International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1234

(01/2022)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cyberspace security – Countering spam

Guidelines for countering multimedia messaging service spam

Recommendation ITU-T X.1234

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security (1)	X.1140–X.1149
Application Security (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	**X.1230–X.1249**
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1350–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1399
Distributed ledger technology (DLT) security	X.1400–X.1429
Application Security (2)	X.1450–X.1459
Web security (2)	X.1470–X.1489
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
Cyber Defence	X.1590–X.1599
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699
QUANTUM COMMUNICATION	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	X.1712–X.1719
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	X.1750–X.1759
Data protection	X.1770–X.1789
IMT-2020 SECURITY	X.1800–X.1819

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1234

Guidelines for countering multimedia messaging service spam

Summary

Recommendation ITU-T X.1234 specifies guidelines for countering multimedia messaging service (MMS) spam. It analyses typical scenarios, characteristics and recognition methods of MMS spam, and provides a technical framework, workflows and some key technologies of MMS spam recognition, to help MMS providers and MMS users to counter spam.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1234	2022-01-07	17	11.1002/1000/14796

Keywords

Multimedia messaging service, multimedia messaging service spam, technical framework

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Introduction

A multimedia messaging service (MMS) is a standard way to send messages that include multimedia content to and from a mobile phone over a cellular network. Users and providers may refer to such a message as a picture, video, sound, animation, etc. With the development of telecommunication technologies and the popularity of smartphones, MMS has become a mainstream way to send messages, especially for young people, and media companies which utilize it on a commercial basis as a method of delivering news and entertainment content. MMS brings convenient social contact and colourful messages, but it also becomes the way for spammers to send MMS spam. Such MMS spam, including unexpected advertisements, fraud information and viruses, is becoming a widespread problem and has caused a significant benefit loss to telecommunication operators, service providers and users.

Therefore, it has become an important direction in the field of countering spam technology to effectively counter MMS spam.

Recommendation ITU-T X.1234

Guidelines for countering multimedia messaging service spam

1 Scope

This Recommendation proposes a technical framework for countering MMS spam to achieve MMS spam governance and control. This framework specifies functional components, workflows and some key technologies of MMS spam recognition. In addition, this Recommendation covers typical scenarios of MMS spam with analyses of different types and general characteristics of MMS spam.

It is worth noting that all the operations in this Recommendation need to be permitted by users and administrative regulations. All the processes should follow applicable legislation carefully in order to avoid violating users' privacy.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1231] Recommendation ITU-T X.1231 (2008), *Technical strategies for countering spam.*

[ITU-T X.1247] Recommendation ITU-T X.1247 (2016), *Technical framework for countering mobile messaging spam.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 multimedia messaging service (MMS) [ITU-T X.1231]: Multimedia messaging service refers to a kind of messaging service after short message service which can transfer various multimedia messages including text, graphics, audio, video and so on through mobile network, wireless network or fixed network.

3.1.2 multimedia message service (MMS) spam [ITU-T X.1247]: Spam sent via MMS.

3.1.3 spammer [ITU-T X.1231]: Spammer refers to the entity or the person creating and sending spam.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 MMS spam identification functions (MMSSIF): A counter MMS spam system that is independent from a Multimedia Message Service Centre (MMSC), which includes the following functional components: monitoring function, data acquisition function, preprocessing function, recognition function, verification function, disposal function and system management function.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ASR	Automatic Speech Recognition
MMS	Multimedia Messaging Service
MMSC	Multimedia Message Service Centre
MMSSIF	Multimedia Messaging Service Spam Identification Function
SMS	Short Message Service
UICC	Universal Integrated Circuit Cards
URL	Uniform Resource Location

5 Conventions

This Recommendation uses the following conventions:

The keyword "**should**" indicates a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keyword "**may**" indicates an optional requirement which is permissible, without implying any sense of being recommended.

In the body of this Recommendation, the word "**can**" sometimes appears, in which case it is to be interpreted as "**is able to**".

6 Overview

MMS refers to a kind of messaging service introduced after the short message service (SMS), which can transfer various multimedia messages including text, voice and video through mobile networks or IP networks. With fast-developing telecommunication and Internet technologies, as well as the fast-growing popularity of smartphones, MMS, which brings convenient social contact and colourful messages, is an important means to send messages, especially for young people, and media companies which utilize it on a commercial basis as a method of delivering news and entertainment content.

