国 际 电 信 联 盟

ITU-T X.1247

(03/2016)

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 – 反垃圾信息

打击手机垃圾短信的技术框架

ITU-T X.1247 建议书

国际电信联盟

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	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
PITV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
PKI相关建议书	X.1340–X.1349
网络安全信息交换	
网络安全综述	X.1500–X.1519
脆弱性/状态信息交换	X.1520–X.1539
事件/事故/探索法信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
探索法和信息要求	X.1560–X.1569
标示和发现	X.1570–X.1579
确保交换	X.1580–X.1589
云计算安全	
云计算安全综述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳实践和指导原则	X.1640–X.1659
云计算安全实现	X.1660–X.1679
其他云计算安全	X.1680–X.1699

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1247 建议书

打击手机垃圾短信的技术框架

摘要

随着手机短信业务的快速发展，手机垃圾短信正在迅速扩散。不幸的是，没有一种措施可作为打击手机垃圾短信的万能良药。因此，有必要为打击手机垃圾短信建立一个实用框架。ITU-T X.1247建议书概要介绍了打击手机垃圾短信的程序，为打击手机垃圾短信提出了一种技术框架。此框架具体介绍了有关实体功能和处理程序。此外，本建议书就单个打击垃圾短信域内及各打击垃圾短信域之间共享信息的机制做了介绍。

历史沿革

版本	建议书	批准日期	研究组	唯一ID*
1.0	ITU-T X.1247	2016-03-23	17	11.1002/1000/12600

关键词

打击垃圾信息、手机垃圾短信、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/。

目录

页码

1 范围 1
2 参考文献 1
3 定义 1
3.1 在其他地方定义的术语 1
3.2 本建议书中定义的术语 1
4 缩写词和首字母缩略语 2
5 惯例 3
6 打击手机垃圾短信概况 3
7 打击手机垃圾短信功能的结构 4
7.1 总体结构 5
7.2 参考模型 6
7.3 各构成成份的功能 7
8 打击手机垃圾短信的技术 8
8.1 用户反馈机制 8
8.2 蜜罐 8
8.3 MNO的识别方法 8
8.4 更多强化机制 9
9 各打击垃圾信息域之间的关系 9
10 手机垃圾短信的处理 11
参考资料 14

引言

包括短信服务和多媒体信息服务的移动信息由于价格低廉、高度灵活和便于使用而在迅速发展。然而，手机垃圾短信正在干扰着消费者的日常生活，并带来诸多负面影响。

仅使用于一种解决方案难以有效缓解手机垃圾信息。如果通力合作，利用多种打击垃圾信息技术打击手机垃圾短信，则可以大大减少手机垃圾短信带来的危害。此外，考虑到手机垃圾短信在全世界广为扩散，因此，在多个打击垃圾信息领域开展合作可能会大大降低成本并提高效率。有鉴于此，有必要建立能够满足各种解决方案需求并支持协作机制的开放框架。该框架应与多数打击垃圾信息技术相兼容，不应仅限于特定技术细节。该框架所涉程序须得到移动装置最终用户的明确同意并须符合国家相关法律法规。

ITU-T X.1247 建议书

打击手机垃圾短信的技术框架

1 范围

本建议书提供打击手机垃圾短信的技术框架。在该框架中，具体规定了实体功能和处理程序。该框架所涉程序须得到手机装置最终用户的明确同意并须符合国家相关法律法规。此外，本建议书就单个打击垃圾短信域内及各打击垃圾短信域之间的信息共享机制做了说明。

本建议书适用于短信服务（SMS）和多媒体信息服务（MMS）。

2 参考文献

无。

3 定义

3.1 在其他地方定义的术语

本建议书使用以下在其他地方定义的术语：

3.1.1 垃圾短信（SMS spam）[b-ITU-T X.1242]：通过短信发送的垃圾信息。

3.1.2 垃圾信息（spam）[b-ITU-T X.1240]：“垃圾信息”一词的含义取决于各国根据其国家技术、经济、社会和实际情况对隐私和垃圾信息构成的看法。值得一提的是，随着技术的发展，其含义不断变化并拓宽，为滥用电子通信创造了新的可乘之机。尽管在全球范围内没有有关垃圾信息的一致定义，但该术语一般用来描述为推销商业化产品或服务通过电子邮件或移动信息批量传送的推介性电子通信。

3.1.3 垃圾信息制造者（spammer）[b-ITU-T X.1240]：制造并发送垃圾信息的实体或个人。

3.2 本建议书中定义的术语

本建议书定义了下列术语：

3.2.1 打击垃圾信息域（anti-spam domain）：一个独立系统，包括打击垃圾信息管理功能、打击垃圾信息监测功能、打击垃圾信息处理功能和移动信息客户机。

注 – 打击垃圾信息域内的功能须服从运营商的统一管理。

3.2.2 打击垃圾信息过滤实体（anti-spam filtering entity）：应用打击垃圾信息措施的设备或系统，根据过滤规则对手机信息进行过滤。它可以阻止垃圾信息、将信息标为可疑信息或向接收方发送信息。

3.2.3 打击垃圾信息管理功能（anti-spam management functions）：一组用于管理和监督打击垃圾短信域的功能，包括与其它打击垃圾信息域通信，以共享有关垃圾信息的信息、通过对垃圾信息分析产生新的过滤规则并将规则提供给打击垃圾信息处理功能。

