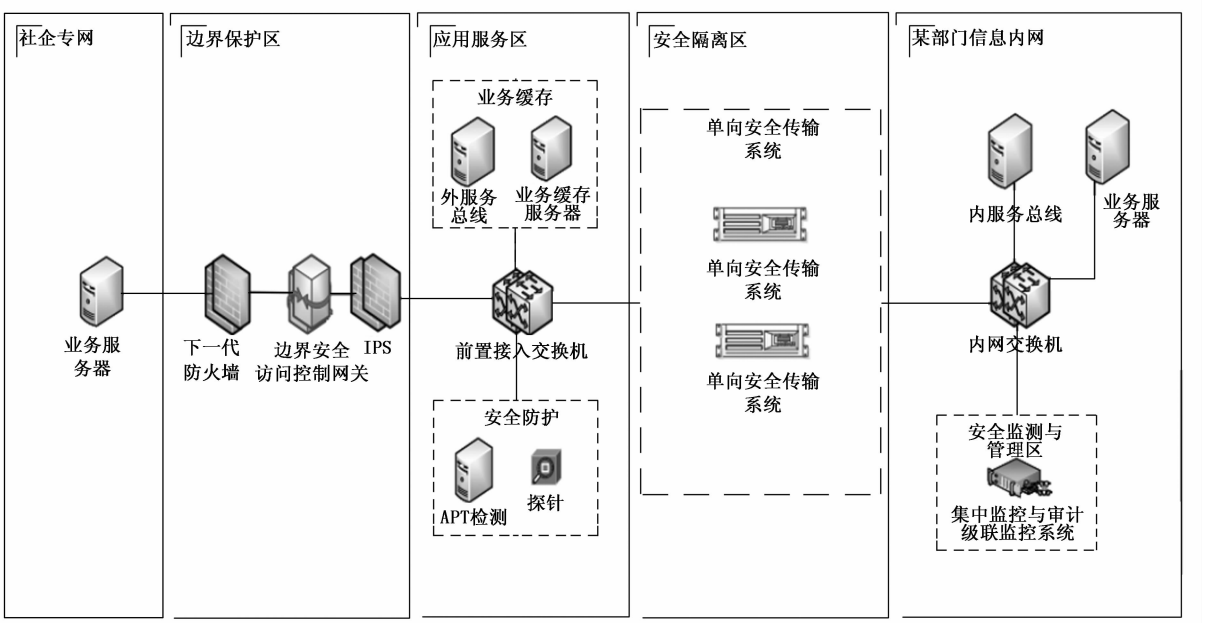

图 21　某市相关部门服务总线平台部署方式

息内网业务服务器发起请求，在内服务器总线取得业务服务器响应后，转发请求响应信息至社企专网侧请求方。

结合该部门业务需求，平台在设计登陆时采用了证书加密码的多因子验证登陆，用来实现超时鉴别登陆功能；系统管理权限采用了系统管理员、安全管理员、审计管理员三权分立管理能力；业务服务支持服务请求方、服务方的注册、修改、审批、查询功能；请求业务传输支持 Restful、Webservice 接口方式，并提供统一入口，支持 http 通讯协议；支持访问控制，包括黑白名单访问控制、调用频率控制、字段过滤等功能。此外，为了满足该部门请求服务的性能要求，本平台设计了一种包含一个 CRSS-CT（主节点）和三个 CRSS-ND（子节点）的部署方式，当请求数据包大小 1 kB 时，请求并发数能达到 7 200 个/秒。

为了提升方案整体的安全性，通常在实际应用中需要在边界保护区、应用服务区、安全隔离区进行安全加固。其中，各区域作用如下：

边界保护区：该区域主要实现平台和数据的第一层跨网域安全防护。

应用服务区：该区域主要处理各类与应用相关的操作，是跨网交互进行数据交换的数据缓存区域。

安全隔离区：该区域实现部门信息内网与应用服务区的信息单向传输，保证跨区域之间的安全隔离。

5 结束语

当前，面对以大数据、物联网、人工智能为代表的新一轮科技革命浪潮，全国泛政府行业均在积极推进行业大数据战略，在科技创新、数据共享、安全保护等方面进行前瞻性布局，全面推动政府工作质量变革、效率变革。本文提出的泛政府行业信息化数据资源跨域共享的服务总线，采用“资源状态联动计算”机制，实现独占通道、独占带宽、共享带宽三种类型的资源调度；采用“统一申请、授权”接口定义，实现服务资源、资产的统一管理，有效保障数据传输的安全、可控、可管；基于服务总线（ESB）体系架构，以及统一定义请求调用接口，实现跨区域、跨网络间服务授权访问、资源授权调用、数据安全转发、监控信息上报。本文所提泛政府行业信息化数据跨域共享服务总线技术及系统，有效解决不同网域间数据的互联互通，为政府行业实战提供数据实时共享和应用。

