
Question(s): 5/17

Geneva, 8-17 December 2010

TEMPORARY DOCUMENT

Source: Editor

Title: Updated text of X.oacms: Overall aspects of countering messaging spam in mobile networks

This document is the updated draft text of X.oacms which is based on the discussion of SG 17 meeting in December 2010.

The modifications are:

1. change the title name into “Overall aspects of countering messaging spam in mobile networks”.
2. move the Chapter 10 “Proposed solutions on countering messaging spam for mobile phones” to Annex A.
3. add a new chapter A.1 to describe the performance consideration of the proposed solutions.
4. delete the original chapter 6 “current status analysis of messaging spam” which is TBD; and remove to Appendix II.
5. change the name of Appendix I to “Activities on countering messaging spam”.
6. apply the editorial suggestions in C334 to Chapter 8 “current technologies and mechanisms on countering messaging spam” based-on the discussion in the meeting.
7. merge the new contents in C317, C318 into Appendix I, II based-on the discussion in this meeting.

Contact:	Linlin Zhang China Academy of TeleCom. Research MIIT China	Tel:0086-10-62304633-2752 Mob: 0086-13811876439 Email:zhanglinlin@emcite.com
-----------------	--	--

TSB Note: All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.
--

CONTENTS

1	Scope.....	4
2	References.....	4
3	Definitions	4
	3.1 Terms defined elsewhere	4
	3.2 Terms defined in this Recommendation.....	5
4	Abbreviations and acronyms	5
5	Conventions	6
6	Classification and characteristics of messaging services.....	6
	6.1 SMS	6
	6.2 MMS.....	6
7	Types of messaging spam.....	7
	7.1 SMS spam.....	7
	7.2 MMS spam	7
8	Current technologies and mechanisms on countering messaging spam	7
	8.1 Technologies and mechanisms on countering messaging spam.....	8
	8.2 The comparison of technologies and mechanisms on countering messaging spam.....	9
Annex A	Proposed solutions on countering messaging spam for mobile phones	12
	A.1 Introduction	12
	A.2 Solution based on the locations and hash values of mobile phones	12
	A.3 Solution based on sending behaviours of mobile phones.....	15
	A.4 Other solutions.....	15
Appendix I	Activities on countering messaging spam.....	16
	I.1 Development of technical specifications for countering messaging spam.....	16
	I.2 International activities on countering messaging spam.....	22
	I.3 List of industry alliances and initiatives for countering messaging spam.....	22
Appendix II	Current status analysis of messaging spam	23

Introduction

[TBD]

Overall aspects of countering messaging spam in mobile networks

1 Scope

This Recommendation provides the overview of messaging spam, including the current status analysis of messaging spam, classification and characteristics of messaging services and types of messaging spam. However, this Recommendation only focuses on short message service (SMS) spam and multi-media message service (MMS) spam.

This Recommendation also introduces relative works in different organizations, relative technologies and mechanisms on countering messaging spam; furthermore, this Recommendation makes specific comparison of these technologies and mechanisms.

In addition, this Recommendation proposes new solutions on countering messaging spam in mobile networks.

The relative activities on countering messaging spam are introduced in Appendix I.

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

[3GPP TR 33.cde s3-091238], 3GPP TR 33.cde s3-091238 (1000), *Study of Different SPAM Protection Mechanisms: Protection against SMS and MMS SPAM*

[3GPP TR 33.837] 3GPP TR 33.837 V7.4 (), *Study of Mechanisms for Protection against Unsolicited Communication for IMS (PUCI)*

[Editor's note]: The contents will be updating during the drafting of this recommendation.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 call detail record (CDR): Formatted collection of information about a single call or data communication session, (e.g. time of call set-up, duration of the call, amount of data transferred, etc) for use in billing and accounting. [b-ETSI TR 122 924]

3.1.2 enhanced messaging service (EMS): The Enhanced Messaging Service (EMS) is based upon the standard SMS, but with formatting added to the text. The formatting may permit

the message to contain animations, pictures, melodies, formatted text, and vCard and vCalendar. Objects may be mixed together into one message. [b-ETSI TS 123 040]