3.2.4 打击垃圾信息监测功能（anti-spam monitoring functions）：用以监测和分析打击垃圾信息处理域过滤结果的一组功能，包括证实蜜罐捕获的可疑垃圾信息、分析垃圾信息数据、产生垃圾信息统计数据和垃圾信息分析结果。

3.2.5 打击垃圾信息处理功能（anti-spam processing functions）：通过过滤规则和政策处理手机信息的一组功能，方法是阻止垃圾信息、发送专门标记或向接收方发送信息。

3.2.6 错误否定（false negative）：过滤系统错误地将手机垃圾短信作为非垃圾短信予以处理。

3.2.7 错误肯定（false positive）：过滤系统将信息错误地确认为垃圾信息。

3.2.8 过滤规则（filtering rules）：打击垃圾信息过滤实体采用的一套消除算法（countering algorithms）规则，如黑名单/白名单、相似度门限值和统计门限值。过滤规则也可以包含用户规定的过滤规则。

3.2.9 手机信息客户（mobile messaging client）：手机信息服务签约用户。

3.2.10 手机垃圾短信（mobile messaging spam）：通过手机信息服务进行的推介性电子通信，通常包括短信（SMS）垃圾信息和多媒体（MMS）垃圾信息。

3.2.11 多媒体垃圾信息（multimedia message spam (MMS) spam）：通过MMS发送的垃圾信息。

3.2.12 报告服务（reporting service）：在用户许可情况下，按照国家相关法律法规收集和汇总签约用户有关垃圾信息报告的服务。

3.2.13 垃圾信息分析报告（spam analysis report）：得到分析的结果代表过滤系统的性能，应包括过滤的错误否定/错误肯定发生率、垃圾信息特性、垃圾信息的趋势及其它分析。

3.2.14 垃圾信息统计数据（spam statistics）：得到汇总的垃圾信息数据代表在特定限制条件下垃圾信息发生的程度，如在打击垃圾信息域的一段时间内。它应包括相关域中或进入及离开该域的信息量、不同类型的垃圾信息的比例、垃圾信息制造者清单及其它有关垃圾信息的统计数据。

3.2.15 可疑垃圾信息（suspicious spam）：被怀疑是垃圾信息的、未得到确定的手机短信。

3.2.16 用户报告（user report）：收到手机垃圾短信签约用户的投诉。一般来说，这一报告可包括收到垃圾信息的时间、发送方和接收方的移动签约用户国际综合业务数字网/公众交换电话网（ISDN/PSTN）号码（MSISDN）等。该报告还包含被错误标记为手机垃圾信息或应被标为垃圾信息而未被加以标注的信息情况，即，错误肯定、错误否定。

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：

AO 始发应用

AMgmt 打击手机垃圾短信管理功能

AMon 打击手机垃圾短信监测功能

APr 打击手机垃圾短信处理功能

GGSN 关口站GPRS支持节点

GPRS 通用分组无线业务

HPLMN 归属公众陆地移动网络

HTTP	超级文本传送协议
ISDN	综合业务数字网
MAP	移动应用部分
MMS	多媒体信息服务
MMSC	多媒体信息服务中心
MNO	移动网络运营商
MO	面向手机
MSC	移动交换中心
MSISDN	移动签约用户国际ISDN/PSTN号码
MT	移动终接
PSTN	公众交换电话网
SMPP	短信对等
SMS	短信服务
SMSC	短信服务中心
UICC	通用集成电路卡
VPLMN	受访公众陆地移动网
WAP	无线应用协议

5 惯例

无。

6 打击手机垃圾短信概况

如同图6-1所示，多数情况下可以通过两种方法制造短信（SMS）垃圾信息，一种方法是垃圾信息制造者利用垃圾信息工具发送大宗信息 – 利用众多获得的或复制的通用集成电路卡（UICC）发送正常点对点短信。另一种方法是垃圾信息制造者利用服务提供商提供的大综信息发送服务制造垃圾短信 – 利用运营商的短信关口站接口。由于运营商没有有效的关口站接口技术和管理监督机制，因此，很容易被垃圾信息制造者利用。

根据信息前转方向，垃圾信息制造者可通过两种程序制造垃圾短信，即，面向手机（MO）/面向应用（AO）的程序和移动终接（MT）程序。在MO程序中，通过垃圾信息工具产生的垃圾信息经发送方网络的相关实体发送至短信服务中心（MSC）。在AO程序中，通过运营商短信关口站注入垃圾信息中的短信被前转至SMSC，之后，SMSC对服务接收方的移动交换中心（MSC）发出询问并向其前转该信息。最终短信通过访问MSC网络前转至接收方，该程序称作MT程序。

经签约用户许可并按照相关行政规定，移动网络运营商（MNO）有权通过过滤实体减缓垃圾短信。打击垃圾信息程序须严格遵守适用的法律条款，以避免侵犯签约用户的隐私。

目前得到广泛认可的做法是在MO/AO程序或在MT程序或在二者中部署打击垃圾信息过滤实体。如果在MO程序中进行垃圾信息过滤，则打击垃圾信息过滤实体从SMSC那里收集短信。为了在接收方网络中有效过滤垃圾信息，还需要在MSC与打击垃圾信息过滤实体之间进行通信。