参考文献：

[1] 田洪亮，张 勇，李 超，等. 云环境下数据库机密性保护技术研究综述 [J]. 计算机学报，2017，40 (10)：2245－2270.

[2] 沈昌祥，张大伟，刘吉强，等. 可信 3.0 战略：可信计算的革命性演变 [J]. 中国工程科学，2016，18 (6)：53－57.

[3] 张玉清，王晓菲，刘雪峰，等. 云计算环境安全综述 [J]. 软件学报，2016，27 (6)：1328－1348.

[4] 张雪亚. 计算存储数据安全访问控制机制研究 [J]. 计算机测量与控制，2018，26 (5)：242－244.

[5] 刘 江，张 静. 基于企业服务总线的电子战系统集成方法 [J]. 电子信息对抗技术，2021，36 (4)：16－19.

[6] 王晓妮，段 群. 基于云计算的数据安全风险及防御策略研究 [J]. 计算机测量与控制，2019，27 (5)：199－202.

[7] 方 路，胡 勇. 基于 UDP 协议的文件单向传输系统 [J]. 网络安全技术与应用，2014，(12)：56－57.

[8] 樊志杰，胡正梁，熊已兴，等. 基于单向光的数据安全传输控制系统的设计与实现 [J]. 计算机测量与控制，2021，29 (2)：103－107.

[9] DING Y L，ZHAI Y Q. Intrusion detection system for NSL－KDD dataset using convolutional neural networks [C] //Proceedings of the 2018 2nd International Conference on Computer Science and Artificial Intelligence. ACM，2018：81－85.

[10] FAN Z J，CAO Z W. Method of network intrusion discovery based on convolutional long－short term memory network and implementation in VSS [J]. IEEE Access，2021，9：122744－122753.

[11] AKBANOV M，VASSILSKOS V G，LOGOTHETIS M D. Ransomware detection and mitigation using software－defined networking：the case of WannaCry [J]. Computers & Electrical Engineering，2019，76：111－121.

[12] 李 超，韩 翔，刘 钊，等. 基于可信计算的跨网数据安全交换技术 [J]. 计算机工程与设计，2021，42 (10)：2762－2769.

[13] 樊志杰，郑长松，曹志威. 基于动态策略的移动警务终端安全管控系统的设计与实现 [J]. 计算机测量与控制，2021，29 (6)：219－223.

[14] CAO Q，SHEN H W，GAO J H，et al. Popularity prediction on social platforms with coupled graph neural networks [C] //Proceedings of the 13th International Conference on Web Search and Data Mining，Houston，Texas，UAS，2020：70－78.

[15] 周 昕，张春慧. 基于微服务架构的融合指挥调度应用 [J]. 警察技术，2021，5：47－50.

[16] ZHAO P，FAN Z J，CAO Z W，et al. Intrusion detection model using temporal convolutional network blend into attention mechanism [J]. International Journal of Information Security and Privacy，2022，16 (1)：1－20.

[17] 魏松杰，李莎莎，王佳贺. 基于身份密码系统和区块链的跨域认证协议 [J]. 计算机学报，2021，44 (5)：908－920.

[18] 谢绒娜，郭云川，李凤华. 面向数据跨域流转的延伸访问控制机制 [J]. 通信学报，2019，40 (7)：67－76.

[19] 王蒙蒙，朱婉婷. 面向联合作战的跨域数据安全互联方法 [J]. 中国电子科学研究院学报，2020，15 (5)：442－448.

[20] 鲁金钿，肖睿智，金舒原. 云数据安全研究进展 [J]. 电子与信息学报，2021，43 (4)：881－891.

[21] 郭 亮，张吉智，陈心怡，等. 数据安全复合治理模式研究 [J]. 信息安全研究. 2021，7 (12)：1110－1120.