文章编号:1671-4598(2023)04-0264-08 DOI:10.16526/j.cnki.11—4762/tp.2023.04.041 中图分类号:TP399 文献标识码:A

移动警务跨域消息提醒服务系统的设计与实现

邵旭东[1]，曹志威[2]，樊志杰[1,2]，吕抒钺[2]，姚文猛[2]，张 林[2]
(1. 公安部第三研究所 信息安全技术部，上海 200031；
2. 上海辰锐信息科技有限公司 研发中心，上海 200031)

摘要：对移动警务平台双域终端消息无法互达的问题进行了研究，提出了移动警务平台侧跨域互通的即时消息提醒服务系统的设计方案；基于MQTT技术实现移动端消息推送，基于AMQP等移动警务平台跨域边界消息队列同步服务实现平台侧消息跨域同步，基于restful规范设计移动警务平台内面向业务应用的跨域终端消息推送服务接口，为移动警务平台内业务应用统一提供跨域终端消息推送服务；整个系统由消息接口模块、终端档案管理模块、跨区域同步模块、消息匹配审计模块和消息推送模块构成，可实现业务系统不同重要等级消息即时高效、安全合规的跨域终端推送。系统关键性能指标消息丢失率≤0.1‰，接口处理能力（TPS）≥20 000。

关键词：移动警务；跨域消息；消息提醒；边界隔离；同步服务

Design and Implementation of Cross Domain Notification Service System for Mobile Police

SHAO Xudong[1], CAO Zhiwei[2], FAN Zhijie[1,2], LYU Shuyue[2], YAO Wenmeng[2], ZHANG Lin[2]
(1. Department of Information Security Technology, The Third Research Institute of the Ministry of Public Security, Shanghai 200031, China;
2. Research and Development Center, Shanghai Chenrui Information Technology Company, Shanghai 200031, China)

Abstract: Aimed at the problem that the notifications of mobile police platforms with dual-mode terminal cannot be delivered, a feasible design scheme of cross domain instant notification service system for mobile police platforms is proposed, the system is composed of the notification receiving module, terminal file management module, cross domain synchronization mechanism, message matching audit module, notification service push module. Based on the MQTT technology, the message push of the mobile terminal is realized; Based on the AMQP mobile police platform with cross domain border message queue synchronization service, the cross-domain synchronization of the platform messages is realized. Based on the restful specification design, the cross-terminal service message of applying in the mobile police platform is pushed to the service interface, which provides with the cross-terminal push service message for the mobile police platform application, it realizes the instant high efficient and secure cross-terminal service push of different important levels in business systems. The message loss rate of key performance index is up to 0.1‰ and the interface processing capacity is greater than or equal to 20 000 transactions per second (TPS).

Keywords: mobile police; cross-domain message; notification; border gap; service synchronization

0 引言

移动警务平台是相关部门组织建设为广大警务人员以及社会协治力量提供移动办公、移动执法等活动的信息化平台。移动警务平台基于信息系统处理数据的安全需求和服务用户群体性质分为移动互联网服务子平台（以下简称Ⅰ类区）、联网服务子平台（以下简称Ⅱ类区）和信息网服务子平台（以下简称Ⅲ类区）。其中Ⅰ类区平台允许普通商业移动终端接入，Ⅱ类区和Ⅲ类区只允许符合GAT1466.1—2018《智能手机型移动警务终端第1部分：技术要求》和GAT1466.2—2018《智能手机型移动警务终端第2部分：安全监控组件技术规范》的移动终端接入。

并且，为推进移动化办公，和在提升执法效率同时维护信息系统数据安全，各地相关部门为广大一线人员采购配发了移动警务专用终端。此类终端的共同特点是同一个硬件终端运行生活域和工作域双系统，满足警务用户在同一个终端处理不同安全要求的业务应用和数据的需求，生活域和工作域两个系统之间在终端侧完全隔离，信息无法互通。实际使用过程中工作域系统只能连接Ⅱ类区，然后

收稿日期:2022-12-14； 修回日期:2022-12-18。
基金项目:上海市自然科学基金资助(21ZR1422000)；上海市人才发展资金资助(2020016)；中国博士后科学基金资助(2020M670998)；公安部科技计划项目资助(2019JZX004)；四川省科技计划项目(重点研发项目)(2021YFS0310)。
作者简介:邵旭东(1976-)，男，浙江余姚人，硕士，副研究员，主要从事信息与网络安全方向的研究。
通讯作者:曹志威(1985-)，男，山西朔州人，博士，助理研究员，主要从事信息与网络安全方向的研究。
引用格式:邵旭东，曹志威，樊志杰，等.移动警务跨域消息提醒服务系统的设计与实现[J].计算机测量与控制，2023，31(4)：264-271.

