国　际　电　信　联　盟

ITU-T X.1234

(01/2022)

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

网络空间安全 – 打击垃圾信息

关于打击多媒体消息服务垃圾信息的导则

ITU-T X.1234建议书

ITU-T X 系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
消息处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定	X.1080–X.1099
安全应用和服务（1）	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
网页安全（1）	X.1140–X.1149
应用安全（1）	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
网络安全	X.1200–X.1229
打击垃圾信息	**X.1230–X.1249**
身份管理	X.1250–X.1279
安全应用和服务（2）	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1319
智能电网安全	X.1330–X.1339
验证邮件	X.1340–X.1349
物联网（IoT）安全	X.1350–X.1369
智能交通系统（ITS）安全	X.1370–X.1399
分布式账簿技术（DLT）安全	X.1400–X.1429
应用安全（2）	X.1450–X.1459
网页安全（2）	X.1470–X.1489
网络安全信息交换	
网络安全概述	X.1500–X.1519
漏洞/状态信息交换	X.1520–X.1539
事件/事故/启发式信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
启发式和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589
网络保卫	X.1590–X.1599
云计算安全	
云计算安全概述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳做法和指导原则	X.1640–X.1659
云计算安全实施方案	X.1660–X.1679
其他云计算安全	X.1680–X.1699
量子通信	
术语	X.1700–X.1701
量子随机数发生器	X.1702–X.1709
QKDN安全框架	X.1710–X.1711
QKDN安全设计	X.1712–X.1719
QKDN安全技术	X.1720–X.1729
数据安全	
大数据安全	X.1750–X.1759
数据保护	X.1770–X.1789
IMT-2020安全	X.1800–X.1819

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1234 建议书

关于打击多媒体消息服务垃圾信息的导则

摘要

ITU-T X.1234建议书规定了关于打击MMS垃圾信息的导则。建议书对MMS垃圾信息的典型场景、特性和识别方法做出分析，提供MMS垃圾信息识别技术框架、工作程序和一些关键性技术，以帮助MMS提供商和MMS用户对抗垃圾信息。

历史沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T X.1234	2022-01-07	17	11.1002/1000/14796

关键词

多媒体消息服务、多媒体消息服务垃圾信息、技术框架

* 欲查阅建议书，请在您的网络浏览器地址域键入URL http://handle.itu.int/，随后输入建议书的唯一识别码，例如，http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利/软件版权保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列ITU-T网址查询相应的可用ITU-T据库：http://www.itu.int/ITU-T/ipr/。

目录

引言

多媒体消息服务（MMS）是通过蜂窝网络向移动电话发送和接收包括多媒体内容消息的标准方式。用户和提供商可将这种消息称为图片、视频、声音、动画等。随着电信技术的发展和智能手机的普及，MMS已成为一种主流信息发送方式，尤其是年轻人和媒体公司，他们将其作为一种商业方式来传递新闻和娱乐内容。MMS带来了便捷的社交和丰富多彩的信息，但也成为垃圾信息制造（发送）者发送MMS垃圾信息的方式。此类MMS垃圾信息，包括人们不期望的推介性广告、诈骗信息和病毒等，已成为一个普遍存在的问题，给电信运营商、服务提供商和用户造成了巨大的利益损失。

因此，有效打击MMS垃圾信息已成为反垃圾信息技术领域的一个重要方向。

ITU-T X.1234建议书

关于打击多媒体消息服务垃圾信息的导则

1 范围

本建议书提出打击MMS垃圾信息的技术框架，以实现MMS垃圾信息的治理和控制。该框架规定了MMS垃圾信息识别的功能成份、工作程序和一些关键性技术。此外，本建议书还涵盖了MMS垃圾信息的典型场景，并对不同类型MMS垃圾信息及其一般特性做出分析。

值得注意的是，本建议书中的所有操作都需要得到用户和管理法规的许可。为了避免侵犯用户的隐私，所有的程序都应严格遵循适用的法律。

2 参考文献

下列ITU-T建议书和其他参考文献的条款，通过在本文本中的引用而构成当前建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其他参考文献均面临修订；因此鼓励本建议书的使用者探讨使用下列建议书和其他参考文献最新版本的可能性。当前有效的ITUT-T建议书清单定期出版。在本建议书中引用某个独立文件时，并未给予该文件建议书的地位。

