

国际电信联盟

ITU-T

国际电信联盟
电信标准化部门

X.1242

(02/2009)

X系列：数据网、开放系统通信和安全性
网络安全 – 反垃圾信息

基于用户指定规则的短消息业务（SMS）
垃圾过滤系统

ITU-T X.1242建议书

ITU-T



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
报文处理系统	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
生物测定安全	X.1080–X.1099
安全应用和服务	
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	X.1140–X.1149
安全协议	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	
计算网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1339

欲了解更详细信息，请查阅 *ITU-T* 建议书目录。

ITU-T X.1242建议书

基于用户指定规则的短消息业务（SMS） 垃圾过滤系统

摘要

ITU-T X.1242建议书描述基于用户指定规则的短消息业务（SMS）垃圾信息过滤系统的实现。它定义了短消息业务（SMS）垃圾信息过滤系统的结构、垃圾短消息过滤功能、用户的服务管理、通信协议和具备SMS功能终端的基本功能要求。

来源

ITU-T第17研究组（2009-2012年）按照世界电信标准化全会（WTSA）第1号决议规定的程序，于2009年2月20日批准了ITU-T X.1242建议书。

关键词

过滤系统、SMS、垃圾短消息、基于用户指定规则的垃圾短消息过滤系统。

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ITU-T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”等其他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他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网址查询电信标准化局（TSB）的专利数据库：<http://www.itu.int/ITU-T/ipr/>。

© 国际电联 2009

版权所有。未经国际电联事先书面许可，不得以任何手段复制本出版物的任何部分。

目录

页码

1	范围	1
2	参考文献	1
3	定义	1
3.1	其他资料规定的术语	1
3.2	本建议书规定的术语	2
4	缩写词和首字母缩略语	2
5	惯例	3
6	系统描述	3
7	系统结构	3
7.1	总体结构	3
7.2	模块要求	4
7.3	设备要求	6
8	垃圾短消息过滤功能	6
8.1	短消息业务工作模式	6
8.2	垃圾短消息过滤要求	7
9	用户服务管理	9
9.1	管理方法	9
9.2	管理能力	11
10	通信协议	12
10.1	通信协议的结构	12
10.2	认证协议	13
10.3	ISMG 协议	13
附录一	对支持垃圾短消息过滤的终端软件的要求	14
I.1	一般问题	14
I.2	垃圾短消息过滤基本软件	14
I.3	垃圾短消息过滤增强软件	15
参考资料	16

引言

随着移动服务的越来越普及，短消息业务以其低廉的价格、良好的灵活性和方便的使用方法已经成为最有收益的增值服务之一，但是，与此同时，垃圾短消息也正在迅速增加，并带来下列严重影响：

- 降低用户对短消息业务的满足度
- 浪费网络资源
- 增加了社会不安定因素
- 带来其他负面影响

因此，当前至关重要的是，寻找到一种有效和高效率的解决方案阻止垃圾短消息，同时维持短消息系统的运营效率。应该考虑到下列各项原则：

- 对用户SMS接口的变动减到最小
- 增加用户对SMS业务的信心
- 易于实施和部署
- 对现有的网络系统的变动减到最小

根据上述原则，基于用户指定规则的短消息业务（SMS）垃圾过滤系统是阻止垃圾短消息的一种有效和高效率的方法。这意味着，建立一个垃圾短消息过滤系统，其中用户可以管理短消息过滤规则，并委托系统所属的服务提供商或网络运营商阻止相关的短消息。

该系统有下列优点：

- 通过用户指定规则保护用户隐私不受侵犯
- 满足用户阻止垃圾短消息的要求
- 在没有改变现有的网络系统情况下容易实现
- 作为一项可以为服务提供商带来收益的增值业务运营

本建议书适用于在移动网络和固定网络中，对基于用户指定规则的垃圾短消息过滤系统进行设计、部署和评估。

基于用户指定规则的短消息业务（SMS） 垃圾过滤系统

1 范围

本建议书描述基于用户指定规则的短消息业务（SMS）垃圾过滤系统（以下简称垃圾短消息过滤系统或过滤系统）的实现。本建议书规定：

- 过滤系统的结构
- 垃圾短消息过滤功能
- 用户的服务管理
- 通信协议
- 终端的功能要求

本建议书适用于在移动网络和固定网络中，基于用户指定规则的垃圾短消息过滤系统的设计、部署和评估。

注 – 本建议书中描述的某些过滤机制可能会影响到电信业务的隐私。因此，实施短消息业务（SMS）垃圾信息过滤系统需要考虑遵守可适用的法规。由于德国的法规另有规定，本建议书或其一部分不适用于德国。

2 参考文献

下列ITU-T建议书和其他参考文献的条款，通过在本建议书中的引用而构成本建议书的条款。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都面临修订，使用本建议书的各方应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ITU-T建议书清单定期出版。

本建议书中引用某个独立文件，并非确定该文件具备建议书的地位。

[ETSI TR 101 632] ETSI TR 101 632 V7.0.0 (2000-06)，《数字蜂窝通信系统（阶段 2+）（GSM）；把短消息业务中心（SMSC）连接到短消息实体（SME）的接口协议》点到点业务（PP）的技术实现》（GSM 03.39 版本7.0.0，1998年发布）。
<<http://pda.etsi.org/exchangefolder/tr-101632v070000p.pdf>>