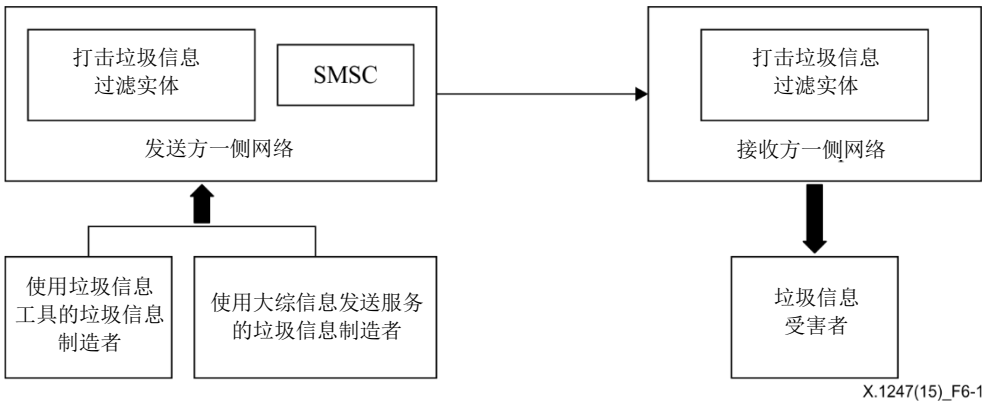

图6-1 – 移动网络中的垃圾短信

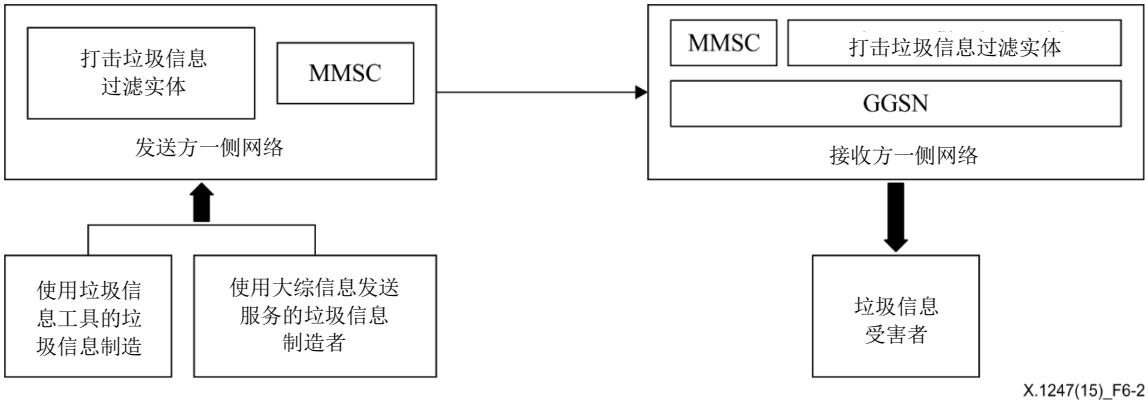

图6-2 – 移动网中的多媒体垃圾信息

如图6-2所示，多媒体信息服务（MMS）的信息程序与短信信息程序类似，唯一的不同是由关口站GPRS支持节点（GGSN）取代了SMSC，SMSC由多媒体信息服务中心（MMSC）取代。MMS信息被前转至接收方网络的MMSC，之后，SMSC将信息发至接收方，然后，接收方从MMSC那里下载MMS短信。由于这一原因，可在MMSC相邻处部署MMS打击垃圾信息过滤实体，这意味着，在发送方一侧或接收方一侧部署过滤实体不会有任何差别。

7 打击手机垃圾短信功能的结构

打击手机垃圾短信的结构包括打击手机垃圾短信管理功能（AMgmt）、打击手机垃圾短信监测功能（AMon）、打击手机垃圾短信处理功能（APr）和手机信息客户机。这些功能共同确定了打击手机垃圾短信域。

建议将不同打击手机垃圾短信域相互关联，它们可根据相关协议确定的规则或政策相互协调。

这些功能可通过现有信息协议相互通信，其特性描述如下。

7.1 总体结构

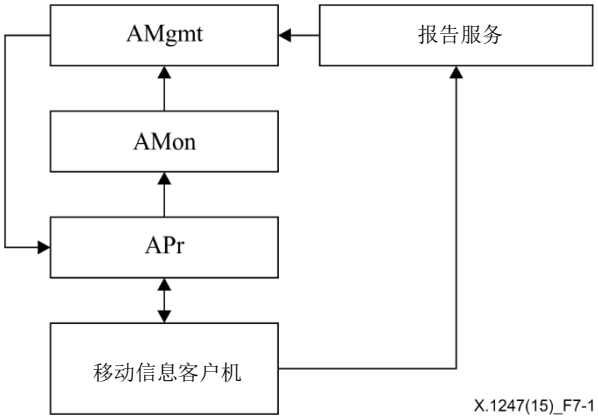

图7-1 – 总体结构

AMgmt从Amon那里收到垃圾信息统计数据并在其域中更新过滤规则。AMgmt还与报告服务中心和其它AMgmt共享有关垃圾信息的信息。

AMon从APr那里收到可疑手机垃圾短信（通过蜜罐或类似平台获得）并证实这些信息是垃圾信息。AMon还在对垃圾信息数据进行汇总和分析后向AMgmt发送垃圾信息分析和垃圾信息统计数据报告。