However, it is also possible for spammers to send MMS spam. The MMS spam, including unsolicited information like advertisements, frauds, viruses and other unwanted messages, is becoming a widespread problem and has caused a large benefit loss to telecommunication operators, service providers and users. Therefore, how to effectively counter MMS spam technically has become an important challenge in the field of countering spam.

7 Scenarios and characteristic of MMS spam

As shown in Figure 7-1, the MMS procedure has three major steps: (1) The sender prepares MMS content and sends to MMSC, which his universal integrated circuit card (UICC) belongs to; (2) the MMSC receives the MMS content which was sent by the sender and decides whether to send this MMS to the next MMS centre or directly to the receiver; (3) the receiver gets the MMS from the MMSC, which may be different from the MMSC that the sender used.

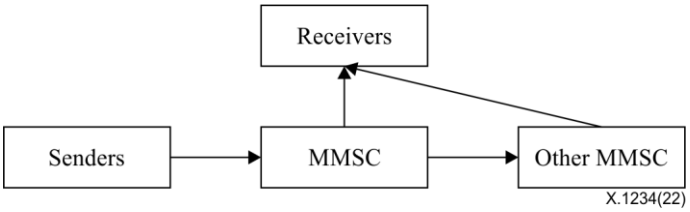


Figure 7-1 – MMS procedure

Spammers will use the above procedure to send spam to users, which is very annoying and may causes benefit loss to users. The spam content may include advertisements, fraud, etc. Here are some typical scenarios of MMS spam:

1. Fraud spam: This is MMS spam that makes up reasons to attract receivers to believe that he/she may receive some benefits or that something is true. If the receiver replies as the message indicates, the receiver will be charged or subscribed to some kind of value-added service of the fraud company for payment.
2. Trojan spam: Some MMS spam carries a media file with a trojan, and once they find a mobile phone that is vulnerable, and the phone's user opens the media file, they would get the highest administration authorization of the phone's system, then all secret information on the phone may be stolen, leaving the receiver totally unaware that this has occurred.
3. Virus spam: MMS spam may contain a certain kind of virus set-up file that looks like a normal one. Once the receiver clicks and finishes the set-up, the virus starts to destroy the phone system in many possible ways, usually by rapid deletion or disaggregation.
4. Unwanted advertisements: Advertisement MMS spam usually includes various kinds of advertisement for things such as loans, housing sales, training, etc. This spam is sent to receivers without receivers' permission or subscription. Some of them are typically deceptive and may put a link of ads on the MMS graphic or video, and if the receiver clicks the graphic or video, the web browser will be redirected to the ads' page.

8 Guidelines on the technical framework

8.1 General structure

As shown in Figure 8-1, a sender sends an MMS message to the MMSC and the receiver downloads the MMS message form the MMSC, so the MMSC stores all MMS messages. For that reason, it is recommended that MMS spam identification functions (MMSSIF) should be deployed adjacent to the MMSC.

It is difficult for any counter spam technology to guarantee 100% accuracy, and MMSSIF also require offline manual configuration and management, therefore service operators should be set up as shown in Figure 8-1.

At the same time, the working process of the original MMSC should be modified so that the MMSC sends the MMS message to the MMSSIF instead of forwarding it directly to the receiver or next MMSC after it receives the MMS message. The MMSSIF judges whether the MMS message is spam or not, and then gives corresponding suggestions to the MMSC. According to the suggestions, the MMSC will decide whether to continue sending this MMS message to the receiver or the next MMSC.