3 定义

3.1 其他资料规定的术语

本建议书采用其他资料规定的术语：

3.1.1 mobile station (MS) 移动台：能够通过一个或多个无线电接口接入一组UMTS业务的实体。该实体在接入UMTS业务的UMTS服务区内可以是固定的或移动的，并可以同时服务一个或多个用户。[b-ETSI TR 125 990]。

3.1.2 short message 短消息：通过SMSC从发送方用户到接收方用户传送的信息。[b-ETSI TS 102 507]。

3.1.3 short message entity 短消息实体: 该实体组成和分解短消息。SME可以或可以不设置于, 并不能区别于HLR, MC, VLR, MS或MSC。[b-ITU-T Q.1742.3]。

3.1.4 short message service centre (SMSC) 短消息业务中心: 一种功能单元, 负责在两个SM-TE或SME和MS之间中继并存储转发短消息(SM)。网络中SM-SC在功能上可以分开或合并。[b-ETSI ES 201 986]。

3.1.5 SMS-DELIVER: 短消息发送协议数据单元, 包括从SC发送至MS的用户数据(短消息)。[b-ETSI TS 100 901]。

3.1.6 SMS-STATUS-REPORT: 短消息发送协议数据单元通知接收MS, 关于由MS先前发送的移动始发的短消息的状态, 即, 无论是否SC能够转发此消息, 或无论消息被存储在SC中待发送。[b-ETSI TS 100 901]。

3.1.7 SMS-SUBMIT: 短消息发送协议数据单元, 包括从MS发送至SC的用户数据(短消息)。[b-ETSI TS 100 901]。

3.1.8 status report 状态报告: SC通知始发MS, 关于向SME发送的短消息的结果。[b-ETSI TS 100 901]

3.2 本建议书规定的术语

本建议书规定下列术语:

3.2.1 Internet short message gateway (ISMG) 互联网短消息网关: SP和SMSC之间的实体, 实现从SP到SMSC和从SMSC到SP传输短消息, 同时实现SP和SMSC之间交互信息的协议转换。

3.2.2 short message service (SMS) 短消息业务: 电信网络中的业务, 提供手机、电话及其他SME通过SMSC(如果接收端不能接通时的存储消息)发送和接收文本消息。

3.2.3 spam 垃圾信息: 通过终端如计算机、移动电话、电话等由发送方向接收方发送的电子信息, 该信息对接收方来说通常是未经请求、不需要和有害的。

3.2.4 SMS spam SMS垃圾信息: 通过SMS发送的垃圾信息。

4 缩写词和首字母缩略语

本建议书采用下列缩写词和首字母缩略语:

FMD	被过滤的消息数据库
ISMG	互联网短消息网关
MS	移动台
SC	业务中心
SCM	服务控制模块
SM MO	点到点移动始发短消息
SM MT	点到点移动终接短消息
SME	短消息实体
SMPP	短消息点到点
SMS	短消息业务

SMSC	短消息业务中心
SP	服务提供商
SS	秘书台
SSFMM	垃圾短消息过滤模块
SSFS	垃圾短消息过滤业务
URD	用户指定规则数据库
USMM	用户服务管理模块

5 惯例

无。

6 系统描述

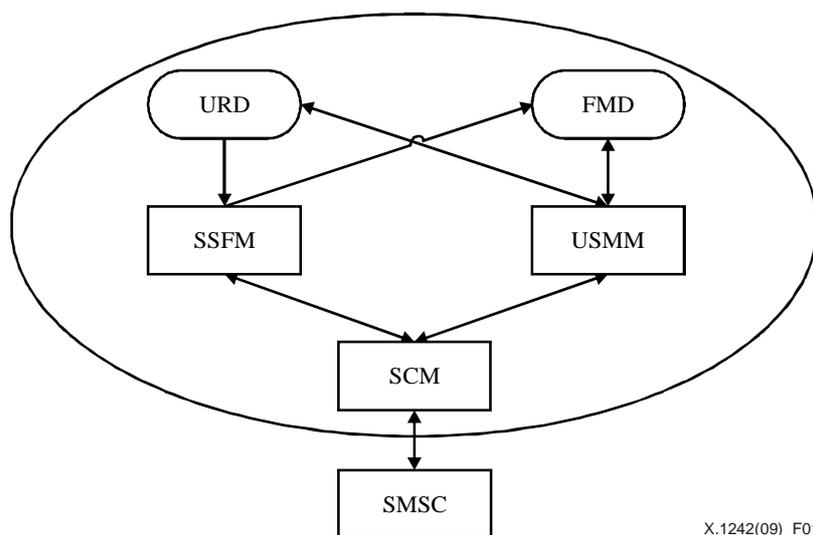
基于用户指定规则的垃圾短消息过滤系统指附加于SMSC的过滤系统，其中用户可以配置（新增、删除和编辑）过滤规则，同时发往该用户的所有短消息可以根据那些过滤规则进行过滤。另外，用户可以采用特定的方法管理（查询、删除和恢复）被过滤的短消息。

过滤规则可以基于地址（电话号码）、时间、内容等。此外，特定的过滤规则可以单独使用或与其他过滤规则相结合使用。如果过滤规则与其他过滤规则相结合使用，在规定规则时设置各过滤规则的优先次序是必要的步骤之一。为了此项服务的使用方便和实用，至少为用户提供下列管理方法之一：SMS、网络和秘书台。