APr将规则用于手机短信，之后，在用户许可下，按照不同政策和过滤结果，将信息标为垃圾信息予以发送或进行阻止。APr从AMgmt那里接收过滤规则并从手机短信客户机那里得到用户反馈。建议在APr上部署诸如蜜罐等平台以收集可疑垃圾信息。

手机短信客户机通过发送用户反馈为打击手机垃圾短信做出贡献（向APr发送信息，表明收到的手机短信被错误地标为垃圾信息，并向报告服务中心提供垃圾信息报告）。

报告服务的目的是经用户许可并根据国内相关法律法规，收集和汇总签约用户的垃圾信息报告。它有助于在打击垃圾信息域之间共享用户报告的数据。报告服务可由监管部门、安全公司或MNO等运营。各域之间的协议有助于打击手机垃圾短信域共享量身定制的有关垃圾信息的信息。

7.2 参考模型

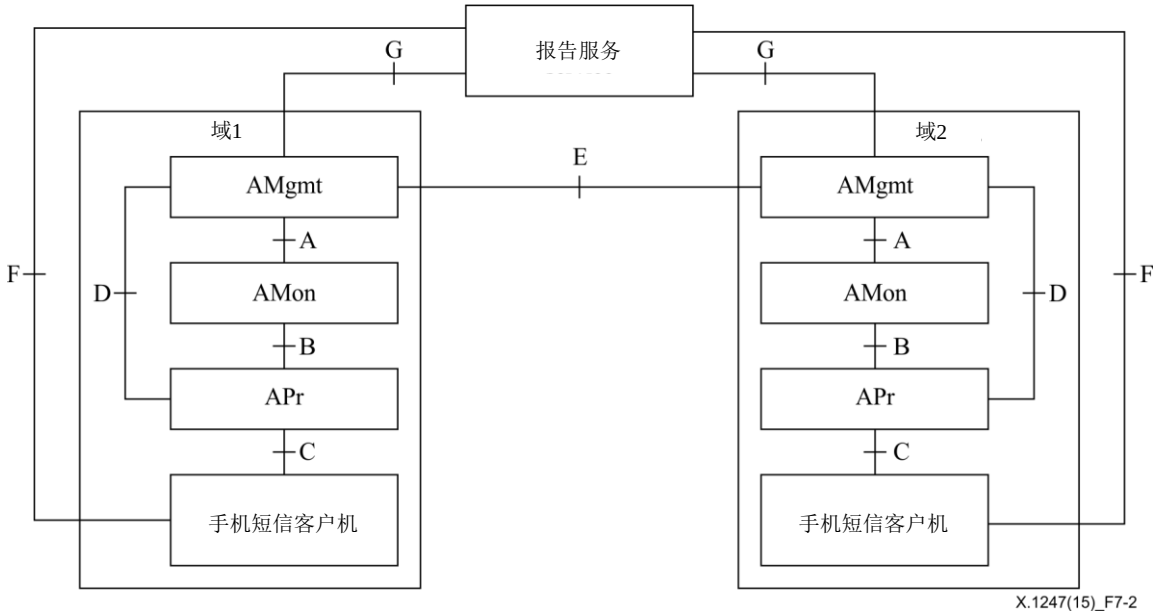

图7-2 – 参考模型

A接口是AMgmt和AMon之间的逻辑接口。A接口用来传送垃圾信息分析报告和垃圾信息统计数据。

B接口是AMon和APr之间的逻辑接口。B接口用来传送蜜罐获得的可疑垃圾信息和用户反馈 – 手机短信客户机发送的、说明其所收的信息被错误地标为垃圾信息。

C接口是APr和移动信息客户机之间的逻辑接口。C接口由手机短信客户机用来告知APr，其所收到信息被MNO错误地标为垃圾信息。此外，C接口还用来从APr向手机短信客户机发送信息。按照不同类型手机短信客户机，应在C接口上支持多种不同协议，如移动应用部分和无线应用协议（MAP/WAP）、超级文本传送协议（HTTP）和短信对等（SMPP）。

D接口是AMgmt和APr之间的逻辑接口。D接口用来传送过滤规则。

E接口是AMgmts与其它域之间的逻辑接口。E接口用来在不同打击手机垃圾短信域之间交换垃圾信息数据。

F接口是手机短信客户机与报告服务中心之间的逻辑接口。F接口由手机短信客户机用来向报告服务中心发送用户报告（须得到用户明确同意）。F接口应支持多种不同协议，如移动应用部分和无线应用协议（MAP/WAP）、超级文本传送协议（HTTP）和短信对等（SMPP）。

G接口是AMgmt与报告中心之间的逻辑接口。G接口用来从报告服务中心向AMgmt发送有关垃圾信息报告的信息。

在本参考模型中，A至D接口为域内接口，E至G接口为域间接口。

7.3 各构成成份的功能

7.3.1 手机短信客户机

手机短信客户机的功能包括：

- 提供机制，帮助用户向报告服务中心发送用户报告。
- 提供机制，帮助用户告知APr其收到的信息被错误地标为垃圾信息。
- 利用安全应用通过具体过渡规则过渡信息。