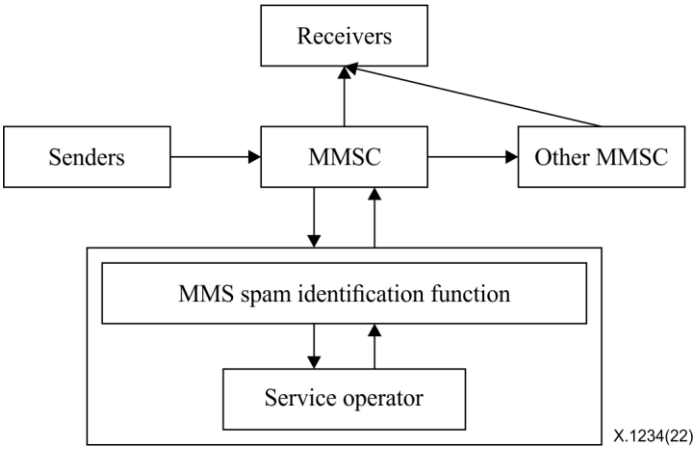


Figure 8-1 – General structure for countering MMS spam

8.2 Reference structure of MMSSIF

The reference structure of the MMSSIF mainly includes seven modules corresponding to different functions: monitoring, data acquisition, preprocessing, recognition, verification, disposal and system management. Different modules are recommended to be associated. Also, they should coordinate with each other according to rules or policies defined by relevant agreements.

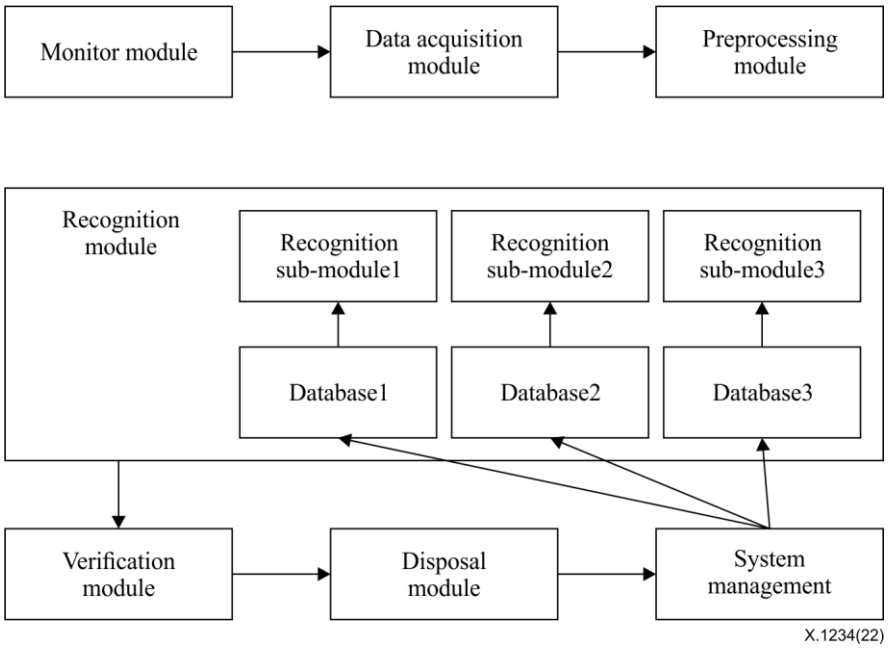


Figure 8-2 – Reference structure of MMSSIF

In Figure 8-2, the monitor module receives an MMS from the MMSC and gets the header of this MMS, including the subject, the sender's phone number, the number of attachments, the URL of those attachments, etc.

The data acquisition module receives those messages of the MMS header from the monitor module, and then downloads all attachments from the URL.

The preprocessing module receives all messages of this MMS from the data acquisition, including the header, all attachments, and then normalizes the messages by rules. The messages may be from the header or the body of the MMS, and the types of those messages may be text, image, video, audio, etc., so the rules are recommended to be compound rules such as "the source+ message type+ the message".

The recognition module receives normalizing messages from the preprocessing module and analyses whether this MMS is spam by some technologies, such as a blacklist, text recognition, image recognition, video recognition, etc.

The verification module receives the possible result from the recognition module and makes further judgements, such as manual determinations in order to decrease the possibility of false alarms.

The disposal module receives the recognition result from the verification module, and disposes of the MMS which is judged as spam, such as by blocking the MMS, sending an alert message to the spammers, etc. It also sends the original MMS, disposal log and the sender's phone number to the system management module.

The system management module receives the records from the disposal module and saves the operation log and system log. And it also sends the spammer's phone number, keywords, and images to the different databases in the recognition module in order to update the databases.

8.3 Functional components of MMSSIF

8.3.1 Monitor module

The functions of the monitor module include:

- Monitoring whether there is a new MMS sending from MMSC;
- receiving the whole data stream of the MMS;
- analysing the data stream and getting the header of the MMS;
- sending the subject, ender's phone number, number of attachments, URL of those attachments and the body of the MMS to the data acquisition module.