7 系统结构

7.1 总体结构

垃圾短消息过滤系统包括下列逻辑模块：服务控制模块（SCM）、垃圾短消息过滤模块（SSFMM）、用户服务管理模块（USMM）、用户指定规则数据库（URD）和被过滤的消息数据库（FMD）。垃圾短消息过滤系统的结构如图 1 所示：



X.1242(09)_F01

图 1 – 垃圾短消息过滤系统的结构

根据位置，图1中的5个模块可以分为3层：接入层、业务层和数据层。接入层包括SCM；业务层包括USMM和SSFM；数据层包括URD和FMD。

7.2 模块要求

7.2.1 接入层

接入层，直接连接SMSC的外层，主要负责接入到过滤系统的外部实体（包括用户）。

7.2.1.1 服务控制模块（SCM）

SCM是过滤系统的综合业务管理平台，包括下列功能：

- 服务订购查询：垃圾短消息过滤为一项用户任选业务。因此，在SCM中，任何短消息在发送前都可以被查询，以确定接收方是否具有垃圾短消息过滤业务服务订购。如具有，则短消息将发送到SSFM继续执行下列的过滤处理；否则，短消息将通过正常过程（不过滤）发送。
- 管理指导的发送：短消息包括业务管理指导（业务状态、过滤规则和被过滤的短消息的管理）应被确认并从SCM发送到USMM。

SCM 为一种相对独立的模块，可以与其他增值业务组合而形成一个综合的业务平台以便于实施和部署。实际上，SCM 通常具有计算功能。

7.2.2 业务层

业务层实现过滤系统的核心功能：垃圾短消息过滤、过滤规则管理和被过滤的短消息管理。实际上，业务层至少包括2个模块：垃圾短消息过滤模块（SSFM）和用户服务管理模块（USMM）。SSFM实现垃圾短消息过滤，USMM实现过滤规则管理和被过滤的短消息管理。

7.2.2.1 垃圾短消息过滤模块 (SSFM)

SSFM, 过滤系统的核心单元, 处理来自SCM的过滤请求, 根据存储在用户指定规则数据库 (URD) 中的过滤规则, 确定短消息是否为垃圾消息, 然后用结果回复SMSC。如果短消息是垃圾, 则将其存储在被过滤的消息数据库 (FMD) 中等待进一步管理 (查询、删除和恢复); 否则, 短消息将正常发送到接收方。

另外, 本模块中应考虑到SCM、URD、FMD和SSFM间的接口协议。

SSFM和SCM之间的接口协议: SSFM接收认证消息包括从SCM始发的短消息并以认证结果回复SCM。

SSFM和URD之间的接口协议: SSFM获得来自URD的用户特定过滤规则。

SSFM和FMD之间的接口协议: 如果被确定为垃圾信息, 则SSFM在FMD中存储被过滤的短消息。

7.2.2.2 用户服务管理模块 (USMM)

用户使用USMM来管理过滤规则和被过滤的短消息。通过USMM, 用户可以新增、删除、修改和查询过滤规则。与此同时, 通过USMM, 用户可以查询、删除和恢复被过滤的短消息。USMM应至少支持下列管理方法之一: SMS管理方法; 网络管理方法和SS管理方法。

另外, 本模块中应考虑到SCM、URD、FMD和USMM之间的接口协议。

USMM和SCM之间的接口协议: 通过SCM, USMM接收来自用户的短消息, 包括过滤规则和被过滤的短消息的管理指导, 并且将结果回复给用户。

USMM和URD之间的接口协议: USMM发送管理指导 (新增、删除、修改或查询过滤规则) 到URD并获得来自URD的相关信息。

USMM和FMD之间的接口协议: USMM发送管理指导 (恢复、删除或查询被过滤的短消息) 到FMD获得来自FMD的相关信息。

7.2.3 数据层

数据层主要负责存储过滤规则和被过滤的短消息。这些数据应以数据库格式或文本格式存储到永久媒质中, 如磁盘、磁带等。此外, 数据可以被发送和删除。当数据文件的尺寸超过存储限制时, 过滤系统应立即提醒运营商, 但自动备份数据。

7.2.3.1 被过滤的消息数据库 (FMD)

FMD用于存储被SSFM作为垃圾过滤掉的短消息。存储时间可以由用户规定。如果对存储时间没有明确的规定, 被过滤的短消息应至少保存3个月。

应考虑从FMD到SSFM和USMM的接口协议。

7.2.3.2 用户指定规则数据库（URD）

URD用于存储用户特定过滤规则。用户特定过滤规则可以基于地址、时间和内容。基于地址的黑名单是强制性的，基于地址的白名单则为可选的。

应考虑从URD到SSF和USMM的接口协议。

7.3 设备要求

SCM, SSFM, USMM, FMD和URD为过滤系统的全部逻辑模块。它们不仅可以作为独立的设备使用，也可以组合为一个设备或几个设备使用。对于大规模的短消息业务中心（SMSC），推荐第一种形式以完善性能和扩展能力。此外，作为一个完整的系统，系统管理功能和日志审查功能都是非常重要的。