[ITU-T X.1231] ITU-T X.1231建议书（2008年）– 打击垃圾信息的技术策略

[ITU-T X.1247] ITU-T X.1247建议书（2016年）– 打击移动消息垃圾信息的技术框架

3 定义

3.1 他处规定的术语

本建议书使用以下在其它文献中定义的术语：

3.1.1 多媒体消息服务（MMS）[ITU-T X.1231]：多媒体消息是在短消息之后，基于移动通信网、无线网或者固定网提供的可以传送包括文本、图形、音频、视频等多媒体消息的消息服务。

3.1.2 多媒体消息服务（MMS）垃圾信息 [ITU-T X.1247]：通过MMS发送的垃圾信息。

3.1.3 垃圾信息制造者 [ITU-T X.1231]：产生和发送垃圾邮件的实体或个人。

3.2 本建议书定义的术语

本建议书定义的术语如下：

3.2.1 MMS垃圾信息识别功能（MMSSIF）：独立于多媒体消息服务中心（MMSC）的打击MMS垃圾信息的系统，包括以下功能成份：监控功能、数据采集功能、预处理功能、识别功能、核实功能、处置功能和系统管理功能。

4 缩写词和首字母缩略语

本建议书使用以下缩写词和首字母缩略语：

ASR 自动语音识别

MMS 多媒体消息服务

MMSC 多媒体消息服务中心

MMSSIF 多媒体消息服务垃圾信息识别功能

SMS 短消息服务

UICC 通用集成电路卡

URL 统一资源定位

5 惯例

本建议书使用下列惯例：

关键词“**应该**”（**should**）指的是一项建议性的、并非绝对要求的要求，因此，宣称遵循本建议书时无需提及该项要求。

关键词“**可以**”（**may**）表示允许作为选项但并非建议遵守的要求。

在本建议的正文中，有时会出现“**能/能够**”（**can**）一词，在这种情况下，它们将被解释为“**能/能够**”（**is able to**）。

6 概述

MMS是在短消息（SMS）之后引入的，基于移动通信网或IP网提供的可以传送包括文本、话音和视频等多媒体消息的消息服务。随着电信和互联网技术的高速发展，以及智能手机的快速普及，带来便捷的社交联系和丰富多彩信息的MMS，是发送信息的重要手段，尤其是年轻人和媒体公司，他们将其作为一种商业方式来传递新闻和娱乐内容。

然而，垃圾信息制造者也有可能发送MMS垃圾信息。MMS垃圾信息，包括未经请求的信息，如广告、欺诈、病毒和其他不需要的信息，正在成为一个普遍的问题，并给电信运营商、服务提供商和用户造成了巨大的利益损失。因此，如何从技术上有效地打击MMS垃圾信息已成为反垃圾信息领域的一项严峻挑战。

7 MMS垃圾信息的场景和特性

如图7-1所示，MMS程序包括三大步骤：(1) 发送方准备MMS内容，发送到其通用集成电路卡（UICC）所属的MMSC；(2) MMSC接收发送方发送的MMS内容，并决定是将该MMS发送至下一个MMS中心还是直接发送给接收方；(3) 接收方从MMSC接收MMS，但其使用的MMSC可能与发送方不同。

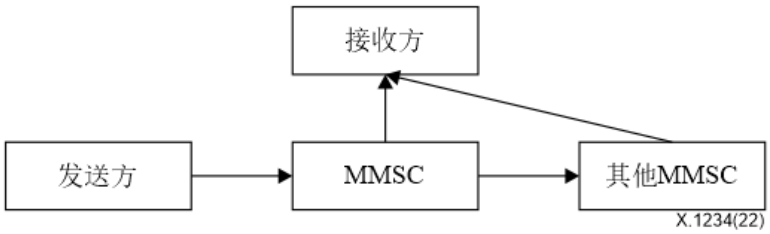


图7-1 – MMS程序

垃圾信息制造者会使用上述程序向用户发送垃圾信息，这非常令人讨厌，且可能给用户造成利益损失。这些垃圾信息内容可能包括广告、欺诈信息等。以下是MMS垃圾信息的一些典型场景：