通过 VPN 加密通道的方式连接Ⅲ类区，生活域系统只能连接Ⅰ类区，这就导致终端处于生活域状态时用户无法获悉其工作域信息，处于工作域状态时用户无法获悉其生活域信息，严重导致了警务用户处理流转型和通知型业务的滞后，违背了移动警务业务的效率提升的初衷。

基于此研究人员提出了一套基于移动警务平台侧信息同步的消息推送方案，实现移动警务终端生活域和工作域之间的业务提醒消息的互通。基于该方案设计开发了一套移动警务跨区域消息提醒服务系统，通过平台侧进行信息的同步，然后在移动警务相应子平台区域内进行信息的终端推送，以满足用户跨区域的消息接收的需求。

其中包括：设计了平台侧消息、系统配置、系统状态等数据同步协议；设计了移动终端保活、消息推送协议；设计了消息内容匹配审计算法，按照移动警务平台的数据安全要求，对跨区域的信息进行白名单式的匹配审计，防止敏感信息泄漏。

1　系统结构及原理

本文所设计“移动警务跨域消息提醒服务系统”，由“移动警务跨域消息提醒服务端”和“移动警务专用终端消息提醒组件”两个部分组成，如图 1 所示。

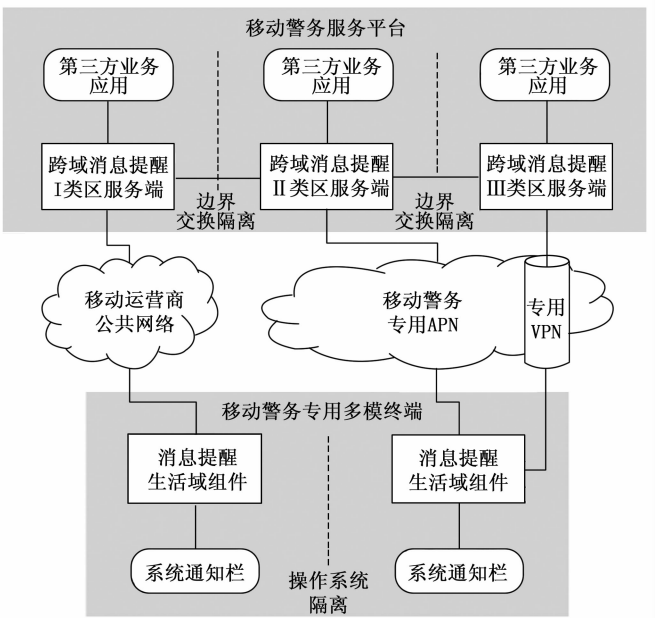

图 1　系统部署结构示意图

1.1　移动警务跨域消息提醒服务端

以下简称：服务端。适用于在“移动警务服务平台”（以下简称：平台）的三个被边界所隔离的Ⅰ/Ⅱ/Ⅲ类区子平台中分别部署：

服务端与其它内外部系统须要建立起业务连接，包括：

1）与“移动警务第三方业务应用”（以下简称：第三方应用）连接，通过本系统消息提醒服务接口，承接第三方发起的向移动端送达消息的请求；

2）与移动端衔接，支撑消息提醒向移动端送达所必须的相关交互；

3）透过边界交换隔离，与临近区域子平台的服务端进行沟通，实现消息提醒相关数据的跨域交换和同步；

4）Ⅱ类区服务端，除了与Ⅰ、Ⅲ类区两个服务端跨接外，还为Ⅰ、Ⅲ类区提供数据交换同步的中转代理，实现两个类区的间接连接。

1.2　移动警务专用终端消息提醒组件

以下简称：移动端。适用于在“移动警务专用双域终端”（以下简称：终端）的两个隔离操作系统中分别安装：

1）生活域：接入移动运营商公共移动通信网络，可访问互联网及移动警务Ⅰ类区平台；

2）工作域：接入移动警务专用 APN，可访问移动警务Ⅱ类区平台；通过拨通专用 VPN，还可在与Ⅱ类区隔离的情况下，访问Ⅲ类区平台。

移动端与平台可访子平台的服务端之间建立业务连接，支撑消息的送达；同时调用终端操作系统相关接口，将消息最终发送到系统通知栏显示。

1.3　消息送达

基于上述系统形态、组成及其相互连接关系，第三方应用在任意子平台内发起的消息推送请求皆可沿一定路径，跨越 n（$0 \leqslant n \leqslant 2$）次边界，送达至终端当前激活系统中的移动端组件，并在系统通知栏中显示给用户。