8.3.2 Data acquisition module

The functions of the data acquisition module include:

- receiving the messages from the monitor module and finding the URL of those attachments;
- downloading all attachments;
- sending all message of the MMS to the preprocessing module, including the header and the body of the MMS, which includes all attachments.

8.3.3 Preprocessing module

The functions of the preprocessing module include:

- receiving all messages from the data acquisition module;
- checking all attachments and judging whether they are text, image, audio or video, because according to the current MMS transport protocol, it is only allowed to include text, image, audio or video in an MMS;
- classifying the messages according to different types and normalizing the messages by rules, such as a compound rules "the source+ message type+ the message";
- sending the original MMS, all normalizing messages and the sender's phone number to the recognition module.

8.3.4 Recognition module

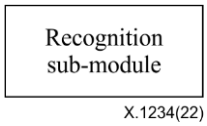
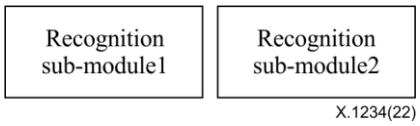
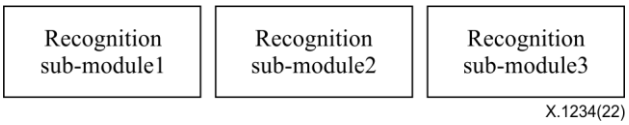
The functions of the recognition module include:

- analysing whether the MMS is spam;
- sending the recognition result to the verification module.

There are mainly three types of recognition technologies according to different parts of an MMS. The first one is based on the phone number, such as blacklist and whitelist. The second one is based on

the text, such as text recognition. The last one is based on the attachments, such as image recognition, video recognition, etc. Depending on the specific requirements and characteristics of the service provider, the recognition module may deploy a different sub-module according to the type of technologies.

Table 8-1 – Recognition module configuration model

Model	Description
Model 0	 Model 0 only has one sub-module, and has one type of recognition technology.
Model 1	 Model 1 is a shape of sub-module1 and sub-module2 configured together. Sub-module1 and sub-module2 are any two of the three types.
Model 2	 Model 2 is a shape of sub-module1, sub-module2 and sub-module3 configured together.

In Model 1 and Model 2, the recognition result may have different ways of being calculated. For example, in Model 1, Recognition sub-module1 deploys text recognition and Recognition sub-module2 deploys image recognition. Recognition sub-module1 recognized an MMS as spam, but Recognition sub-module2 did not recognize the same MMS as spam. Therefore, whether or not an MMS is recognized as spam requires an overall strategy for the recognition module. It's recommended to configure the strategy according to the actual needs and situation.

8.3.5 Verification module

The functions of the verification module include:

- receiving the possible results from the recognition module;
- making further judgement, such as manual determinations.

8.3.6 Disposal module

The functions of the data disposal module include:

- receiving the result from the verification module;
- disposing the MMS according to the recognition result, which is able to judge whether the MMS is spam;
- sending the disposal result to the system management module if the MMS is recognized as spam;
- sending the original MMS to the MMSC if the MMS does not recognize it as spam.

8.3.7 System management module

The functions of the system management module include:

- saving the operation log and system log;
- updating the databases;
- receiving feedback from users.