1) 欺诈垃圾信息：这些是MMS垃圾信息，通过编造理由来吸引接收方相信他/她可能会得到一些好处或某事是真实的。如果接收方如消息所示做出回复，则接收方将被收取费用或签约订购欺诈公司的、旨在让其付款的某种增值服务。

2) 特洛伊垃圾信息：一些MMS垃圾信息带有特洛伊媒体文件，一旦它们发现手机有漏洞且手机用户打开媒体文件，则将获得手机系统的最高管理权限，然后可能在接收方完全未意识到的情况下窃取手机中的所有机密信息。

3) 病毒垃圾信息：MMS垃圾信息可能包含看起来正常的某种病毒设置文。一旦接收方点击并完成设置，则病毒即开始以多种可能的方式破坏电话系统，通常是通过快速删除或解离数据方式。

4) 不需要的广告：广告形式的MMS垃圾信息通常包括各种广告，如贷款、房屋销售、培训等。这些垃圾信息是在没有接收方许可或订购的情况下发送给接收方的。其中一些往往具有欺骗性，可能会在MMS图片或视频上放置广告链接，如果接收方点击图片或视频，则网络浏览器将被重新定向，转至广告页面。

8 技术框架导则

8.1 一般性结构

如图8-1所示，发送方向MMSC发送MMS，接收方从MMSC下载MMS，因此MMSC存储所有MMS。有鉴于此，建议在MMSC附近部署MMS垃圾信息识别功能（MMSSIF）。

任何打击垃圾信息技术都很难保证100%的准确率，为此MMSSIF也需要进行离线手动配置和管理，所以如图8-1所示，我们应该设置服务运营商。

同时，应修改原MMSC的工作流程，使MMSC向MMSSIF发送MMS，而不是在收到MMS后直接转发至接收方或下一个MMSC。MMSSIF判断MMS是否为垃圾信息，然后向MMSC提出相应建议。根据这些建议，MMSC将决定是否继续向接收方或下一个MMSC发送这条MMS。

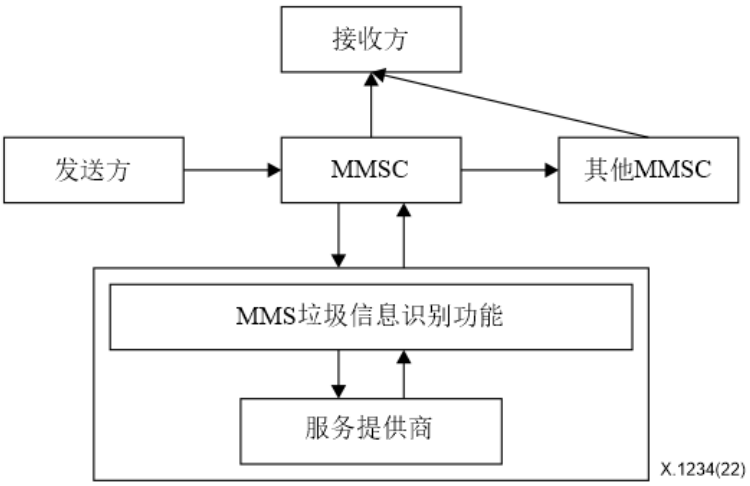


图 8-1 – 打击MMS垃圾信息的一般性结构

8.2 MMSSIF的参考结构

MMSSIF的参考结构主要包括对应不同功能的七个模块：监控、数据采集、预处理、识别、核实、处置和系统管理。建议将不同模块予以关联。此外，它们应根据相关协议确定的规则或政策相互协调。