8 垃圾短消息过滤功能

8.1 短消息服务工作模式

短消息点到点业务包括下列两种基本业务：

- SM MT（点到点移动终接短消息）；
- SM MO（点到点移动始发短消息）。

SM MT表示从SMSC到接收方MS发送短消息的能力，并通过传递报告或具有稍后发送特定机制的失败报告，提供关于短消息的传递信息，参见图2。

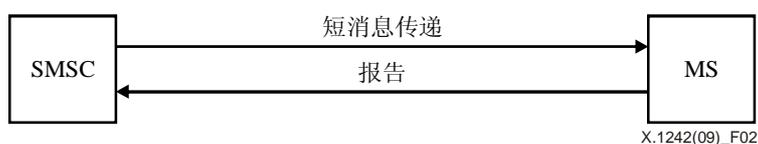


图2 – 移动终接的短消息业务，点到点业务

SM MO表示从发送方MS到SME经由SMSC发送短消息的能力，并通过传递报告或失败报告提供关于短消息的传递信息。该消息必须包括SMSC将最终要将短消息转发到的SME的地址；参见图3。

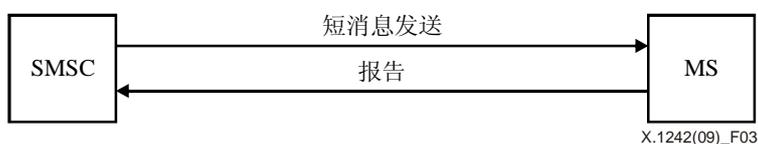


图3 – 移动始发的短消息业务，点到点业务

但是，在SM MO之后，SMS传递到接收方MS可以通过2种模式实现。第一种模式，在SM MO后，直接将短消息传递到接收方MS。第二种模式中，在SM MO后，通过通信机制将短消息发送到接收方的SMSC（即，通过在IP网络中实施SMPP协议），再传递到接收方MS。虽然采用不同的工作模式用户对SMS工作的感觉相同，但两种模式过滤系统的实施过程差别巨大。为了简便起见，第一种工作模式称为发送侧传递，第二种工作方式称为接收侧传递。

8.2 垃圾短消息过滤的实现

垃圾短消息过滤是一种接收方订购业务，可向接收方提供配置用户特定过滤规则的能力和在被过滤短消息的能力。用户特定过滤规则和被过滤短消息通常存储于接收侧的URD和FMD中。

在接收侧传递模式中，过滤规则管理、被过滤的短消息管理和短消息传递均在接收侧实现。因此，在接收侧传递模式实现的过滤系统将较容易，因为只有设置在接收侧的设备需要修改。

在发送侧传递模式中，短消息传递在发送侧的SMSC中实现，同时过滤规则和被过滤的短消息的管理在接收侧URD和FMD中实现。因此发送和接收侧垃圾短消息过滤系统之间需要同步机制。通常，在过滤过程之前，短消息将发送到接收侧的过滤系统。一般而言，由于该同步机制，发送侧传递模式的过滤系统的实现比接收侧传递模式困难。

8.2.1 接收侧传递模式中实现垃圾短消息过滤

在接收侧传递模式中，在接收侧部署的SCM、SSFm和USMM没有发送侧设备或模块参与；参见图4。

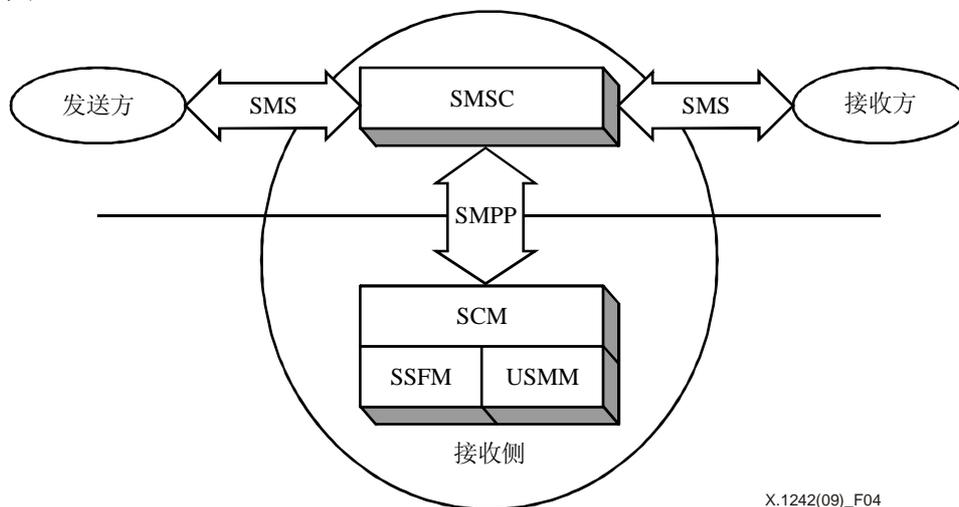


图 4 – 接收侧传递模式中的垃圾短消息过滤

工作过程示于图 5：

- 在收到发送方的短消息后，SMSC将向SCM发送包括始发短消息的SMPP认证；
- SCM将查询接收短消息的业务订购。如果接收方具有业务订购，短消息将发送到SSFm；否则，短消息将正常发送；

- **SSF**M将根据接收方过滤规则检查是否短消息有效。如是短消息合法，过滤系统应将短消息传递到接收方并以成功**SMPP**响应回复**SMSC**。如果短消息无效，垃圾短消息过滤系统应阻止短消息并将其存储在**FMD**待进一步管理（询问、删除和恢复）。

由于同时需要处理的**SMS**的数量可能很大，并且过滤过程可能需要很长时间，因此，在**SMSC**中设置一个定时器是必要的，以防止**SMS**的丢失和延迟。如果**SMSC**在定时器规定的时间内不能收到**SMPP**响应，短消息将正常发送。通常，网络运营商或服务提供商设置定时器。