8.4 Reference model

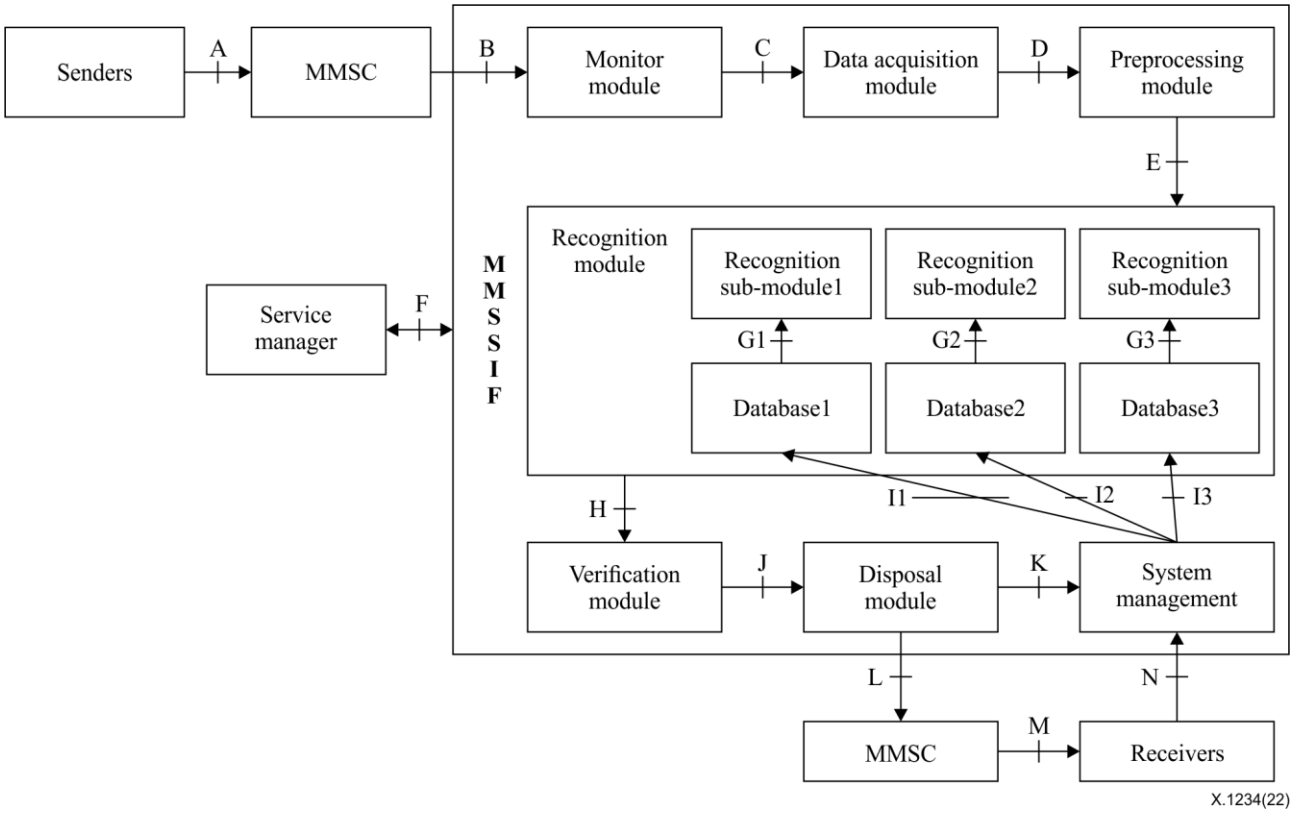


Figure 8-3 – Reference model for countering MMS spam

Interface A is between the senders and the MMSC. Interface A is used to transmit an MMS to the MMSC. This has already been realized when the service provider started to provide the MMS service to users. And it does not need to change in this model.

Interface B is between the MMSC and the monitor module. Interface B is a new interface and is used to transmit an MMS to the monitor module instead of forwarding it directly to the receiver or to the next MMSC.

Interface C is between the monitor module and the data acquisition module. Interface C is used to transmit the header of the MMS, sender's phone number, URL, etc., which are analysed by the monitor module.

Interface D is between the data acquisition module and the preprocessing module. Interface D is used to transmit all the messages, including the header of the MMS, the body of the MMS, the subject, all attachments, etc.

Interface E is between the preprocessing module and the recognition module. Interface E is used to transmit the normalizing messages, such as "the source+ message type+ the message". Interface E should support FTP and HTTP.

Interface F is between the service operator and the MMSSIF. Interface F is used to transmit the configuration rules and spam statistics.

Interface G is between the database and the sub-module. Interface G is not a specific interface. It represents a class of interfaces that are between different databases and its corresponding recognition sub-module. Interface G is used to transmit the suspicious number, text, image, etc., which are matched in the databases in order to recognize spam.

Interface H is between the recognition module and the verification module. Interface H is used to transmit the possible result and the original MMS.

Interface I is between the system management and the database. Interface I is not a specific interface, just like Interface G, and it represents a class of interfaces that are between different database and the system management.

Interface J is between the verification module and the disposal module. Interface J is used to transmit the recognition result and the original MMS.

Interface K is between the disposal module and the system management. Interface K is used to transmit the sender's phone number, recognition result, disposal and the original MMS.

Interface L is between the disposal module and the MMSC. Interface K is used to transmit the original MMS, which is not recognized as spam.