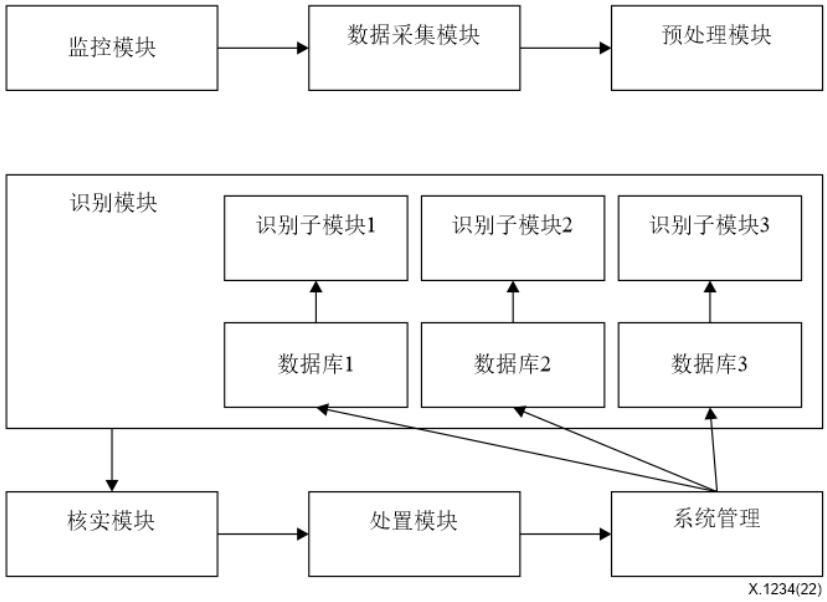


图 8-2 – MMSSIF的参考结构

在图8-2中，监控模块接收来自MMSC的MMS，并获取该MMS的字头，包括主题、发送方电话号码、附件数量、这些附件的URL等。

数据采集模块从监控模块接收MMS字头信息，然后从URL下载所有附件。

预处理模块从数据采集模块接收MMS的所有信息，包括字头和所有附件，然后根据规则对信息进行规范化。信息可能来自MMS的字头或正文，且信息类型可能是文本、图像、视频、音频等，因此建议规则为“来源+信息类型+信息”的综合规则。

识别模块接收来自预处理模块的规范化信息，通过黑名单、文本识别、图像识别、视频识别等技术分析该MMS是否为垃圾信息。

核实模块从识别模块接收可能的结果，并做出进一步的判断（如手动确定），以降低误报警的可能性。

处置模块接收来自核实模块的识别结果，并处置被判断为垃圾信息的MMS，如拦截MMS、向垃圾信息发送者发送提醒消息等。该模块还将原始MMS、处置日志和发送方电话号码发送至系统管理模块。

系统管理模块接收来自处置模块的记录，并保存操作日志和系统日志。该模块还将垃圾信息发送方电话号码、关键词和图像发送至识别模块中的不同数据库，以便更新数据库。

8.3 MMSSIF的功能成份

8.3.1 监控模块

监控模块的功能包括：

- 监控是否有新的MMS从MMSC发出；
- 接收MMS的完整数据流；
- 分析数据流并获取MMS字头；
- 向数据采集模块发送主题、发送方电话号码、附件数量、这些附件的URL和MMS正文。

8.3.2 数据采集模块

数据采集模块的功能包括：

- 接收来自监控模块的信息，并找到这些附件的URL；
- 下载所有附件；
- 向预处理模块发送MMS的所有信息，包括MMS的字头和含有所有附件的正文。

8.3.3 预处理模块

预处理模块的功能包括：

- 接收来自数据采集模块的所有信息；
- 检查所有附件并判断它们是文本、图像、音频还是视频，因为根据当前的MMS传输协议，只允许在MMS中包含文本、图像、音频或视频；
- 根据不同类型对信息进行分类，并根据规则对信息予以规范化，例如“来源+信息类型+信息”的综合规则；
- 向识别模块发送原始MMS、所有规范化信息和发送方电话号码。

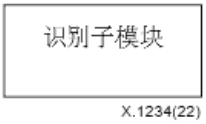
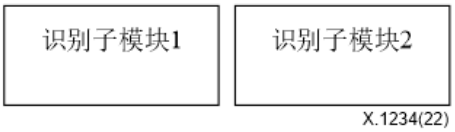
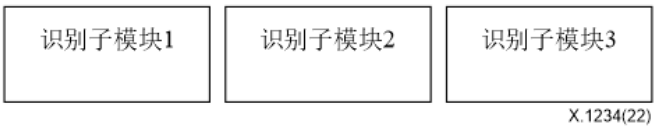
8.3.4 识别模块