按跨越边界次数 n 不同，消息送达路径可分为三类场景：

1.3.1　临近跨域送达类（$n=1$）

如图 2 所示，此类消息送达路径仅须跨越边界一次，并经由两个部署于不同区域的服务端：

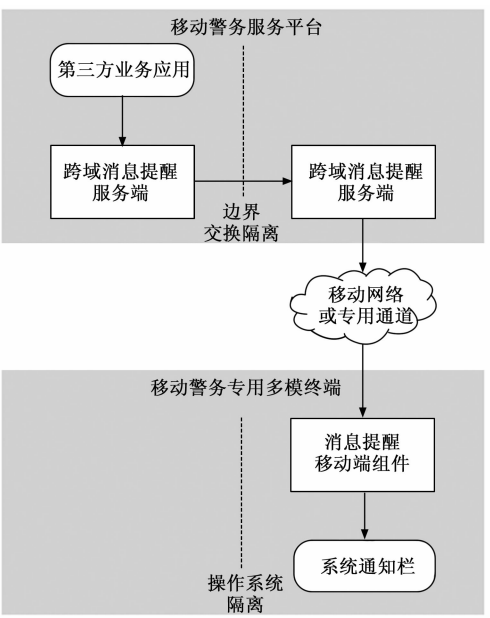

图 2　临近跨域送达路径图

在实际应用中，存在 4 种场景：

1）Ⅰ类区→Ⅱ类区→工作域（未拨 VPN）；

2）Ⅱ类区→Ⅰ类区→生活域；

3）Ⅲ类区→Ⅱ类区→工作域（未拨 VPN）；

4) Ⅱ类区→Ⅲ类区→工作域（已拨 VPN）。

1.3.2 代理跨域送达类（$n=2$）

如图 3 所示，此类消息送达路径须跨越边界两次，并经由三个部署于不同子平台的服务端。

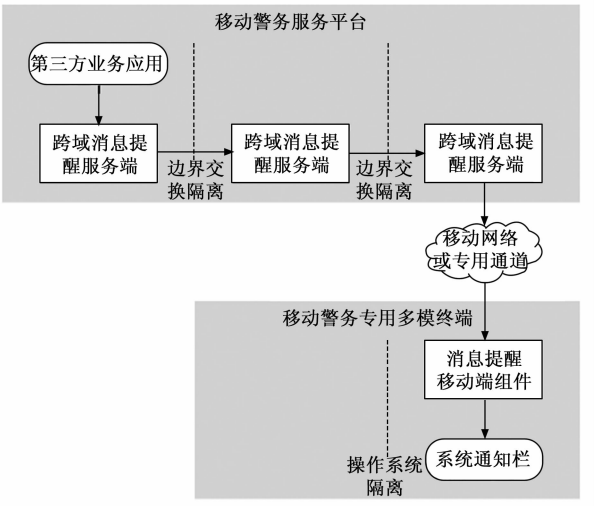

图 3 代理跨域送达路径图

在实际应用中，存在 2 种场景：

1) Ⅰ类区→Ⅱ类区→Ⅲ类区→工作域（已拨 VPN）；

2) Ⅲ类区→Ⅱ类区→生活域。

1.3.3 非跨域直接送达类（$n=0$）

如图 4 所示，此类消息送达路径不用跨越边界，仅须经由当前区域的服务端即可。

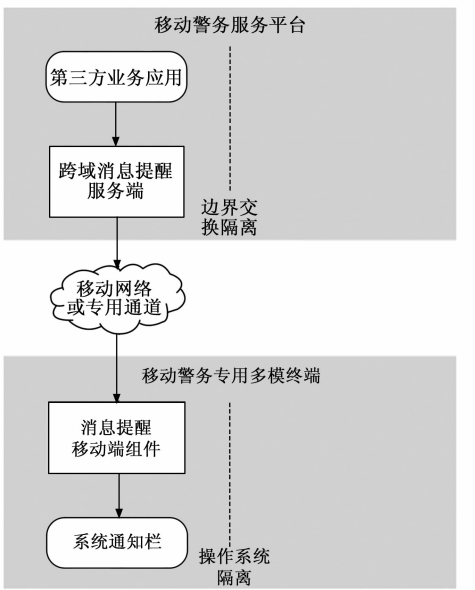

图 4 非跨域送达路径图

在实际应用中，存在 3 种场景：

1) Ⅰ类区→生活域；

2) Ⅱ类区→工作域（未拨 VPN）；

3) Ⅲ类区→工作域（已拨 VPN）。

此类非跨域场景，通常可由第三方应用自行完成向其在移动端中安装的对应客户端的消息送达，因此在实际应用中鲜有需求。

1.4 终端激活区域的识别

基于对上述送达路径的分析可知：系统在进行消息推送服务时，必须根据本次请求指定的目标终端当前实际激活的系统区域来确定消息的送达路径。

鉴于终端生活域和工作域的激活是排他性的，非激活区域下的移动端组件随系统处于冻结状态，失去了与服务端进行任何交互的能力。因此，对于同一终端，在任何时间，只可能有不多于 1 个服务端检测到其在线状态。