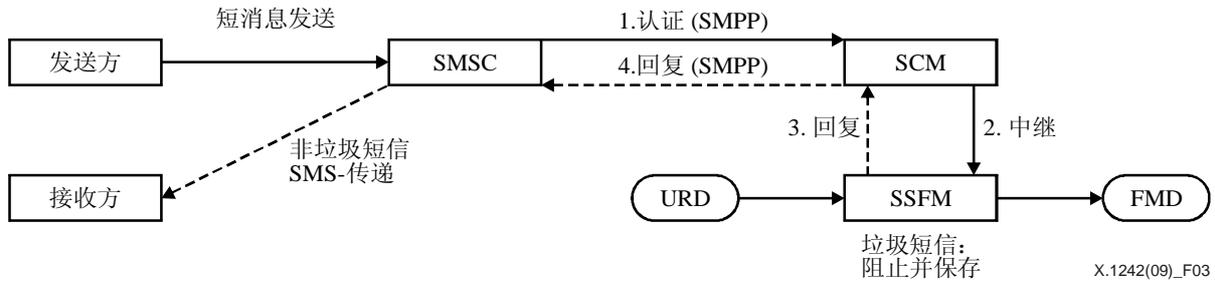


图 5 – 接收侧传递模式中的垃圾短消息过滤系统的过程

8.2.2 发送侧传递模式中实现垃圾短消息过滤

在发送侧传递模式中，**SCM**、**SSF**M和**USMM**只部署在发送侧，短消息的传递也在发送侧实现。因此，应考虑发送侧和接收侧垃圾短消息过滤系统之间的一些同步机制。通常，短消息将发送到接收侧的过滤系统以继续下述过滤过程；参见图6。

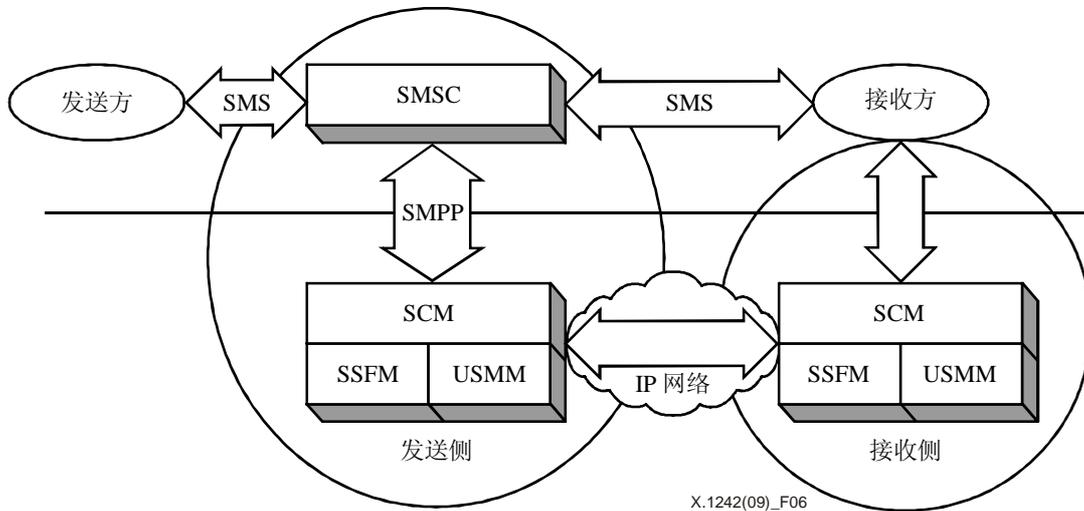


图 6 – 发送侧传递模式中的垃圾短消息过滤

工作过程如图7所示：

- 在接收源自发送方的短消息后，SMSC将发送SMPP认证，该认证包括到发送侧SCM的始发短消息；
- 发送侧的SCM将询问接收短消息业务订购状态。如果接收方具有业务订购，短消息将发送到发送侧的SSFM；否则，短消息将正常发送给接收方；
- 发送侧的SSFM将发送短消息到接收侧的SSFM。接收侧的SSFM将根据存储在URD的接收方过滤规则确定短消息是否有效，如果短消息合法，过滤系统将短消息传递到接收方，并以成功SMPP响应回复SMSC；如果短消息不合法，垃圾短消息过滤系统将阻止短消息并将其存储在接收侧的FMD中待进一步询问。