识别模块的功能包括：

- 分析MMS是否是垃圾信息；
- 向核实模块发送识别结果。

根据MMS的不同部分，主要有三种识别技术。第一种是基于电话号码的，比如黑名单和白名单。第二种是基于文本的，比如文本识别。最后一种是基于附件的，如图像识别、视频识别等。根据服务提供商的具体要求和特点，识别模块可根据技术种类部署不同的子模块。

表 8-1 – 识别模块配置模型

模型	描述
模型0	 模型0只有一个子模块，且只有一种识别技术。
模型1	 模型1是子模块1的形状，和子模块2一起配置。子模块1和子模块2是三种类型中的任意两种。
模型2	 模型2是子模块1的形状，子模块2和子模块3一起配置。

在模型1和模型2中，识别结果可能有不同的计算方式。例如，在模型1中，识别子模块1部署文本识别，识别子模块2则部署图像识别。识别子模块1将MMS识别为垃圾信息，但识别子模块2不将同一条MMS识别为垃圾信息。因此，是否将一个MMS识别为垃圾信息需要识别模块制定整体策略。建议根据实际需要和情况配置策略。

8.3.5 核实模块

验证模块的功能包括：

- 从识别模块接收可能的结果；
- 做出进一步的判断，如人工确定。

8.3.6 处置模块

数据处置模块的功能包括：

- 从核实模块接收结果；
- 根据识别结果对MMS进行处置，能够判断MMS是否为垃圾信息；
- 如果MMS被识别为垃圾信息，则将处置结果发送至系统管理模块；
- 如果MMS不被识别为垃圾信息，则将原始MMS发送至MMSC。