因此，系统基于终端在线状态信息，即可实现对终端激活区域的准确识别，并用于确定本次消息的送达路径。

2 系统软件设计

综合前面章节内容，整个消息提醒系统在设计上分为两个部分：

1) 消息提醒服务端；

2) 消息提醒移动端组件。

如图 5 所示。

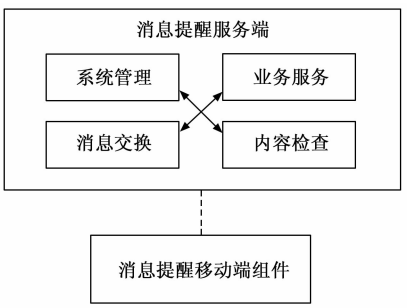

图 5 系统模块组成结构图

其中，服务端的功能和组成更为复杂，核心模块包括：系统管理模块、业务服务模块、通用消息交换组件、内容检查过滤组件等。

2.1 系统管理模块

本系统的 WEB 管理后台，提供给业务管理人员和运维人员使用，执行档案管理、运维管理、审计管理等操作。功能组成如图 6 所示。

系统管理模块采用典型三层架构设计，基于主流 Spring 框架构建。

2.2 业务服务模块

业务服务模块是服务端的对外服务界面，基于 Spring Boot 框架构建，结构如图 7 所示。

按照业务服务对象不同，以及交互承载协议的不同，服务分为消息推送服务和移动端服务两部分。

2.2.1 消息推送服务

向第三方提供业务服务，设计采用 HTTPS 作为接口承载协议，引入 WebFlux 技术支撑高并发处理。

消息提醒接口设计符合 RESTful 风格，请求数据体为 JSON 结构，定义如下：

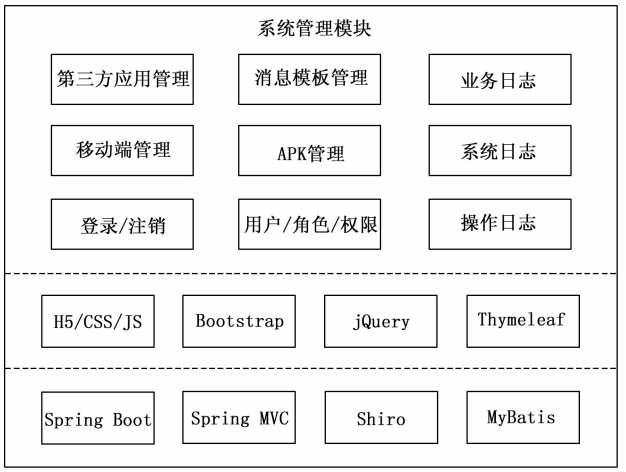

图 6　系统管理模块结构图

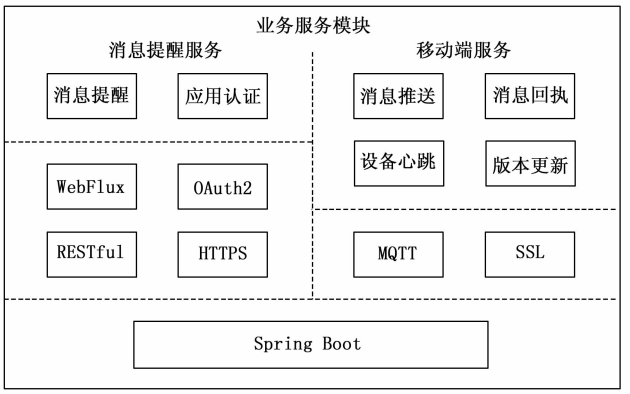

图 7　业务服务模块结构图

```
{
  "notification": {
    "application": String,
    "category": String,
    "title": String,
    "content": String,
    "importance": String
  },
  "recipients": [String, …]
}
```

应用身份认证设计采用 OAuth2 规范。

2.2.2　移动端服务

向移动端组件提供业务服务，设计采用 MQTT＋SSL 作为接口承载协议。作为轻量的发布/订阅范式消息协议，MQTT 具有简单、开放、易于实现的特点，适用于移动端耗能敏感和网络质量受限环境。

移动端服务包括 4 个核心接口：

1）消息推送接口（Notify）。由服务端向移动端下行推送，携带消息标题、正文、源应用、重要性等信息，并携带一个唯一 ID 作为回执凭据；

2）消息回执接口（Receipt）。由移动端向服务端上行推送，携带移动端已收讫消息的唯一 ID；

3）设备心跳接口（Alive）。由移动端向服务端上行推送，携带 IMEI 号等设备信息及组件版本信息，推送时机由移动端基于网络环境、耗电情况自适应确定；

4）版本更新接口（Upgrade）。由服务端向移动端下行推送，携带版本号、下载地址等更新信息，服务端根据设备上行心跳信息确定是否需要下行版本更新通知。

2.3　通用消息交换组件

跨域消息推送的实现，依赖于有效的跨边界数据交换能力。基于功能内聚、分层解耦的原则，设计一个专用组件——通用消息交换（以下简称：GMX），将相关功能进行抽象封装，作为基础服务层，向整个系统统一提供跨边界操作能力。

如图 8 所示，GMX 组件设计由以下几层组成：

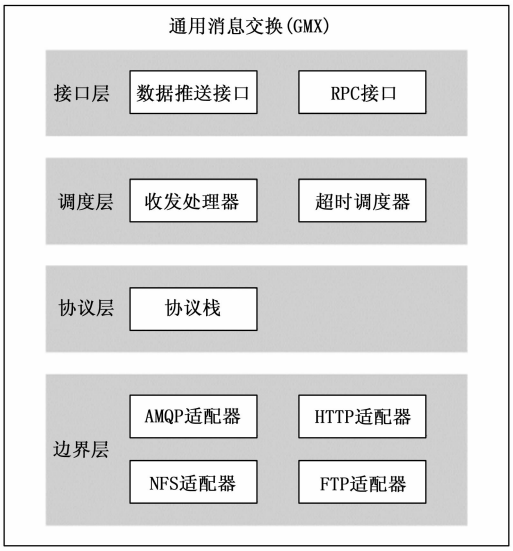

图 8　通用消息交换（GMX）组件结构图

2.3.1　接口层

接口层是 GMX 组件对外提供服务的界面，设计有两种跨边界操作接口。

1）数据推送接口：简单的单向点到点异步消息传送模式，提供从本地服务端跨越边界向其它类区服务端发送特定业务消息的能力，不提供对端响应机制；此种方式更为简单、轻量、高效，因其不包含回馈处理机制，仅适用于发送后不管，或有其它机制保障一致性的场景；

2）远程过程调用（RPC）接口：基于双向平衡传输模式（即：一问一答），提供从本地服务端跨越边界异步调用其它类区服务端相关方法、接口、过程并返回结果的能力；相比推送方式，此方式提供了响应回调机制，因而更加可靠、完整，相应的也更为复杂，适用于数据同步等一致性要求较高场景。