7.3.2 APr

Apr的功能包括：

- 应用源自AMgmt的打击垃圾信息规则，根据不同政策和过滤结果，选择发送、发送标为可疑的信息或阻止信息。
- 接收手机短信客户机发送的用户反馈--表明被标明垃圾信息的所收移动短信实际上并非垃圾信息。
- 通过蜜罐或其他类似平台收集可疑垃圾信息。
- 向AMon提供用户反馈以及通过蜜罐收集的可疑垃圾信息。

7.3.3 AMon

AMon的功能包括：

- 汇集从APr那里通过蜜罐收集的可疑垃圾信息以及从报告服务中心那里获得的用户报告信息。
- 证实源自APr的可疑垃圾信息。
- 分析得到汇集的垃圾信息数据，以挖掘新垃圾信息的特性。
- 向AMgmt报告垃圾信息统计数据和垃圾信息分析。

7.3.4 AMgmt

AMgmt的功能包括：

- 从AMon那里接收垃圾信息统计数据和分析报告。
- 分析从AMon那里收到的数据并产生过滤规则。
- 向APr发送过滤规则，这些过滤规则将被用于手机短信客户机。
- 与其他AMgmts进行通信，交换和共享垃圾信息数据，如垃圾信息数量、垃圾信息的来源和特性以及新的垃圾信息制造者清单等。
- 从报告服务中心那里接收有关用户报告的信息，包括最大滥用者、垃圾信息统计数据和趋势。用户报告信息可以量身订制，因此，可以在国家相关法律法规许可的范围内并根据与报告服务中心达成的协议，包含源自用户报告的一些经处理的的数据。
- 为签约用户提供制定针对用户的过渡规则的能力，并在证实其有效性后向APr发送规则。

7.3.5 报告服务中心

报告服务中心的功能包括：

- 收集用户报告并证实这些是否是垃圾信息。

- 存储和分析垃圾信息，以利用指纹代替内容来生成垃圾信息特性，以避免侵犯隐私。
- 提供用户报告数据，以便于MNO能够了解来自其他运营商的、在其网络内或进入和离开其网络的垃圾信息程度。该功能要求MNO利用这一曝光度仅针对垃圾短信采取执法行动，同时不影响用户和内容。

8 打击手机垃圾短信的技术

本节所述技术适用于上述打击垃圾信息结构并旨在提供示例。须谨慎利用这些措施，以便 符合适用的国家相关法律法规并获得用户许可。这样做的目的是为了避免侵犯签约用户的隐私。

8.1 用户反馈机制

用户反馈机制有助于用户向过滤系统表明其对垃圾信息过滤结果的意见。建议实施报告服务中心和用户反馈机制，以改善MNO的过滤结果。

报告服务中心是收集用户有关所收手机垃圾短信报告的系统，可由政府、运营商等方面设立。报告服务中心可以是服务热线、网站或垃圾短信报告中心，以便MNO能够收集垃圾短信并相应调整过滤规则。通常而言，有关所报告的垃圾短信投诉记录应包含垃圾短信散列、收到时间以及发送方的MSISDN等。根据不同政策以及只有经用户同意，MNO不仅可以阻止垃圾信息，而且还可以向接收方提供隔离（quarantine）途径。这意味着，在具体网站上，可以在做标记后发送这些信息或对其进行记录。这将有助于接收方看到这些已被标为可疑垃圾信息的“潜在垃圾信息”，从而使其有机会提出反馈（如果他们认为对于具体信息的决定是不正确的，亦或是一种“错误肯定”）。并非所有用户反馈本身都是可靠的，接收方也可能犯错，或由于其他原因而将信息报告为垃圾信息。首先需人工核实垃圾信息识别信息，然后再用来产生指纹或过滤规则。可以开发一种报告可信度分级系统，以便自动确定有效反馈或错误或恶意反馈。

8.2 蜜罐

电话号码蜜罐是作为“圈套”创建的一个账户，目的是发现、扭转或抵抗对手机短信的未经授权的使用。通常，这是一个旨在由垃圾制造者发现的账户，其中包括已停止使用或不存在的电话号码。由此，任何不同于预期的信息都可被当作可疑垃圾信息处理，且分析其内容是适当的。电话号码需要进行快速重新分配且电话号码常常被输错，因此，电话号码蜜罐将收到许多无意发出的信息和非垃圾短信信息。有必要核实这种可疑垃圾信息，以便在为了获得特性而分析可疑垃圾信息时先将这些不必要的数据过滤掉。

用户反馈可能会延误，因为在接收方报告无用信息之前，可能已过了数分钟到数天的时间。与此相反，蜜罐圈套则可以在无用信息一经发送即可对其发现。

8.3 MNO的识别方法

除用户反馈和蜜罐外，MNO可采用一些其他措施来识别垃圾信息，然后将其发送给接收方。根据不同政策，可以阻止这些信息，或在发送时以可疑进行特别标注。这些识别方法可能取决于垃圾信息的特性或发送规律。

- 发送方移动签约用户的国际综合数字业务网/公众交换电话网（ISDN/PSTN）号码（MSISDN）白名单/黑名单：

MSISDN是区分来自签约用户还是来自垃圾信息制造者的短信的最基本信息。黑名单/白名单利用发送方的MSISDN中止/接受信息。移动运营商可以阻止众所周知或人们认识的垃圾信息制造者，而签约用户可确定其自身的黑名单/白名单，以阻止或接受来自特定发送方的信息。