8.3.7 系统管理模块

系统管理模块的功能包括：

- 保存操作日志和系统日志；
- 更新数据库；
- 接收用户的反馈。

8.4 参考模型

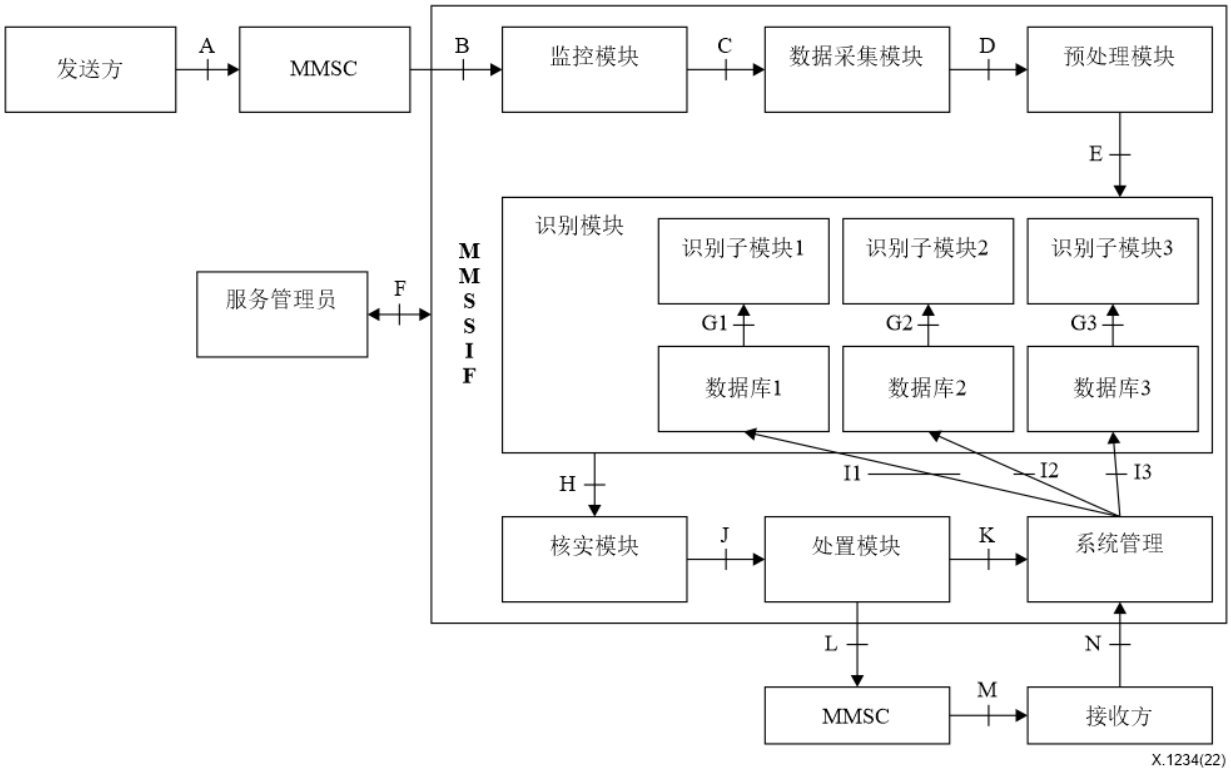


图 8-3 – 打击MMS垃圾信息的参考模型

接口A是发送方与MMSC之间的接口。接口A用于向MMSC传送MMS。当服务提供商开始向用户提供MMS服务时它即已意识到，所以在该模型中它不需要改变。

接口B是MMSC与监控器模块之间的接口。接口B是一个新的接口，用于向监控模块发送MMS，而不是直接转发至接收方或下一个MMSC。

接口C是监控模块与数据采集模块之间的接口。接口C用于传送MMS的字头、发送方电话号码、URL等，这些均由监控模块进行分析。

接口D是数据采集与预处理模块之间的接口。接口D用于传送所有信息，包括MMS的字头、MMS的正文、主题、所有附件等。

接口E是预处理模块与识别模块之间的接口。接口E用于传送规范化信息，如“来源+信息类型+信息”。接口E应该支持FTP和HTTP。

接口F是服务运营商与MMSSIF之间的接口。接口F用于传送配置规则和垃圾信息统计数据。

接口G是数据库与子模块之间的接口。接口G不是特定的接口，它代表一类不同数据库与其对应的识别子模块之间的接口。接口G用于传送可疑号码、文本、图像等（在数据库中进行匹配），以识别垃圾信息。