以上两种 GMX 接口调用的服务时序设计如图 9 所示（省略了与移动警务平台跨边界交换服务部分）。

2.3.2　调度层

调度层包含了 GMX 组件的核心逻辑，包括：数据发送、数据接收、异步数据处理、异步回调处理、RPC 超时

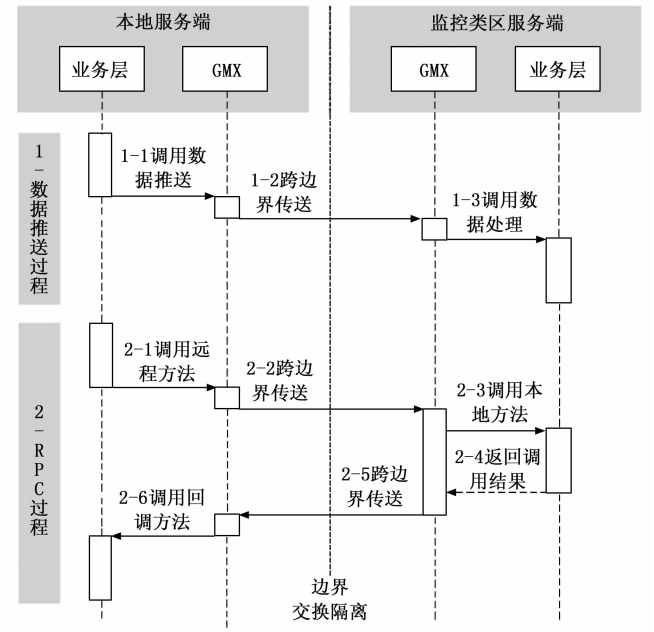

图 9 GMX 服务时序图

处理、等等。为了适应跨边界交互的高并发要求，调度层设计采用全异步非阻塞（NIO）处理技术，提升计算资源利用率；同时构建专用线程池，作为任务容器，实现可伸缩事务处理。

2.3.3 协议层

GMX 调度层中的逻辑操作针对的是 GMX 业务对象，而边界层实际传输数据为字节流形式。协议层设计在调度层和边界层之间，实现 GMX 业务对象与数据字节流之间的相互转换。

按照分层解耦的设计原则，协议层采用可插拔协议栈设计，如图 10 所示。

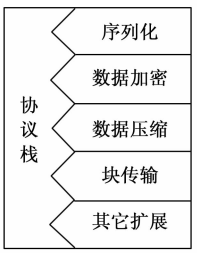

图 10 GMX 协议栈示意图

协议栈从上至下可根据不同场景需求，插入多层不同用途协议，包括但不限于：

1）序列化。核心协议，实现 GMX 业务对象与数据字节流之间的转换，可选实现有：JAVA Serializable、JSON、BSON、XML、Protobuf、等等；

2）数据加密。可选协议，用于提升数据安全性，可用实现有：DES、AES、RSA、等等；

3）数据压缩。可选协议，用于提升数据传输效率；

4）块传输。消息提醒业务典型的跨边界交互对象较小，若每个业务对象都分开传送，则跨边界通道资源利用会较低，传输负载越高，传输效率降低将越显著；为此，设计块传输协议，实现在高并发情况下，将多个较小的业务对象合并为大数据块一次性传送，降低服务端输出到跨边界通道的 IPS 压力，提升通道运行性能和传输效率。

2.3.4 边界层

边界层是 GMX 组件乃至整个服务端，面向移动警务平台跨边界交换服务的最外层界面，通过与边界交换对接，实现与边界对端的数据收发。

AMQP 是面向消息队列的，基于与上层产品、语言无关的，工作在应用层的，二进制开放协议。AMQP 提供客户端应用与消息队列服务之间，建立多通道、协商、异步、安全、中立和高效的交互。AMQP 协议是消息提醒业务跨边界数据交互的首选方案。

但是，鉴于移动警务体系中，跨边界环境和方式较为复杂，确实存在不兼容 AMQP 的情况。其它较常用的跨边界交换方式还有：文件方式（包括：本地文件、NFS、FTP 等）、基于 HTTP 协议的服务总线、等等。针对多种不同交换方式共存的情况，边界层采用适配器模型设计，针对不同交换方式，实现不同适配器，并按需加载，以提供兼容性。

2.4 内容检查过滤组件

内容检查过滤是服务端的核心功能之一，针对的是第三方发起的消息提醒请求，实现对消息提醒的细粒度约束性检查，过滤掉不符合安全定义的非法请求。

消息提醒的内容检查过滤规则由消息模板定义。第三方发起消息提醒服务请求时，必须指定本次使用的消息模板。服务端则装载该指定模板，并依据约束定义完成对消息请求的各项检查。根据检查结果，确定是提供本次服务还是过滤本次请求。