3.1.3 multimedia messaging service (MMS): A multimedia message service allows transfer of multimedia messages between users without the requirement for the multimedia messages to be transferred in real-time. [b-ETSI TS 122 140]

3.1.4 short message service (SMS): The SMS provides a means to transfer short messages between a GSM/UMTS MS and an SME via an SC. The SC serves as an interworking and relaying function of the message transfer between the MS and the SME. The present document describes only the short message services between the MS and SC. It may, however, refer to possible higher layer applications.[b-ETSI 123 040]

3.1.5 spam: The meaning of the word "spam" depends on each national perception of privacy and what constitutes spam from the national technological, economic, social and practical perspectives. In particular, its meaning evolves and broadens as technologies develop, providing novel opportunities for misuse of electronic communications. Although there is no globally agreed definition for spam, this term is commonly used to describe unsolicited electronic bulk communications over e-mail or mobile messaging for the purpose of marketing commercial products or services.[b-ITU-T X.1240]

3.1.6 SMS spam: Spam sent via SMS.[b-ITU-T X.1242]

3.1.7 spammer: An entity or a person creating and sending spam.[b-ITU-T X.1240]

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 MMS spam: Spam sent via MMS.

[Editor's note]: The contents will be updating during the drafting of this recommendation.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CDR	Call Detail Records
CID	Cell ID
EMS	Enhanced Messaging Service
GSM	Global System for Mobile Communications
MMS	Multimedia Messaging Service
MSC	Mobile Switching Centre
VLR	Visitor Location Register
LAC	Location Area Code
SMS	Short Messaging Service
SMSC	Short Message Service Centre
WAP	Wireless Application Protocol

SCM	Service Control Module
SSFM	SMS Spam Filtering Module
USMM	User Service Management Module
URD	Userspecified Rules Database
FMD	Filtered Messages Database
SCCP	Signalling Connection Control Part
MAP	Mobile Application Part
TCAP	Transaction Capabilities Application Part
TCAPsec	TCAP user security – the SS7 security gateway security protocol suite
SM	Short Message
MT-SM	Mobile Terminated – Short Message
UC	Unsolicited Communication
PUCI	Protection against Unsolicited Communication for IMS
IMR	Identification, Marking and Reacting
CBCS	Categorization Based Content Screening
SpamRep	Spam Report
SCIDM	Secure Content Identification Mechanism
CIM	Content Identity Manager
MO	Mobile Originated
MT	Mobile Terminated

[Editor's note]: The contents will be updating during the drafting of this recommendation.

5 Conventions

None.

6 Classification and characteristics of messaging services

6.1 SMS

SMS was originally defined to exchange the short text message between mobile phone devices in GSM mobile communication system by 3GPP. Since then, support for the service has expanded to other mobile networks after GSM, such as 3G network. SMS is a non-real-time service, using the store-and-forward way for message transmission; the message is stored in a short message service centre (SMSC) before sent out. The using of signalling channels limits the size of the short message; the maximum individual size for a short message is 140 octets, which is the same with 160 characters of GSM 7-bit alphabet and 70 characters of 16-bit UTF-16 alphabet. The convenience and relatively low price make SMS the most widely used messaging service with enormous commercial value.

6.2 MMS

MMS is based on new service architecture and high-bandwidth data channels in message

transmission. MMS provides multimedia messaging services; the multimedia message content includes variety of media types such as photos, videos, voices and text, etc. The MMS is viewed as a non-real-time delivery service and also provides a store-and-forward usage paradigm. The data channels offer larger message size and high performance in message transmission. The maximum size for an MMS message recommended by OMA is 300kbytes due to the limitations on the wireless application protocol (WAP) gateway side, and the size also depends on the network and mobile phones the subscribers use.

[Editor's note]: Add Introduction or overview in the beginning of this chapter, EMS should be included in this chapter.

7 Types of messaging spam

The messaging spam types that this recommendation concerns are SMS spam and MMS spam in mobile networks. This clause describes characteristics for SMS spam and MMS spam.