接口H是识别模块与核实模块之间的接口。接口H用于传送可能的结果和原始MMS。

接口I是系统管理与数据库之间的接口。接口I不是特定的接口，如同接口G一样，它代表一类不同数据库与系统管理之间的接口。

接口J是核实模块与处置模块之间的接口。接口J用于传送识别结果和原始MMS。

接口K是处置模块与系统管理之间的接口。接口K用于传送发送方电话号码、识别结果、处理情况和原始MMS。

接口L是处置模块与MMSC之间的接口。接口L用于传送未被识别为垃圾信息的原始MMS。

接口M是MMSC与接收方之间的接口。接口M用于向接收方发送MMS。当服务提供商开始向用户提供MMS服务时它即已意识到，且在这种模型下它不需要改变。

接口N是接收方与系统管理之间的接口。接口N用于传送接收方的反馈。

9 工作程序

图9-1显示，打击MMS垃圾信息包含十二个程序。这些程序构成了自适应系统，有助于优化系统性能。

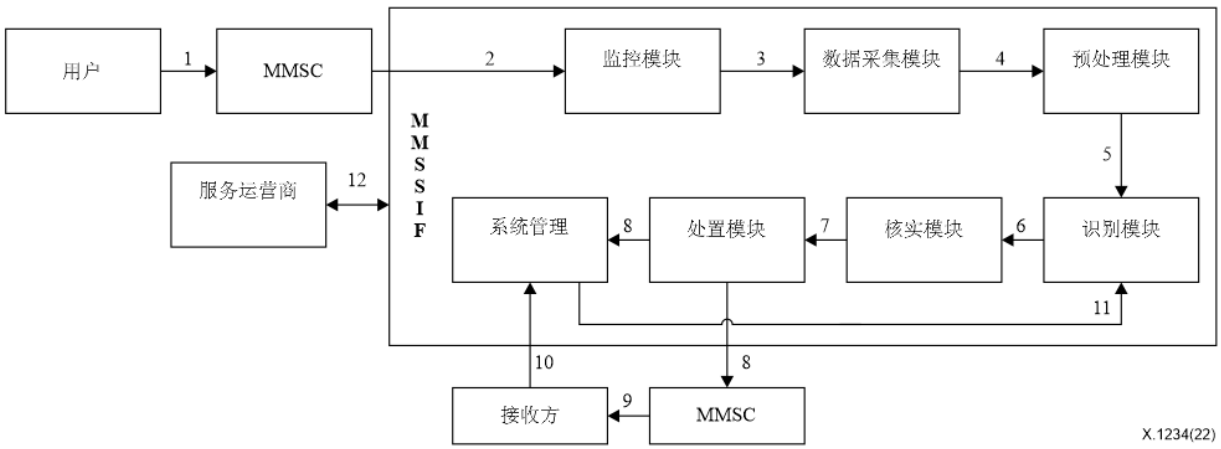


图 9-1 打击MMS垃圾信息的处理程序

程序1：向MMSC发送MMS

发送方准备MMS内容、接收方电话号码，然后将该MMS发送至MMSC。

程序2：MMS前转至监控模块

MMSC从MMSC收到MMS信息，然后直接将其前转至监控模块。

程序3：获得MMS的字头

监控模块会一直监控MMSC是否有新的MMS发送。一旦有了新的MMS，它将接收MMS的完整数据流，分析数据流并获得MMS的字头，包括主题、发送方电话号码、附件数量、这些附件的URL，然后监控模块将所有的信息发送至数据采集模块。

程序4：下载所有附件

数据采集模块将接收来自监控模块的信息，找到附件的URL，并下载所有附件。数据采集模块收到MMS的所有信息后，会将其发送至预处理模块。

程序5：将MMS信息规范化

预处理模块在接收到来自数据采集模块的信息后，将检查所有附件，并判断它们是文本、图像、音频还是视频。如果所有信息都是合法的，则预处理模块将根据不同类型对信息进行分类，并按照规则对信息进行规范化。之后它会将原始MMS、所有规范化信息和发送方电话号码发送至识别模块。

程序6：分析MMS

识别模块将根据实际系统中部署的不同技术，分析MMS是否为垃圾信息，然后识别模块将可能结果发送至核实模块。识别模块需要若干整体策略来获得最终的可能结果，一些特定技术除外。

程序7：做出进一步判断

核实模块将在接收到来自识别模块的可能结果后做出进一步判断，并将识别结果发送给处置模块。

程序8：处置MMS

处置模块将根据识别结果处置MMS。如果MMS被识别为垃圾信息，则处置模块将按照一套规则处置MMS，如拦截MMS、向垃圾信息发送者发送提醒信息等。它还将向系统管理模块发送原始MMS、处置日志和发送方电话号码。接收方将不会收到此MMS。如果MMS未被识别为垃圾信息，则处置模块会将原始MMS发送至MMSC。

程序9：将MMS发送至接收方

MMSC将把此MMS发送给接收方。有时，它会将MMS发送至另一MMSC，然后发送至接收方。如没有MMSSIF功能，此此程序与之前相同。

程序10：接收方的反馈

接收方可能是垃圾向信息的受害者，因此他们可能会主动向服务管理模块发送一些反馈。接收方的参与将有助于有效和高效地打击垃圾信息，因此，建议系统管理模块在开发打击垃圾信息的解决方案或策略时使用接收方反馈功能。

程序11：更新数据库

系统管理模块将保存操作日志、系统日志和原始MMS。它还将根据新样本、电话号码、关键词等更新数据库。

程序12：调整应对措施

根据来自MMSSIF的垃圾信息统计数据和分析报告，服务运营商将评估MMSSIF的性能，以寻求可能的改进。基于评估结果，服务运营商可调整措施和策略，并且可以调整识别模块中的协作机制。

10 有关关键技术的导则

MMS可以传送各种多媒体信息，包括图像、文本、视频、音频等，因此，打击MMS垃圾信息的关键识别技术主要包括图像识别、文本识别、视频识别、音频识别等。

10.1 垃圾信息过滤列表

垃圾信息过滤列表包括黑名单、白名单和不明确列表。服务提供商应配置MMSSIF来记录可疑活动，或作为可选方案将其自动配置为黑名单或白名单（如，拦截可疑MMS，允许正常MMS通过）。服务提供商还应充实完善该列表，以保持MMSSIF随时可用且稳定工作。当发现诸如未列出的电话号码等异常情况时，应手动审查该电话号码，以进行全面评估。