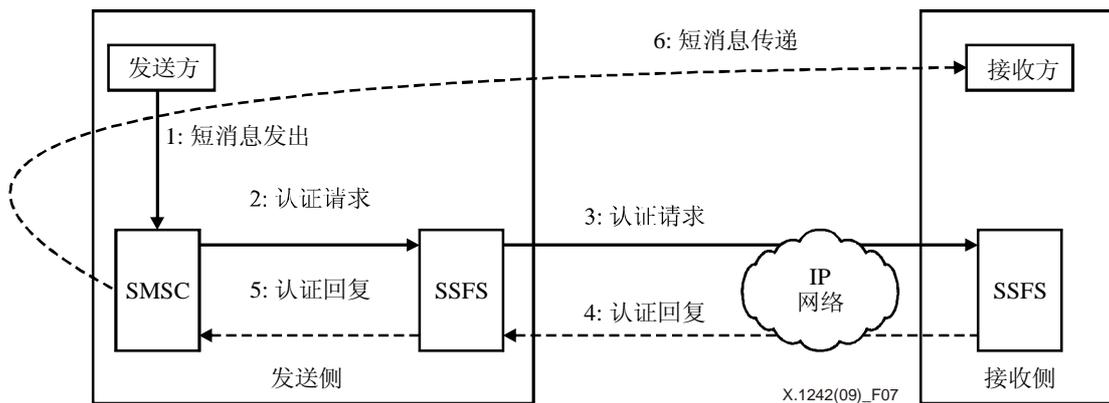


图 7 – 发送侧传递模式中的垃圾短消息过滤过程

由于同时需要处理的SMS的数量可能很大，并且过滤过程可能需要很长时间，因此，有必要在SMSC中设置一个定时器，以防止SMS的丢失和延迟。如果SMSC在定时器规定的时间内不能收到SMPP响应，短消息将正常发送。通常，网络运营商服务提供商设置定时器。

9 用户服务管理

9.1 管理方法

垃圾短消息过滤系统应为用户提供SMS管理方法和网络管理方法。此外，还可根据实际的网络环境提供秘书台管理方法，例如，是否有足够的训练有素的人员可以做此项工作。

9.1.1 短消息管理方法

用户可以管理用户特定过滤规则和被SMS通过附加到USMM的短消息实体（SME）过滤的短消息，如服务提供商（SP）。

一方面，SME 可以接收并识别包括管理指示的 SMS；另一方面，SME 可以发送管理指示到 USMM，并且 USMM 可以根据来自用户的管理指示管理用户特定过滤规则和被过滤的短消息。示于图 8：

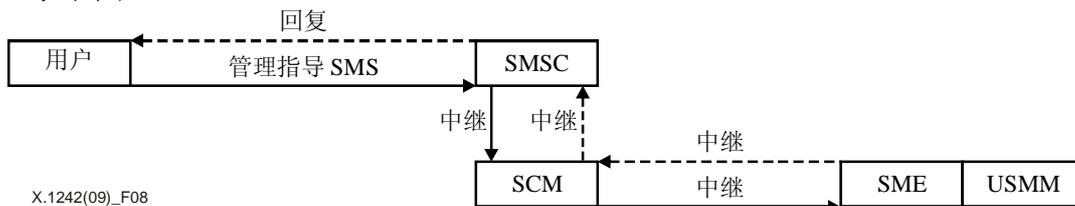


图 8 – 通过短消息管理

如果用户希望管理用户特定过滤规则和被过滤的短消息，用户需要做的工作只有发送 SMS，包括管理指示到一个 SME 的具体接入号码。SME 应完成的任务如下。

短消息的大小非常有限（通常最大 160 个字符）不可能包括足够的信息。此外，大多数 SMS 终端为通常体积较小的移动电话。通过键盘输入数据并且在其屏幕观看大量数据也非常困难，因为屏幕尺寸本身也很有限。因此，在 SMS 终端上管理过滤规则和被过滤的短消息有难度。但是，由于 SMS 终端通常被用户携带，允许用户也采用该终端来管理用户特定过滤规则和被过滤的短消息，并发送和接收短消息是有优势的。

9.1.2 网络管理方法

用户可以通过网络，采用附加到 USMM 上的网络服务器管理用户特定过滤规则和被过滤的短消息。

一方面，网络服务器可以接收管理指示；另一方面，网络服务器可将管理指示发送到 USMM，并且 USMM 可以根据管理指示管理用户特定过滤规则和被过滤的短消息。如图 9 所示：

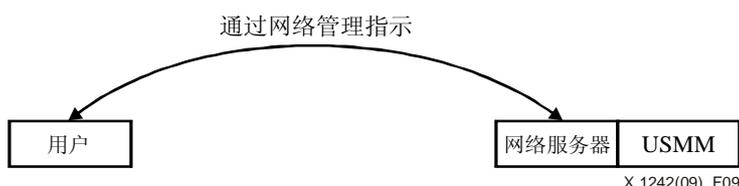


图 9 – 通过网络管理

网络管理方法的操作过程与正常的网络操作相类似，但是网络管理方法可以比短消息管理方法支持更多的管理指导。考虑到安全问题，网络管理方法应支持 SSL/TLS 以鉴别网络服务器和客户，然后使用它将被鉴别的各方之间的消息加密。事实上，采用网络管理方法比 SMS 管理方法更有效。但是它只限于互联网接入点。

9.2 管理能力

9.2.1 用户特定过滤规则的类型

由于过滤系统的工作基于用户特定过滤规则；因此，过滤规则对过滤系统来说非常重要。实际上，过滤规则可以基于地址、时间和内容。

- 基于地址的过滤规则

基于地址的过滤规则确定短消息是否为垃圾的依据是基于其源地址（电话号码）。基于地址的过滤规则有两种：可接受发送方的白名单和疑似垃圾发送方的黑名单。实际上，源自白名单的所有短消息将不再进行判断正常发送；源自黑名单的短消息将立即阻止。白名单/黑名单的项目可以不仅为独立的电话号码，还可以是电话号码分段。然而，白名单/黑名单，特别是黑名单将不可避免地包含技术错误，称为假肯定问题和假否定问题。然而，基于地址的过滤方法对阻止垃圾短消息最为方便有效。因此，尽管白名单/黑名单方法是过于激烈的解决方案，对大多数用户不能接受，但基于地址的过滤方法仍是过滤系统中最为重要的过滤规则。