7.1 SMS spam

SMS spam is unsolicited electronic communications over SMS, usually with the objective of marketing commercial products or services. SMS spam is widely spread in the society; the advertisement in the short message disturbs people's daily life seriously, moreover, the hostile or the illegal information carried in the short message even threatens the safety of the society.

Some service providers are also affected for the charge of the communication; because the charging process is after the sending process, the time interval is used by spammer to send the spam message and it will make huge malicious arrears. Furthermore, the spam consumes storage space and computing resources of mobile network, and it will affect the service quality of legitimate subscribers.

With low cost for bulk sending and large number of subscribers of SMS, the SMS spam is the most common messaging spam type of mobile network.

7.2 MMS spam

MMS spam is unsolicited electronic communications over MMS, usually with the objective of marketing commercial products or services. Since the mobile phones for MMS is more intelligent with more functions, some of them with operating systems, except for the threat of SMS spam, the MMS spam are more easily to be used as a vehicle for phishing, spreading viruses, worms, spywares and other types of malwares.

Even if the cost for individual multimedia message is much higher than the short message, bulk spam will tremendously reduce the cost for the spammer. Furthermore, the rate of return is more than the SMS spam, in most countries, it's free to receive short message, but for multimedia message, subscribers may have to pay the traffic charge for multimedia message that needs internet browsing.

8 Current technologies and mechanisms on countering messaging spam

There are many technologies and mechanisms for countering messaging spam. This clause will discuss each of them.

8.1 Technologies and mechanisms on countering messaging spam

8.1.1 Blacklists/whitelists

The phone numbers of messaging senders are used in blacklists/whitelists on countering messaging spam of mobile networks. The filtering system will accept the messages from whitelists while suspend the messages from blacklists. To avoid complaint of subscribers, the phone numbers in blacklists are only valid within a specific period, after that, the phone numbers will be removed and considered from legitimate subscribers.

The blacklists /whitelists is easy to deploy, basically the message service center doesn't need to be changed. But the ability of recognizing the messaging spam is limited, and it needs continual updating of blacklists and whitelists.

8.1.2 Content filtering

The most common content filtering technology is filtering based on user-specified rules, which is easy to implement, however, the rules have to be updated frequently and just limited to the some key words; it relates to the privacy problem and the spammers can use the spacing, alternate characters and misspelling to counter the content filtering.

Besides, there are many technologies are used in content filtering, such as the hash value method, Bayesian algorithm and support vector machines, etc, which will learn the frequency and the pattern of the key words. These content filtering technologies are more intelligent and sophisticated, but also need frequently updating of the rules and training sets, and real-time performance is generally not good.

8.1.3 Traffic statistics

This mechanism is to statistic the sending message traffic of a subscriber or a service provider, if the statistics exceed the specified threshold, the alarm system will be triggered and the message sender will be monitored and filtered. There are two methods for traffic statistics, one is to measuring the amount of messages that a sender sends out within unit time. Another method is to measuring the interval between two message sending behaviours of a sender.

Traffic statistics is easy to implement, but it's difficult to set the threshold for the number of messages that a sender sends out within unit time, if the threshold is two small, it's easy to cause false positive problems. However, if the threshold is two big, traffic statistics can't achieve the expected results of recognition. In addition, the threshold is easy to be tried out, after that; the spammers can adjust the sending rate and number based on the threshold to counter the traffic statistics.

8.1.4 Analysis of CDR

This mechanism using the call detail record (CDR) as the statistic resource; the filtering system continuously scans the charging server and downloads the latest CDRs to the local system , then the statistic module will scan the local working directory at interval of definite time and analyze the CDRs based on the sequence of arrival, if the amount of messages that a sender originated successfully within unit time exceed the threshold, the sender is considered suspicious and the information will be provided to the administrator to determine if the phone number should be put into blacklists.