如图 11 所示，整个检查过滤流程包含对四个核心约束项的检查过滤：

2.4.1 应用白名单

每个消息模板定义有应用白名单，用于约束适用应用范围。只有在白名单范围内的业务应用可使用该模板发起消息提醒请求，范围以外的应用请求将视为非法，不予提供服务。

2.4.2 送达路径白名单

每个消息模板定义有送达路径白名单，用于约束消息提醒向终端送达时，允许经由的路径（关于可用路径，可参见 1.3 章节）。

服务端在运行时，根据移动端的当前激活区域，确定本次送达的须循路径，并比对消息模板定义的路径白名单，决定是否继续服务。

2.4.3 消息标题

每个消息模板对允许的消息标题文本进行约束定义，设计提供两种检查方式：

1）静态文本检查。第三方提交的消息提醒请求必须严格使用该定义的消息标题，否则将视为非法请求而丢弃；

2）动态表达式匹配。为覆盖动态文本场景，采用正则

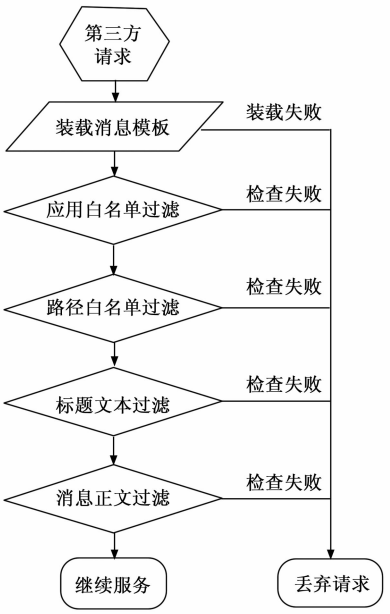

图 11　内容检查过滤流程示意图

表达式作为定义语法，在运行时对第三方提交的消息提醒请求的标题文本进行正则匹配运算，通过检查的放行，否则丢弃。

2.4.4　消息正文

与 2.4.3 中消息标题的检查过滤算法相同，每个消息模本选择“静态文本检查”和“动态表达式匹配”两种检查过滤方式中的一种，对允许的消息正文内容进行约束定义。服务端在运行时执行对该约束项的检查和过滤。

2.5　移动端组件

本文设计的消息提醒移动端组件，针对 Android 系统（9.0 及以上版本），适用于移动警务专用终端的生活域和工作域安装，软件结构设计如图 12 所示。

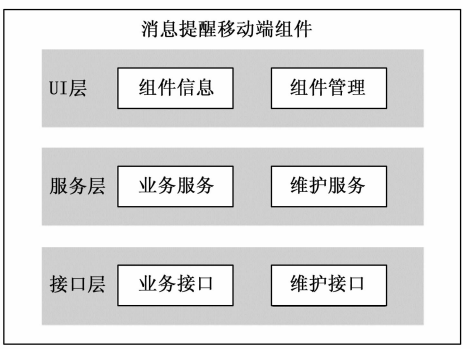

图 12　移动端组件结构图

2.5.1　UI 层

基于 Android Activity 组件构建，提供对移动端组件进行维护性操作的相关用户界面，包括：

1）组件信息。展示维护性信息，包括：组件信息（版本、版权等）、设备信息（品牌、型号、系统版本、IMEI 等）、运行日志、等等；

2）组件管理。提供维护性操作，包括：组件参数设置、可用版本升级等。

2.5.2　服务层

基于 Android Service 组件构建，自动运行于系统后台，分为两类：

1）业务服务。实现消息提醒核心业务逻辑，包括：接收服务端推送的消息提醒、反馈消息回执、基于 Android Notification 组件显示消息提醒到系统通知栏等；

2）维护服务。实现对上行（对接服务端）链路的维护、获取设备信息、推送设备心跳、接收处理版本更新等；

2.5.3　接口层

构建在 MQTT 协议之上，将与服务端的对接接口进行封装，分为两类：

1）业务接口。包括：下行消息推送接口（Notify）、上行消息回执接口（Receipt）；

2）维护接口。包括：上行设备心跳接口（Alive）、下行版本更新接口（Upgrade）。

3　系统主要功能

本系统核心功能包括：消息接收、消息推送、跨区域同步、消息匹配审计、终端档案管理。

3.1　消息接收

消息接收基于 restful 规范设计面向消息发送方的消息推送 API 接口，接口内容主要包括以下几方面内容。

1）应用 ID、事务 ID 等消息发送方标识；

2）消息标题、消息内容、消息模板 ID、消息通知等级等消息内容信息；

3）消息收件人 IMEI 号码等消息接收方的信息。

3.2　终端档案管理

终端档案管理提供移动终端生活域和工作域的 IMEI 对应关系的维护管理，系统移动端消息推送基于该档案进行寻址。终端档案产生允许自动关联和手动创建两种方式。

由于相关部门采购的移动终端主要供应商的生活域和工作域 IMEI 号码存在固定算法的对应关系，系统支持提前预制各终端厂商的 IMEI 关系算法，将移动端采集上报的 IMEI 号码基于厂商型号和 IMEI 预制算法进行自动归档，自动生成移动终端生活域和工作域 IMEI 对应关系。

手动创建，由系统管理员进行手动收集移动终端生活域和工作域 IMEI 对应关系并手动导入创建终端档案。

3.3　跨区域同步

移动警务移动互联网服务子平台、联网服务子平台和信息网服务子平台之间采用双单向系统进行隔离，子平台之间的数据交互由各子平台内部服务总线代理。本系统在移动警务三个子平台内分别部署系统服务端，支持服务端之间的管理面数据和数据面信息同步，服务端之间数据交互由服务总线消息队列同步服务代理。

1）本系统设计由部署在联网服务子平台的系统服务端作为主控服务端，部署在移动互联网服务子平台和信息网服务子平台的系统服务端作控服务端。管理面数据都在主控服务端提供配置操作和集中展示，由主控服务端通过跨