- 基于时间的过滤规则

基于时间的过滤规则在规定的时间内限制传递短消息，因此被阻止在FMD中的短消息可能不是垃圾。通常情况下，用户不希望在夜里、或会议中或某些主要的时间接收短消息，因此他们可以使用基于时间的过滤规则。在基于时间的过滤规则中，用户可以规定其不希望接收短消息的时间范围。然而，用户可以选择，在该时间范围后，对按照基于时间的过滤规则被阻止的短消息的进一步处理方式：重发或不再重发。

- 基于内容的过滤规则

基于内容的过滤方法是最为合理的过滤方法。但是，由于基于内容的过滤方法采用的语言处理面临着难题，基于内容的过滤方法的正确性较其他的过滤方法低。事实上，基于关键词的过滤方法是基于内容的过滤方法中最为常用的过滤方法。在过滤系统中，基于关键词过滤规则为强制性的。与此同时，过滤系统应支持下列匹配方法用于基于关键词过滤规则：精确匹配和模糊匹配。

- 联合过滤规则

事实上，过滤规则通常是联合使用的。因此，过滤规则的优先次序就应认真考虑。实际上，优先次序由业务运营商和用户的实际需求的基本规则决定。

9.2.2 用户特定过滤规则的管理

用户可执行以下管理过滤规则：

- 加载和卸载由业务运营商制定的预先定义的过滤规则：

为了简化用户对过滤规则的操作过程，业务运营商应建立或引用公认的黑名单。因此，用户可以使用此类预先定义的过滤规则。

- 管理基于地址、时间和内容的过滤规则：
用户可以新增、修改、删除和查询过滤规则。但是不同的管理方法中，用户的经验会不同。在SMS管理方法中，用户只使用一种管理指导的一种短消息来管理过滤规则，操作上通常有困难；而在网络管理方法中，用户可以非常容易地管理过滤规则。

9.2.3 被过滤的短消息的格式

所有被过滤的短消息都应存储在FMD中，并备有详细的记录。记录应该至少包括以下几个方面：

- 发送方：发送方的电话号码
- 接收方：接收方的电话号码
- 时间：短消息发送时间
- 内容：短消息内容
- 过滤方法类型：基于地址、基于关键词、基于时间

9.2.4 被过滤的短消息的管理

用户可以管理被过滤的短消息。用户可以进行如下操作：

- 对被过滤的短消息进行统计
- 查看被过滤的短消息详细内容
- 查询被过滤的短消息
- 恢复被过滤的短消息
- 删除指定的被过滤的短消息

10 通信协议

10.1 通信协议的结构

在过滤系统中有8种协议接口：（最后一种用于发送侧传递模式中的过滤系统）：

- SMSC和SCM之间的接口
- SCM和SSFMM之间的接口
- SCM和USMM之间的接口
- SSFMM和URD之间的接口
- SSFMM和FMD之间的接口
- USMM和URD之间的接口
- USMM和FMD之间的接口
- 发送侧和接收侧SSFMM之间的接口

前3种接口协议为外部接口，主要用于相同网络或不同网络中不同模块之间的互连。后5种接口协议为内部接口，并且可以根据服务提供商的实际要求开发，对于外部来说通常是无形的。

通常，SMPP、认证协议可以用于SMSC和SCM之间。ISMG协议可以用于SCM和SSFMM以及SCM和USMM之间。

另外，SMS互连也应考虑到。

10.2 认证协议

认证协议应基于扩展的SMPP（参见[ETSI TR 101 632]）。垃圾短消息过滤系统中采用两种消息：DELIVER_SM和DELIVER_SM_RESP。工作过程示于图 10。

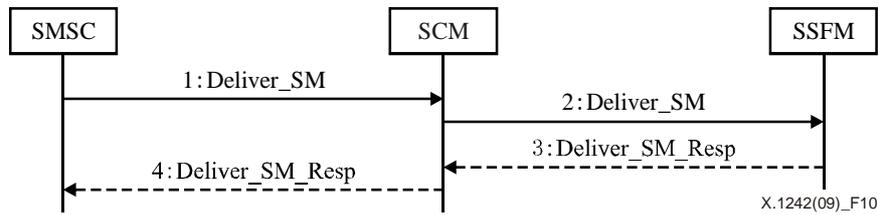


图 10 – SMPP 认证协议

DELIVER_SM由SMSC或SCM发布。采用此命令，SMSC或SCM可以将短消息发送到SCM或SSFM。

DELIVER_SM_RESP作为DELIVER_SM的响应发布，注意，不管发送是否成功。DELIVER_SM_RESP中的状态值表示不同的含义：0代表成功传递；其他值表示传递失败。

10.3 ISMG协议

用户可以使用ISMG协议配置用户特定过滤规则并管理被过滤的短消息。短消息实体（SME）附加到用户服务管理模块（USMM）中，用户借此可以管理过滤规则和被过滤的短消息（存储于FMD中）。SMS网关协议在SMSC和SME之间使用。工作过程如图 11所示。