- 模糊辨识：

  为了躲避垃圾信息过滤，垃圾信息制造者会使用一些混淆视听手法，例如，在信息文本中随意插入一些特定字符，如“*”、“^”等等。字母由类似字符取代，如“porn（淫秽）”可能变为“p0rn”。图像可能被放大或旋转。模糊辨识的作用就是认清这种规避手段并在得到许可的情况下，对其进行过滤。

- 发送频次：

  为了快速传播垃圾信息，垃圾信息制造者可能会在短时间内向一大部分接收方发送信息。垃圾信息制造者发送其信息的速度远远超过普通发送者，因此，两个信息之间的间隔时间更短。当用户发送频次超过预先设定的门限时，该用户可被确定为高度得到怀疑的垃圾信息制造者。

- 信息发送成功率：

  垃圾短信是向未知接收方发送的，因此，垃圾信息制造者会随机选择接收方。有鉴于此，某些不存在的被叫号码的出现则变得司空见惯。垃圾信息的发送成功率远远低于普通手机短信的发送成功率。

- 发送方的呼叫记录：

  用户呼叫记录有助于运营商分析发送规律。该记录至少应包含发送方电话号码、接收方电话号码、发送时间等。如果信息发送给众多签约用户且回应或答复率极低，那么该发送方应被怀疑是垃圾信息制造者。除信息服务外，垃圾信息制造者很少使用运营商提供的其他服务（如话音呼叫）。

8.4 更多强化机制

- 针对具体用户的规则配制：

  针对具体用户的规则配制机制有助于接收方确定并向过滤系统表明不愿意收到哪类信息。通过MNO或利用接收方安装的软件，可以按照具体针对用户的规则过滤信息。

- 将路由返回至接收方归属公众陆地移动网（□PL□□）：

  对于漫游出HPLMN的客户，运营商可采用不同打击垃圾信息程序。将信息路由回HPLMN的程序是可选程序，因此，漫游接收方可能会收到未进行垃圾信息过滤的信息。有鉴于此，发送给漫游客户的信息须路由回HPLMN中的打击垃圾信息过滤实体，而非依赖访问网络。接收方HPLMN在前者到达受访公众陆地移动网（VPLMN）之前，需要利用相关打击垃圾信息措施接收并过滤信息。

9 各打击垃圾信息域之间的关系

从技术和经济角度而言，在单个打击垃圾信息域中采取打击垃圾信息措施的效果是有限的。需要在MNO之间实现互连和互通，且它们在打击垃圾信息域之间创建协作机制也必不可少。协作机制有助于提高效率并改善打击垃圾信息系统的性能。

各打击垃圾信息域之间存在两种关系，即，信任关系和不信任关系（图9-1）。不同打击垃圾信息域之间的默认关系应当是不信任关系。在这种情况下，源自不受信任对等方的所有信息都将得到过滤。在合作协议中，可以建立对等打击垃圾信息域之间的信任关系。在这后一种关系中，运营商可以根据其自身政策和过滤规则，选择不对源自信任对等方的信息进行过滤。

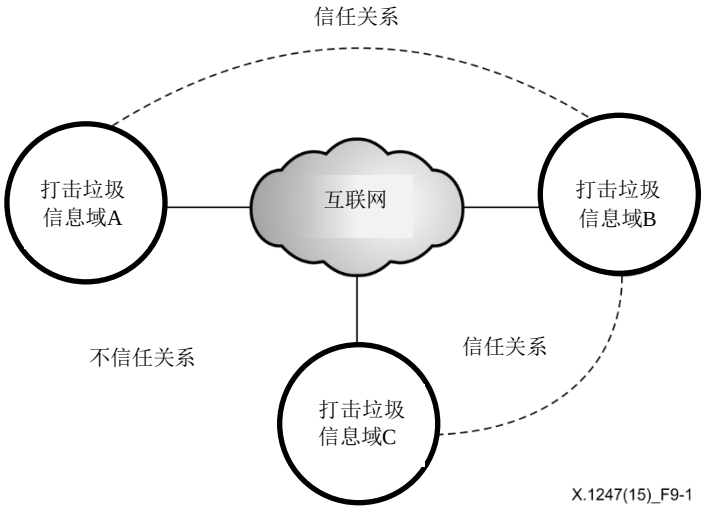

图9-1 – 信任关系与不信任关系

信任关系是非传递性的（non-transitive）。例如，如果域A信任域B且域B信任域C，那么域A可能不信任域C，除非它们之间通过直接谈判建立了任何关系。信任关系是双向的，也就是说，受信任的对等方相互平等对待。

建立信任关系后，建议采用下列协调机制。

- 垃圾信息数据共享：

  通过AMgmt连接共享某些垃圾信息数据。共享的信息包括黑名单、关键词、投诉报告和新的垃圾信息特性。在信任关系建立过程中，将调查了解该信息的意图。垃圾信息数据共享须得到移动装置用户明确无误的同意且必须符合国家相关法律法规。