10.2 图像识别

图像识别首先提取图像表示的特征，建立图像特征值数据库。然后，垃圾信息的检测被转化为特征空间中的二元分类问题，且可以通过传统的机器学习得到解决。或者更简单地说，如果MMS的图像特征值在数据库中匹配，则该信息被识别为垃圾信息。该方法取决于图像特征值数据库的质量。

10.3 文本识别

文本识别主要包括关键词识别和语义识别。关键词识别首先建立关键词数据库。如果MMS信息的文本内容中包含关键词数据库中匹配的任何关键字，则该信息被识别为垃圾信息。此外，文本识别可建立布尔逻辑模型和向量空间模型，经过训练，可得到识别模型，后者可提高文本识别的准确性。这种方法取决于关键词数据库的质量。

有时，垃圾信息发送者在避免被发现方面极具创造力。例如，垃圾信息发送者可伪造普通电子邮件并将其内容随机化，以避免垃圾信息过滤器功能的关键词检测。因此，基于关键词识别，利用语义识别实现二次识别（如基于模糊语义识别的自然语言处理方法）是非常有效和高效的，可以大大降低误报率。

10.4 视频识别

视频识别一般先建立样本数据库，然后将MMS视频与视频样本逐一进行比较，从而判断视频是否为垃圾信息。它还可以通过提取视频的关键帧来进行识别。主要操作如下：对视频进行解码，将其处理为一组图像，然后从这些图像中进行采样，并基于图像识别技术对采样图像进行识别，最后利用这些采样图像的综合分析结果得到视频识别结果。

10.5 音频识别

音频识别可结合自动语音识别（ASR）技术实现。ASR技术的目标是使计算机能够“口授”不同人连续的讲话或关键词或句子的表达，并能够将“声音”转换为“文本”。此外，为了识别相似或相同的音频数据，要提取频谱特征（spectral features），并计算得出了一个短而强健的音频指纹。因此，ASR能够从音频中“识别”某些特定的关键词，从而确定音频是否是垃圾信息。

10.6 最终用户的反馈

来自最终用户的反馈，应适用相关实施指南和[ITU-T X.1231]第8.5节和[ITU-T X.1247]的附件A规定的其他信息。

一些最终用户在收到垃圾MMS时会直接予以删除，很少有最终用户会通过官方客户端反馈机制举报MMS垃圾信息。这种方法的有效性取决于最终用户的积极性和主动性。我们鼓励最终用户积极参与，以有效和高效率地打击MMS垃圾信息。

参考文献

[b-ITU-T X.1240] Recommendation ITU-T X.1240 (2008), *Technologies involved in countering e-mail spam.*

[b-ITU-T X.1241] Recommendation ITU-T X.1241 (2008), *Technical framework for countering email spam.*

[b-ITU-T X.1242] Recommendation ITU-T X.1242 (2009), *Short message service (SMS) spam filtering system based on user-specified rules.*

[b-ITU-T X.1245] Recommendation ITU-T X.1245 (2010), *Framework for countering spam in IP-based multimedia applications.*

[b-ITU-T X.1246] Recommendation ITU-T X.1246 (2015), *Technologies involved in countering voice spam in telecommunication organizations*.

ITU-T 建议书系列

系列 A	ITU-T 工作的组织
系列 D	资费及结算原则和国际电信/ICT 的经济和政策问题
系列 E	综合网络运行、电话业务、业务运行和人为因素
系列 F	非话电信业务
系列 G	传输系统和媒介、数字系统和网络
系列 H	视听及多媒体系统
系列 I	综合业务数字网
系列 J	有线网络和电视、声音节目及其他多媒体信号的传输
系列 K	干扰的防护
系列 L	环境与 ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
系列 M	电信管理，包括 TMN 和网络维护
系列 N	维护：国际声音节目和电视传输电路
系列 O	测量设备的技术规范
系列 P	电话传输质量、电话设施及本地线路网络
系列 Q	交换和信令，以及相关联的测量和测试
系列 R	电报传输
系列 S	电报业务终端设备
系列 T	远程信息处理业务的终端设备
系列 U	电报交换
系列 V	电话网上的数据通信
系列 X	**数据网、开放系统通信和安全性**
系列 Y	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
系列 Z	用于电信系统的语言和一般软件问题

瑞士印刷
2022年，日内瓦