Interface M is between the MMSC and the receivers. Interface M is used to transmit MMS to the receivers. This has already been realized when the service provider started to provide the MMS service to users, and it does not need to change in this model.

Interface N is between the receivers and the system management. Interface N is used to transmit the feedback of the receivers.

9 Work procedures

Figure 9-1 shows that countering MMS spam consists of twelve procedures. These procedures constitute an adaptive system which contributes to the optimization of system performance.

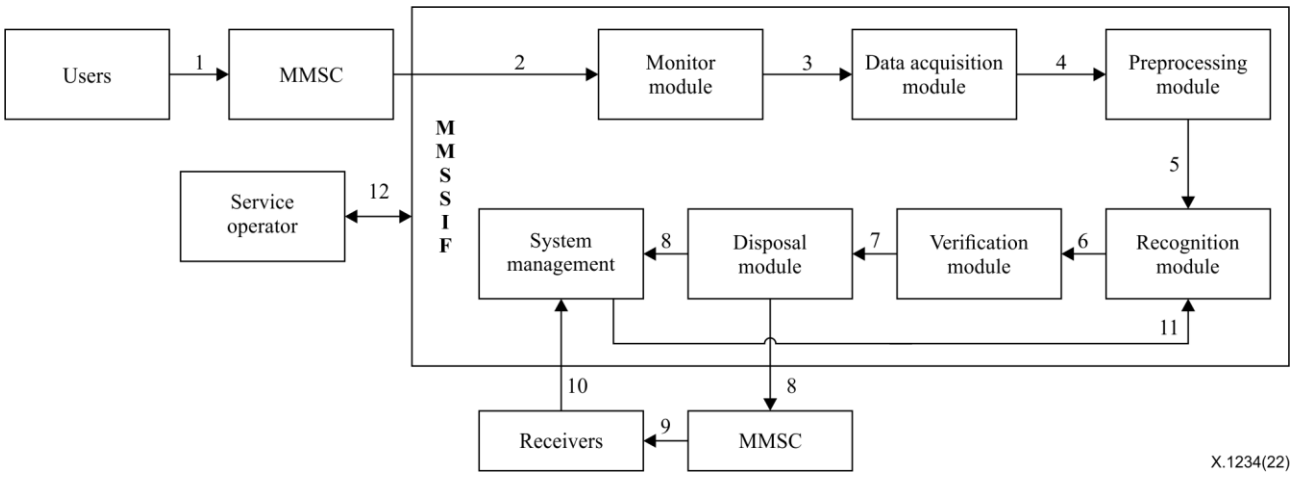


Figure 9-1 – Countering MMS spam processing procedures

Procedure 1: Sending MMS to MMSC

The sender prepares content of an MMS, receiver's phone number and then sends this MMS to the MMSC.

Procedure 2: MMS forwarding to the monitor module

The MMSC receives the MMS message from the MMSC and then forwards it directly to the monitor module.

Procedure 3: Getting the header of the MMS

The monitor module will monitor whether there is a new MMS being sent from the MMSC all the time. Once there is a new MMS, it will receive the whole data stream of the MMS, analyse the data stream and get the header of the MMS, including the subject, sender's phone number, number of attachments, and URL of those attachments. And then the monitor module will send all the messages to the data acquisition module.

Procedure 4: Downloading all attachments

The data acquisition module will receive the messages from the monitor module, find the URL of those attachments and download all the attachments. After getting all the message of the MMS, the data acquisition module will send this to the preprocessing module.

Procedure 5: Normalizing messages of the MMS

The preprocessing module will check all attachments and judge whether they are text, image, audio or video after receiving messages from the data acquisition module. If all the messages are legal, the preprocessing module will classify the messages according to different types and normalize the messages by rules. And then it will send the original MMS, all normalizing messages and the sender's phone number to the recognition module.

Procedure 6: Analysing the MMS

The recognition module will analyse whether the MMS is spam or not according to different technologies, which are deployed in the practical system. Then the recognition module will send the possible result to the verification module. Except for some specific technologies, the recognition module needs some overall strategies to get the final possible result.

Procedure 7: Making further judgement

The verification module will make further judgement after receiving the possible results from the recognition module and send the recognition result to the disposal module.