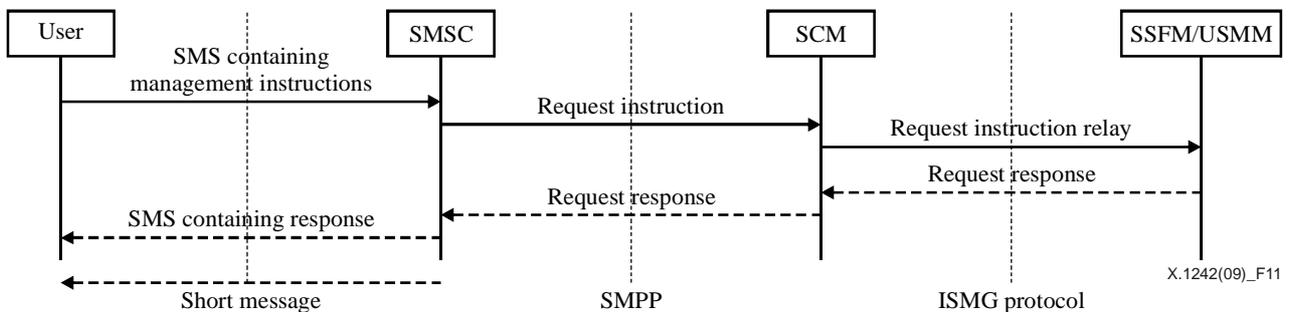


图 11 – ISMG 协议

附录一

对支持垃圾短消息过滤的终端软件的要求

(本附录不是本建议书的组成部分)

本附录适用于智能终端。

I.1 一般问题

几乎所有的SMS终端为移动电话，通常体积很小，特别是屏幕空间有限，键盘很小。因此，用户通过文本命令管理过滤规则和被过滤的短消息非常困难。为便于管理，开发了基于智能终端的支持垃圾短消息过滤的终端软件。一般情况下，该软件为用户提供了操作菜单，其中管理指导与菜单项目相对应。然而，终端软件还应满足下列2项基本要求：

- 全面管理过滤规则和被过滤的短消息
- 适用于用户操作的友好和方便的人机界面

实际上，终端软件有两种类型：

- 垃圾短消息过滤基本软件：

过滤功能在与 SMSC相连接的垃圾短消息过滤系统中实现。终端软件只为用户提供人机界面。

- 垃圾短消息过滤增强软件：

终端软件具有全部垃圾短消息过滤系统的功能模块，可独立地过滤垃圾短消息。通常，增强软件包括基本软件的全部功能。

I.2 垃圾短消息过滤基本软件

I.2.1 过滤规则的配置

应提供下列操作功能，参见表 I.1。

表 I.1 – 过滤规则管理

预先定义的过滤规则	加载预先定义的过滤规则
	卸载预先定义的过滤规则
基于地址的过滤规则	增加白名单项目
	删除白名单项目
	增加黑名单项目
	删除黑名单项目
	询问基于地址的过滤规则
基于关键词的过滤规则	增加关键词
	删除关键词
	询问基于关键词的过滤规则
基于时间的过滤规则	增加时间规则
	删除时间规则
	询问基于时间的过滤规则

表 I.1 – 过滤规则管理
询问所有的过滤规则
删除所有用户特定的过滤规则
开始和停止垃圾短消息过滤

I.2.2 过滤规则配置

表 I.2 – 被过滤的短消息管理

对被过滤的短消息进行统计
查看被过滤的短消息详细内容
查询被过滤的短消息
恢复被过滤的短消息
删除指定的被过滤的短消息

I.3 垃圾短消息过滤增强软件

如果智能终端具有足够的资源（即处理能力、存储空间等），所有的功能模块均可以在智能终端安装和实施。在此情况下，安装在智能终端的软件通常称为SMS防火墙。但是，智能终端仍然需要接入互联网以便对软件和预先定义的过滤规则进行更新。

参考资料

- [b-ITU-T Q.1742.3] ITU-T Q.1742.3建议书（2004年），《由ANSI-41演进的采用cdma2000接入网的核心网的IMT-2000参考资料》（批准日期截至2003年6月30日）。
- [b-ETSI TS 100 901] ETSI TS 100 901 V7.5.0（2001-12），《数字蜂窝通信系统（阶段2+）；短消息业务（SMS）点到点业务（PP）的技术实现》（3GPP TS 03.40 版本 7.5.0，1998年发布）。
http://pda.etsi.org/exchangefolder/ts_100901v070500p.pdf
- [b-ETSI TS 102 507] ETSI TS 102 507 V1.1.1（2006-03），《高级联网电信和互联网会聚业务和协议（TISPAN）；用于IP网络的固定网络短消息业务（F-SMS）；业务描述》。http://pda.etsi.org/exchangefolder/ts_102507v010101p.pdf
- [b-ETSI TR 125 990] ETSI TR 125 990 V3.0.0（2000-01），《通用移动通信系统（UMTS）；词汇》。http://pda.etsi.org/exchangefolder/tr_125990v030000p.pdf
- [b-ETSI ES 201 986] ETSI ES 201 986 V1.1.2（2002-01），《高级网络的业务和协议（SPAN）；PSTN/ISDN的短消息业务（SMS）；业务描述》。
http://pda.etsi.org/exchangefolder/es_201986v010102p.pdf

ITU-T 系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	视听及多媒体系统
I系列	综合业务数字网
J系列	有线网络和电视、声音节目及其他多媒体信号的传输
K系列	干扰的防护
L系列	电缆和外部设备其他组件的结构、安装和保护
M系列	电信管理，包括TMN和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备的技术规范
P系列	电话传输质量、电话设施及本地线路网络
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	数据网、开放系统通信和安全性
Y系列	全球信息基础设施、互联网协议问题和下一代网络
Z系列	电信系统使用的语言和一般性软件情况