区域同步至其它子平台服务端，管理面数据包括：系统配置操作、终端档案、系统状态信息等。

2）数据面信息指各个子平台服务端接收到需要推送到终端的消息。

3.4 消息匹配审计

为保证跨区域消息推送的消息内容不携带平台不允许传递的非法信息，本系统设计要求系统对接收的所有消息均需要通过消息匹配审计后才可以执行移动终端推送。

系统管理员需要预先在本系统进行消息模板配置，配置内容包括消息模板编号、消息标题、消息内容等，其中消息标题和消息内容支持正则匹配规则配置。对匹配成功的消息进行推送执行，匹配失败的消息进行丢弃处理。

3.5 消息推送

系统实现将需要推送到终端的信息准确及时地推送到对应终端，并依据相应消息通知等级进行提示音、震动、亮屏等一种或多种提醒方式。消息推送基于 MQTT 消息队列协议进行设计，实现系统服务端对移动端消息队列通道的管理维护、移动端信息上报以及消息推送。

1）移动端消息队列通道基于 MQTT 协议框架进行连接管理，支持 5 万级的连接保持。

2）移动端信息上报包括了 IEMI 号码、操作系统类型、操作系统版本、终端型号、厂商等移动终端属性信息上报。

3）消息推送分为服务端向移动端远程推送和移动端通知栏本地推送两个过程。远程推送基于服务端 MQTT 协议定制发布和移动端订阅消息队列实现服务端消息的定向推送，同时消息推送基于系统终端档案中 IMEI 号码进行推送寻址。移动端本地推送通过调用终端 notification 通知接口进行消息内容的通知栏推送。

4 系统应用实施方案

本系统由消息提醒服务端和消息提醒客户端组件两部分构成，服务端负责消息接收、匹配审计、终端档案维护、消息寻址推送。消息提醒客户端负责移动终端 IMEI 等信息上报、移动端推送通道维持、终端通知栏推送。

消息提醒服务端分别部署于移动警务平台Ⅰ/Ⅱ/Ⅲ类区，客户端组件分别安装在移动警务专用终端的生活域和工作域，生活域客户端通过互联网通道接入Ⅰ类区服务端，工作域客户端通过移动警务专网接入Ⅱ或Ⅲ类区。业务应用通过统一的消息推送接口将需要跨域发送的消息推送至本区域内的消息提醒服务端，业务应用推送的消息至少包括：消息接收终端的 IMEI 号码、消息标题、消息内容、消息模板 ID；消息提醒服务端基于系统配置的消息模板匹配消息合法性，基于终端档案匹配发送区域和终端寻址；对应合法并寻址成功的消息进行移动终端通知栏推送。

本系统部署实施主要包含：系统服务部署、跨边界通道配置、服务挂载、移动端分发和安装、四个步骤。

1）系统服务部署。消息提醒服务端分别部署于移动警务平台Ⅰ/Ⅱ/Ⅲ类区，本系统基于 centos7.0 操作系统部署运行，Ⅰ类区需要联通互联网，Ⅱ和Ⅲ类区需要联通移动警务专网分别提供移动警务终端生活域和工作域的网络接入。

2）跨边界通道配置。Ⅰ/Ⅱ/Ⅲ类区消息提醒服务端之间通过Ⅰ/Ⅱ/Ⅲ类区边界服务总线的消息队列同步服务进行通信，需要在跨区域服务总线上配置消息队列同步通道，用于承载Ⅰ/Ⅱ/Ⅲ类区消息提醒服务端之间配置数据、系统状态数据、消息数据等数据同步。

3）服务挂载。分别将Ⅰ/Ⅱ/Ⅲ类区消息提醒服务端的消息接收接口挂载注册到本区域内的服务总线，供本区域内的业务应用调用。

4）移动端组件分发和安装。移动端组件分发和安装方案基于首次安装和更新安装有所区分。首次安装基于移动警务专用终端操作系统预制组件的方案推送安装；对于生活域更新安装采用系统内自更新方式更新版本，工作域更新安装采用移动警务Ⅱ类区终端管控系统进行推送安装。

某省移动警务平台用户在工作域有信息需要处理的时候需要定期转到工作域进行查看，信息处理延迟取决于用户自身行为。自部署实施了移动警务跨域消息提醒服务系统之后，覆盖并满足了当地平台 2 万多警务用户的跨域消息提醒信息的传递，将用户跨区域接收信息的平均延迟降低到 1 秒以内，对工作效率起到了巨大的提升作用。

5 系统指标

5.1 功能指标

本方案所具备的功能指标，及其对比原有互通方案所具有的优势有：

1）采用平台侧消息联通机制传递消息，符合移动警务整体平台建设规范要求；而原有方案存在突破移动警务专用终端的双域隔离的情况，不符合移动警务专用终端要求。

2）增加了转发消息留存审计的能力。

3）增加了消息白名单过滤机制，对不符合安全规则的消息予以告警、丢弃等非法处置。

4）对转发消息的应用方进行统一注册和消息发送权限管理。

5）对终端消息组件进行统一管理。

6）对终端的兼容性强，所有警务终端都可以使用。

7）不需要移动端应用进行兼容适配。

8）不同应用可以定制符合规则的个性化消息内容。

9）支持Ⅰ/Ⅱ/Ⅲ类区之间的消息互通。

表 1 功能指标及优势对比

№	功能指标	本方案	原有方案
1	是否合规	合规	不合规
2	是否具备消息安全审计能力	具备	不具备
3	是否具备消息控制能力	具备	不具备
4	是否具备应用管理能力	具备	不具备
5	是否具备终端管理功能	具备	不具备
6	是否存在终端依赖	不存在	存在
7	是否存在 APK 适配	不存在	存在
8	是否支持消息定制	支持	不支持
9	是否支持Ⅱ/Ⅲ类区互通	支持	不支持