- 信息源认证：

  只有在信息源得到认证时来自受信任对等方的信息才被视为是真实的。

- 免除过滤：

  源自受信任域的信息可以直接发送给接收方，以避免重复处理信息。

- 用户投诉报告和可疑垃圾信息反馈：

  如果在受信任对等方信息中收到垃圾信息报告和可疑垃圾信息，则应将其发给受信任对等方，以使其按照适用的国家相关法律法规，改进其过滤规则。

为了满足不同协调机制的要求，APr和Amon应在处理手机短信时采取不同程序。APr将决定是否对信息进行过滤。根据协议，AMon可前转/阻止信息，或向受信任对等方发送反馈。图9-2和9-3具体描述APr和AMon的操作流程。

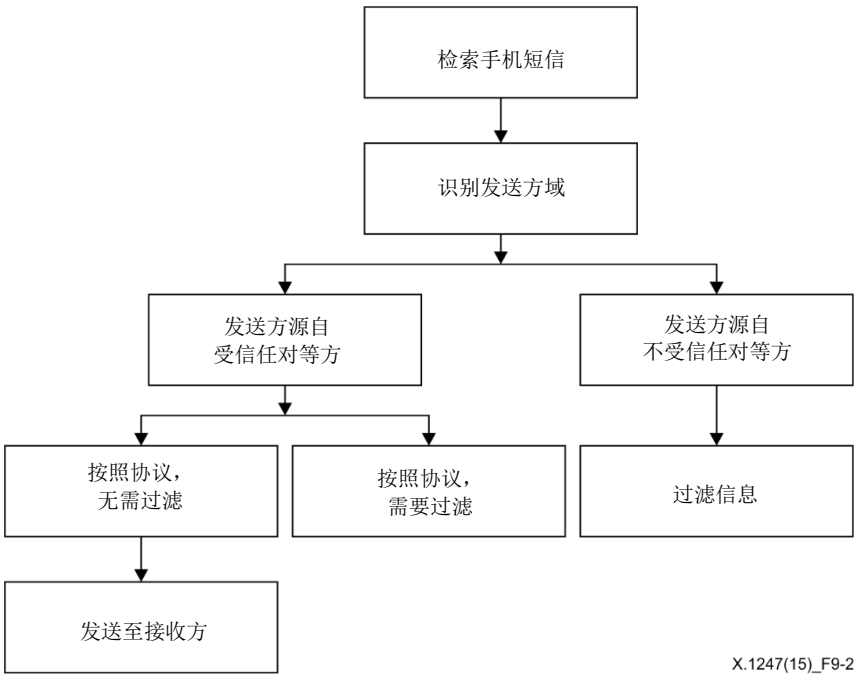

图9-2 – 在 APr 中处理手机短信的流程

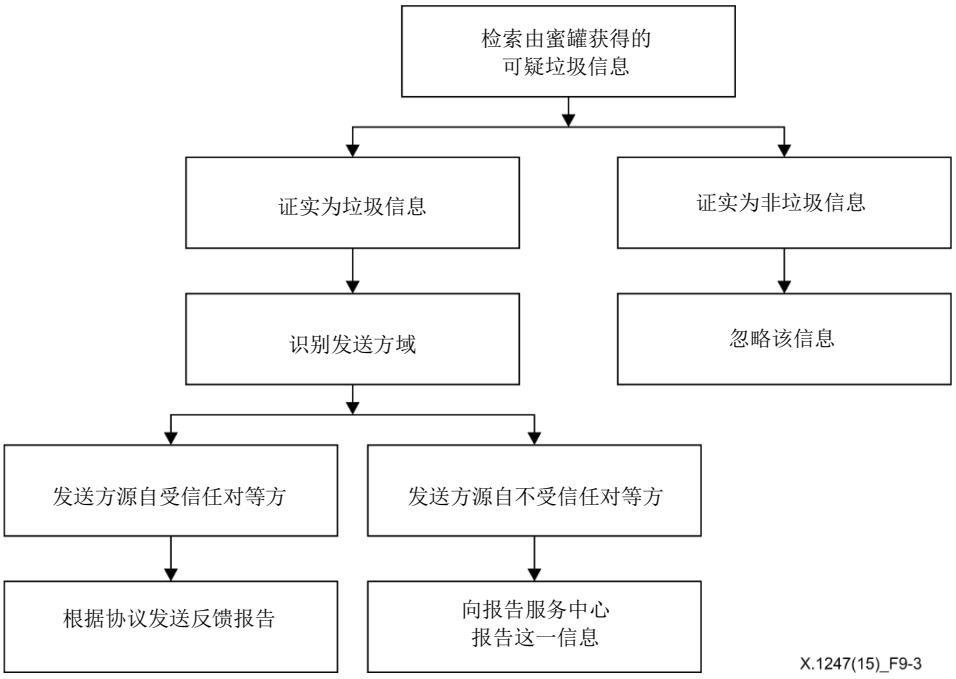

图9-3 – 在AMon中处理手机短信的流程

10 手机垃圾短信的处理

在处理手机垃圾短信流程中，应采用自适应机制，以便打击不时出现的新的垃圾信息以及新的变种。总体而言，我们可以认为，打击垃圾信息流程由图10-1所示的8个程序组成。这8个程序构成了自适应系统，有助于优化系统性能。