Procedure 8: Disposing the MMS

The disposal module will dispose of the MMS according to the recognition result. If the MMS is recognized as spam, the disposal module will dispose of the MMS by a set of rules, such as blocking the MMS, sending an alert message to the spammers, etc. It also sends the original MMS, disposal log and the sender's phone number to the system management module. The receiver will not receive this MMS. If the MMS is not recognized as spam, the disposal module will send the original MMS to the MMSC.

Procedure 9: Sending the MMS to the receiver

The MMSC will send this MMS to the receiver. Sometimes, it will send the MMS to another MMSC and then send it to the receiver. This procedure is the same as before when there is no MMSSIF function.

Procedure 10: Feedback of receivers

The receivers are the possible victims of spam, so they may voluntarily send some feedback to the service management module. The participation of receivers will be helpful for countering spam effectively and efficiently. Therefore, the system management module is recommended to use the feedback of receivers when developing solutions or strategies for countering spam.

Procedure 11: Updating the databases

The system management module will save the operation log, system log and the original MMS. It will update the databases as well, according to the new samples, phone number, keywords, etc.

Procedure 12: Adjustment of countering measures

According to the spam statistics and analysis report from the MMSSIF, a service operator will evaluate the MMSSIF performance for possible improvements. Based on the evaluation result, measures and strategies may be adjusted and collaboration mechanisms in the recognition module may be adjusted by the service operator.

10 Guidelines on key technologies

An MMS is able to transfer various multimedia messages including image, text, video, audio, etc. Therefore, the key recognition technologies for countering MMS spam mainly include image recognition, text recognition, video recognition, audio recognition, etc.

10.1 Spam filter list

The spam filter list includes blacklist, whitelist and ambiguous list. The service providers should configure the MMSSIF to log suspicious activity or optionally configure it automatically (e.g., block suspicious MMS, allow normal MMS) for blacklist or whitelist. The service providers should also maintain the list to keep the MMSSIF available and working stably. While anomalies of an unlisted phone number are detected, the phone number should be given to a manual review process to conduct a full assessment.

10.2 Image recognition

Image recognition firstly extracts a feature for the image representation and establishes a database of image eigenvalue. The detection of spam is then transformed into a binary classification problem in the feature space and can be solved by conventional machine learning. Or more simply, if the image's eigenvalue of an MMS message is matched in the database, the message is recognized as spam. This method depends on the quality of the image eigenvalue database.

10.3 Text recognition

Text recognition mainly includes keyword recognition and semantic recognition. Keyword recognition firstly establishes a keywords database. If the text content of an MMS message contains any keywords that are matched in the keywords database, the message is recognized as spam, further, text recognition can build Boolean logic models and the vector space model, after training, the recognition model is obtained which can improve the accuracy of text recognition. This method depends on the quality of the keywords database.

Sometimes, spammers are highly creative in avoiding detection. For example, spammers may falsify normal email and randomize the content to avoid the keywords detection of spam filters. Therefore, based on keyword recognition, it is very effective and efficient to use semantic recognition to achieve secondary recognition (e.g., a natural language processing approach based on fuzzy semantic recognition), which may greatly reduce the false positive rate.

10.4 Video recognition

Video recognition generally establish a sample database first, and then compares the video of an MMS message with video samples one by one to judge whether the video is spam or not. It can also identify by extracting key frames of a video. The main operations are as follows: decoding the video, processing it as a set of images, and then sampling from those images, identifying the sampled images

based on image recognition technology, and finally getting the video recognition result by using the comprehensive analysis result of those sampled images.

10.5 Audio recognition

Audio recognition can be implemented in combination with automatic speech recognition (ASR) technology. The goal of ASR technology is to enable computers to "dictate" the continuous speech spoken or utterances of keywords or sentences by different people, and it is able to convert "voice" into "text". In addition, in order to identify similar or equal audio data, spectral features are extracted, and a short and robust audio fingerprint is computed. Therefore, ASR is able to "recognize" some certain keywords from an audio, which can determine if the audio is spam.

10.6 Feedback of end users

Feedback from end users, the associated implementation guidance and other information specified in clause 8.5 of [ITU-T X.1231] and in Annex A of [ITU-T X.1247] apply.

Some end users will delete MMS spam directly when they receive it, and a few end users will report the MMS spam through the official client feedback. The effectiveness of this method depends on the enthusiasm and initiative of the end users. The active participation of end users will be encouraged for countering MMS spam effectively and efficiently.

Bibliography

[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*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2022