8.1.5 Greylisting

For the characteristic that most message spammers won't retry a failed delivery, the graylisting can be used for mobile message recognition. The message service center will create a unit doublet in the format {calling number, called number} for each new arrived message; when a unit doublet first

shows, the message service center will send a temporary failure message to the sender and refuse to deliver this message, then record the first arrived time of the unit doublet. Otherwise, if the message sever has had the record for the unit doublet already, and the interval between the current time and first arrived time is larger than a preset threshold; the message will be transferred by message service center.

Greylisting is a good inhibitory action for message without multiple sending attempts, but the disadvantage is it usually causes unacceptable delay for the message sending of legitimate subscribers. Furthermore, the deployment of greylisting needs to make modifications to the message service center.

8.1.6 Duplicate content recognition

For the spammers' interest, the messaging spam pursues the high throughput and large-scale spread, the messages that a spammer sends out in a period of time usually have similar contents which can form a high degree cluster, therefore the object of statistics can be changed from vast amounts of individual messages to message groups, if the amount of duplicate contents in a cluster exceeds the threshold, the cluster will be marked as spam.

Duplicate content recognition using the signature of spam message for recognition, it is not sensitive to counter measures such as the spacing, alternate characters and misspelling used by spammers. The sample of messaging spam which marked by duplicate content recognition can be used for developing the filtering rules, the calling numbers can be added into blacklists, besides, those procedures only with little involvement of administrator and the maintenance cost is relatively low. Moreover, this mechanism well protects the privacy of subscribers.

The disadvantage is it needs learning process in the network, and may cause false positive for legitimate distribution of messages, to solve the problems, it's better to be used with other technologies and mechanisms in combination.

There are two methods to implement the duplicate content recognition, and both need to make change of the network.

- One method is to build the duplicate content recognition in the message service centre. In this method, the recognition of messaging spam and the mark operation are executed within the message service centre, so the processing is relatively fast. But when the third party software is at failure situation, the ordinary work of message service centre will be affected in performance.
- Another method is to bypass the message service centre which doesn't need to be changed. This method needs extra equipments connecting with multiple message service centres. The recognition will have overall perspective, and it won't affect the regular work of message service centres; however, the speed is lower than the first method, but it still has acceptable real-time operation performance. But the spam message signature generation is a problem to solve.

8.1.7 Indication information recognition

Some spam messages contain URLs or phone numbers that subscribers can access, so indication information recognition using this information as resource of statistics, if the occurrence number of URLs or the phone numbers exceed a threshold, the follow-up message that contains the same indication information is considered to be spam.

8.2 The comparison of technologies and mechanisms on countering messaging spam

There are many technologies and mechanisms have been mentioned, this clause will make a comparison of them with 7 performance indicators. The result is shown in Table 8-1.

Table 8-1 Performance comparison of security technologies and mechanisms

Technologies and mechanisms	Maintenance cost	Real-time	Recognition rate	False positive	Complexity	Privacy	Learning process
Blacklists/whitelists	Small	Good	Low	Low	Easy	Good	Short
Content filtering based on user-specified rules	Big	Good	High	High	Easy	Bad	Short
Traffic statistics	Small	Medium	Low	High	Easy	Good	Long
Analysis of CDR	Small	Bad	Low	Medium	Medium	Good	Long
Greylisting	Small	Bad	Medium	Low	Medium	Good	Short
Duplicate content recognition	Small	Good	High	Low	Medium	Good	Medium
Indication information recognition	Small	Good	Medium	Medium	Medium	Good	Medium

Maintenance cost is the cost for keeping the effectiveness of a technology or mechanism. Because the spam technology is developing fast, the spam message also changes frequently, content filtering based on user-specified rules needs continuously updating of the rules, which makes the maintenance work relatively difficult.

The real-time performance is the first consideration when choosing the solutions. Content filtering based on user-specified rules and blacklists/whitelists have good real-time performance; duplicate content recognition and indication information recognition also can work in a liner time. However, traffic statistics, analysis of CDR and greylisting are all working off-line, but they can be used with other technologies and mechanisms in conjunction.

The recognition rate is the rate of successful recognition of spam; it's a very important indicator. Duplicate content recognition and content filtering based on user-specified rules have satisfied indication rate, but blacklists/whitelists has limited recognition ability, graylisting can't act on retry delivery messages and indication information recognition is only used for the spam message contains URL or phone number. Therefore, these solutions also have to be used with other technologies and mechanisms together.