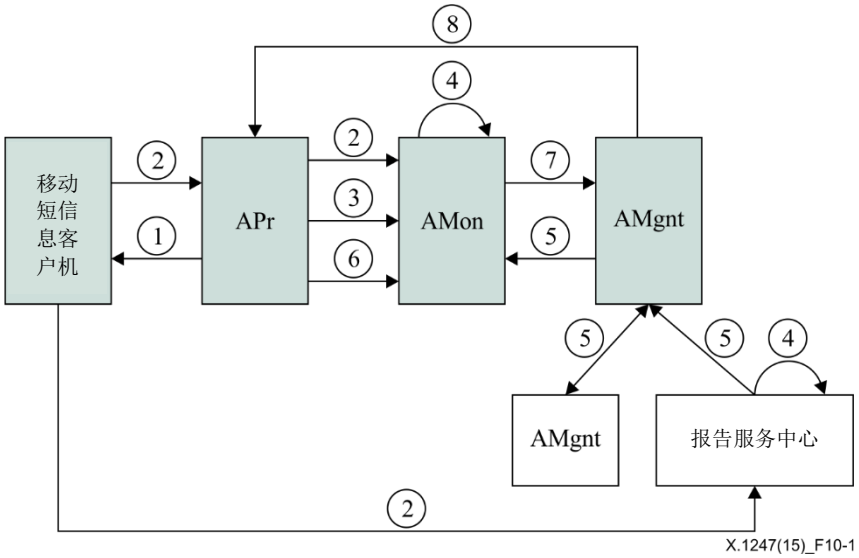

图 10-1 – 打击垃圾信息的处理程序

程序1：信息过滤

按照政策和过滤规则，Apr在将信息发送接收方前，对垃圾信息进行标注和过滤。可由运营商或用户本身量身订制这些过滤规则。

程序2：用户发送反馈

手机短信用户将用户投诉发送至报告服务中心，对未经过滤的垃圾信息予以报告并将用户反馈发至AMon，表明所收到的信息被错误地标为垃圾信息。这将有助于运营商完善其过滤规则。

程序3：前传可疑垃圾信息

APr把由蜜罐积累的可疑垃圾信息发送至AMon进行核实。

程序4：核实垃圾信息

AMon通过核实并向负责用户垃圾信息报告的报告服务中心做出报告来处理可疑垃圾信息。该程序非常复杂，而且是在符合适用的国家相关法律法前题下，基于人工介入的。核实应采用指纹或垃圾信息的散列数据，而非短信内容。可通过一些信息辅助做出判定，例如，垃圾制造者和报告人的声誉，也就是说需要标出用户报告的可信度。

程序5：共享信息

AMgmt与受信任的对等方交换垃圾信息数据，且AMgmt从报告服务中心那里收到量身订制的垃圾信息分析报告。按照商定的一致意见，该数据可包含用户报告统计数据、垃圾制造者清单、投诉反馈和垃圾信息的新特性。该垃圾信息数据须得到谨慎处理，以确保其中不包含用户内容。

程序6：监测系统性能

AMon还负责监测垃圾信息过滤系统的性能。AMon从APr那里收集数据，以生成性能报告并对其做出分析。性能报告可包含垃圾信息与错误否定等之比的实时性能数字。

程序7：分析垃圾信息

源自报告服务中心、受信任对等方和AMon的经确认垃圾信息数据将得到汇集和存储，同时考虑到国家相关法律法规。AMon可定期分析这些数据并挖掘新的垃圾信息规律和特性。这将有助于完善过滤规则和系统性能。最后，这将被用来产生垃圾信息统计数据和垃圾信息分析报告，以发至AMgmt。

程序8：调整应对措施

根据AMon的垃圾信息统计数据和分析报告，AMgmt对垃圾信息过滤系统的打击垃圾信息性能做出评估，以进行必要的完善。根据评估结果，可调整已采用的措施和政策并改变与其他域之间的协作机制。还将采取相关措施，如，建立或终止信任关系并向APr发布新的过滤规则和程序。

参考资料

[b-ITU-T X.1240] Recommendation ITU-T X.1240 (2008), *Technologies involved in countering e-mail 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-M3AAWG report] M3AAWG, *Mobile Messaging Best Practices for Service Providers*, Updated August 2015.
https://www.m3aawg.org/sites/default/files/M3AAWG-Mobile-Messaging-Best-Practices-Service-Providers-2015-08.pdf

ITU-T 系列建议书

系列 A	ITU-T 工作安排
系列 D	一般关税原则
系列 E	整体网络运营、电话业务、服务运营和人为因素
系列 F	非电话电信服务
系列 G	传输系统和媒体、数字系统和网络
系列 H	视听和多媒体系统
系列 I	综合服务数字网络
系列 J	有线电视网络和电视的传播，合理的计划和其他多媒体信号
系列 K	干扰防护
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、包括电信管理网和网络维护
系列 N	维护：国际广播节目和电视传输电路
系列 O	测量设备说明书
系列 P	终端和主观及客观的评价方法
系列 Q	交换和信令
系列 R	电报传输
系列 S	终端服务终端设备
系列 T	远程信息处理服务终端
系列 U	电报交换
系列 V	电话网络之上的数据通信
系列 X	**数据网络、开放系统通信和安全**
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	电信系统的语言和通用软件方面

瑞士印刷
2017年，日内瓦