5.2　性能指标

本系统的性能指标聚焦于消息提醒接口的服务能力方面，包括如下几条：

1）接口并行能力≥5 万；

2）接口处理能力（TPS）≥2 万；

3）消息送达时延≤30 秒；

4）消息丢失率≤0.1‰。

针对以上指标，采用 JMeter、Mock 等工具对消息提醒接口（Notify）进行压力测试和性能验证。测试用例以并发连接数作为区分，共 10 个用例范围覆盖并发范围 500～60 000，具体数据如表 2 所示。

表 2　接口性能压力测试数据表

№	并发连接数	接口平均时延/ms	TPS/(n/s)	错误率/‰
1	500	13	38 462	—
2	1 000	23	43 478	—
3	2 500	54	46 296	—
4	5 000	107	46 729	—
5	10 000	214	46 729	—
6	20 000	426	46 948	—
7	30 000	649	46 225	—
8	40 000	892	44 843	—
9	50 000	1 156	43 253	0.03
10	60 000	1 507	39 814	0.07

其中，接口的处理能力——TPS、接口调用的平均时延，这两个指标与并发连接数的相关性如图 13 所示。

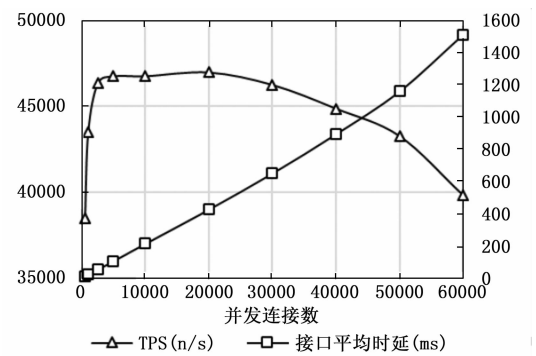

图 13　接口性能压测数据图

基于上述压测数据可见，系统主要性能指标均能满足要求。

6　结束语

在移动互联网广泛应用和革新的大背景下，以移动警务平台为主要信息化、移动化的执法办公平台面临着更大的人与人、人与系统的沟通增效压力。本文提出的通过移动警务平台侧跨域互通的即时消息服务系统基于移动警务平台跨域边界实现跨域消息互通、消息内容审计、移动终端消息推送，在满足平台数据安全要求的同时实现双域终端消息互通的业务需求，极大地提升了广大警务人员和社会协治力量的业务效率。

参考文献：

[1] 张　英. 基于 MQTT 协议的数据安全过滤组件的研究与实现[D]. 北京：华北电力大学，2021.

[2] 段粘粘，王益义. 浅谈基于 OAUTH2.0 统一身份认证的多应用系统优化[J]. 电子元器件与信息技术，2021，5（12）：246－248.

[3] 包晓安，聂凡杰，徐　璐，等. 基于 Reactor 与非阻塞 IO 的服务端框架设计与实现[J]. 浙江理工大学学报（自然科学版），2020，43（4）：520－526.

[4] 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.

[5] LEIBA B. Auto web authorization protocol[J]. IEEE Internet Computing，2012，16（1）：74－77.

[6] 赵思远. Java NIO 与 IO 性能对比分析[J]. 软件导刊，2021，20（4）：214－219.

[7] 吴克河，张　英，崔文超，等. 一种基于随机森林算法的 MQTT 异常流量检测方法[J]. 计算机与现代化，2021（1）：61－64.

[8] 赵思远. 基于 Java NIO 的高性能网络系统的研究与应用[D]. 北京：北京工业大学，2020.

[9] 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.

[10] PARK C S，NAM H M，et al. Security architecture and protocols for secure MQTT-SN[J]. IEEE Access，2020，8：226422－226436.

[11] 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.

[12] 孙丽琼. 基于 Netty 面向 Android 端消息推送系统的实现[D]. 成都：成都理工大学，2018.

[13] 庄国强. 一种基于 Netty 的环保物联网实时双向通信模型研究[J]. 郑州师范教育，2017，6（6）：36－41.

[14] 王　鹏，罗森林，潘丽敏. 一种高并发网络 Web 应用技术研究[J]. 信息网络安全，2017（12）：29－35.

[15] LIU Y，WEN J，JI D. Integration of naval distributed tactical training simulation system based on advanced message queuing protocol[J]. High Technology Letters，2016，22（4）：385－394.

[16] 杨　旸，潘俊臣. 基于 OAuth2.0 安全认证中间件的设计与实现[J]. 网络空间安全，2019，10（7）：6－10.

[17] 顾振德，刘子辰，龙　隆，等. 基于 Netty 的 IoT 终端通信服务系统设计[J]. 计算机应用与软件，2019，36（4）：135－139.

[18] 邢赛楠. MQTT 传输安全问题浅析[J]. 科技与创新，2018，1：17－18.

[19] 张　乐. 基于 AMQP 的即时通讯系统的实现[J]. 电子技术与软件工程，2017（5）：46－47.

[20] 王精丰. 基于单向光闸的传输控制系统的设计与实现[D]. 北京：北方工业大学，2016.

[21] 路晔绵，李轶夫，应凌云. Android 应用第三方推送服务安全分析与安全增强[J]. 计算机研究与发展，2016，53（11）：2431－2445.