The false positive indicator requires the solution doesn't affect the legitimate message when countering spam. Content filtering based on user-specified rules can't separate the spam and the legitimate message efficiently; so as the traffic statistics. The blacklists/whitelists and greylisting are solutions with low false positive rate, duplicate content recognition has the false positive problem when used alone, but if the threshold set higher, the false positive problem will dramatically reduced, but the drawback is it needs more learning time.

Each solution has acceptable complexity, and content filtering based on user-specified rules, blacklists/whitelists and traffic statistics are easy to deploy, while other solutions need development of third party.

For the protection of privacy, except for content filtering based on user-specified rules, all solutions don't have to check the content of the messages.

As for the learning process, content filtering based on user-specified rules and blacklists/whitelists can be used directly; while traffic statistics and analysis of CDR needs long time learning process, duplicate content recognition and indication information recognition also need some training time.

From the analysis, there is no single solution can solve messaging spam problem thoroughly; the combination solution has to be used. And even if the real-time, accurate recognition and no false positive are the ideal situations, it's difficult to reach in reality. The target of these solutions is to cut down the numbers of messaging spam, reduce false positive rate, not make delay of the message sending and provide better service quality to the subscribers.

Annex A

Proposed solutions on countering messaging spam for mobile phones

(This annex forms an integral part of this Recommendation)

A.1 Introduction

There are three phases from a message sending to receiving: mobile originated (MO) phase, store-and-forward phase and mobile terminated (MT) phase, which are related to three entities: sending entity, message service centre and receiving entity.

Countermeasures can be used in each entity, in this clause, some solutions used in message service centre are proposed. The function models of solutions may be deployed in or bypass the message service centres. The proposed solutions will dynamically track and analyze the contents and behaviours of messages based on user specified rules in real-time, but the messages sending don't have to wait for the finish of the analysis. Therefore the solutions will have little effect on QoS of mobile users.

A.2 Solution based on the locations and hash values of mobile phones

From the statistics of the messaging spam, there are two remarkable characteristics that legitimate messages don't have: one is the repeated contents, another is the senders have the same location with different calling numbers.

According to these characteristics, a solution based on the locations and hash values of mobile phones has been proposed. The basic idea is that the messages are able to be classified into different groups based on the repetition rate; the groups can be separate by reasonable threshold, and then, use the calling numbers and location of the senders for spam recognition.

The solution's architecture includes two functional modules: the message classifying module which will convert the original messages into hash values and write into the hash table; classify the messages based on the hash values, and mark the suspicious message groups if the repeated messages exceed the threshold; while spam recognizing module will statistic the calling numbers and the senders' locations of subsequent messages in suspicious groups to recognize spam. The system architecture is shown in Figure 10-1.

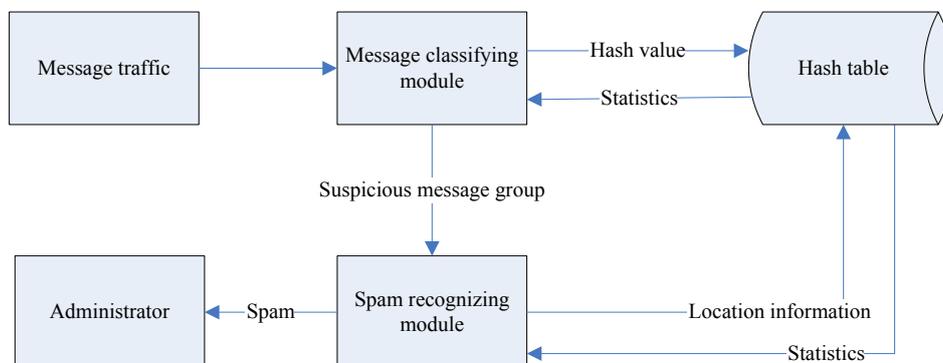


Figure A-1 Architecture of solution based on the location and hash values of mobile phones

A.2.1 Message classifying module

[TBD]

A.2.2 Spam recognizing module

[TBD]

A.2.3 Algorithm

The algorithm for proposed solution is as Figure 10-2, it assigns the parameters $f_0=500$, $f_1=500$, the parameters can be changed as required.

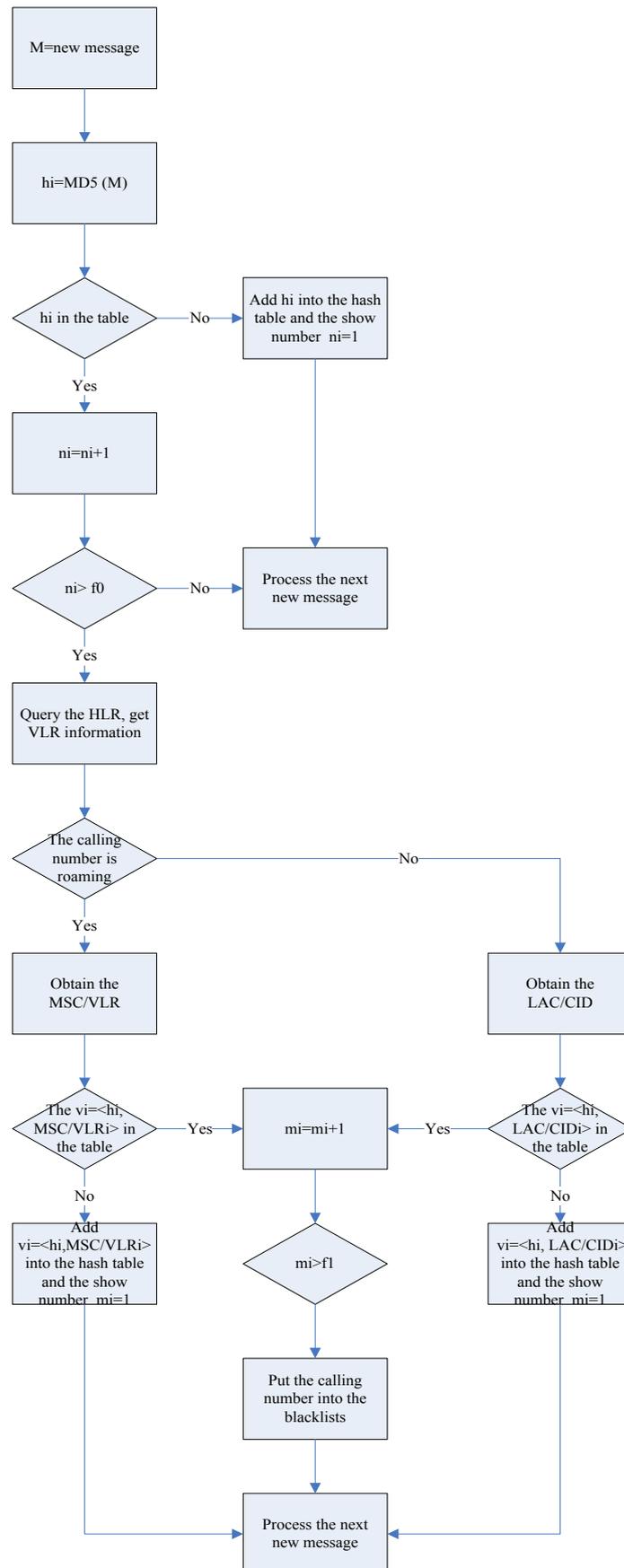


Figure A-2 Algorithm of solution based on the location and hash values of mobile phones

The procedure of the algorithm is as following:

- 1) Initialize the algorithm, create the hash table T.
- 2) Calculate the hash value of the new message M, $h_i = \text{MD5}(M)$.
- 3) If h_i is already in hash table T, the count for occurrence number of h_i is $n_i = n_i + 1$; otherwise, put h_i into table T, $n_i = 1$.
- 4) If $n_i \leq f_0$ (f_0 is the preset threshold), process the next new message; else if $n_i > f_0$, go to step 5.
- 5) Query HLR, if the sender is roaming, get the MSC/VLR information, if the MSC/VLR_i is in the table T, the count for the occurrence number is $m_i = m_i + 1$; otherwise, put MSC/VLR_i into table T and set $m_i = 1$;
If the sender is not roaming, get the LAC/CID information, if the LAC/CID_i is in the table T, the count for the occurrence number is $m_i = m_i + 1$; otherwise, put LAC/CID_i into table T and set $m_i = 1$.
- 6) If $m_i \leq f_1$ (f_1 is the preset threshold), process the next new message; else if $m_i > f_1$, go to step 7.
- 7) Put the calling into the blacklists.

[Editor's note]: The efficiency of this solution needs to be considered.

The functions models can be deployed bypass the message centre; the function models just have to analyze using the collected information, if the spam is found; it will put the calling number into the blacklists.

The message sending doesn't have to wait for the finish of the analysis. So the analysis of messages won't affect the QoS in real-time.

Pick up samples if the message flow is serious.

A.3 Solution based on sending behaviours of mobile phones

[TBD]

A.4 Other solutions

[TBD]

Appendix I

Activities on countering messaging spam

(This appendix does not form an integral part of this Recommendation)

I.1 Development of technical specifications for countering messaging spam

I.1.1 ITU-T

The specification regarding in countering messaging spam are as follows:

-Technical strategies for countering spam

Recommendation ITU-T X.1231 gives a hierarchical model for countering spam. The model includes the following five parts:

- Equipment strategies
- Network strategies
- Service strategies
- Filtering strategies
- Feedback strategies

The five parts above can be divided into three levels: infrastructure level, service level and application level. Figure I-1 shows the relationship between different parts.

Equipment strategies and network strategies belong to the infrastructure level, and they are the foundation of the model. The implementation of them can be a reliable foundation for technical strategies in the upper layers. Service strategies belong to the service level, and it is the most important among the five parts because the layer is directly responsible for the provision of service. Finally, filtering strategies and feedback strategies belong to the application level, which are closer to users for countering spam. Filtering is the most common anti-spam technology. When making solutions for countering spam, feedback of end-users should be taken into account. Because end-users are the final receivers of spam, the feedback of end-users will be helpful for countering spam efficiently.

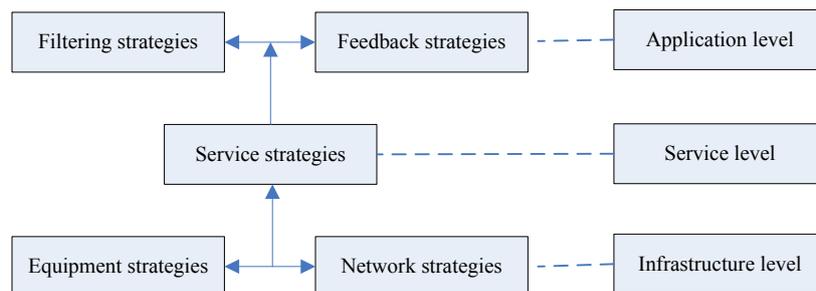


Figure I-1 Relationship between different parts

X.1231 also points out if all the technical strategies are satisfied, the cost may be too high. Therefore, it is very important to make the technical strategies according to different application scenarios.

-SMS spam filtering system based on user-specified rules

SMS spam filtering system based on user-specified rules (Recommendation ITU-T X. 1242) attached to SMSC, in which users can configure (add, delete and edit) filtering rules, and at the same time, all short messages to such users can be filtered according to those filtering rules.

Filtering rules can be based on address (phone number), time, content, etc, and specific filtering rules can be used individually or in combination with other filtering rules. In addition, users can manage (query, delete and restore) filtered short messages and filtering rules by SMS, Web and secretary station.

The SMS spam filtering system includes the following five logical modules: service control module (SCM), SMS spam filtering module (SSFM), user service management module (USMM), user-specified rules database (URD) and filtered messages database (FMD). The structure of the SMS spam filtering system is shown in Figure I-2.

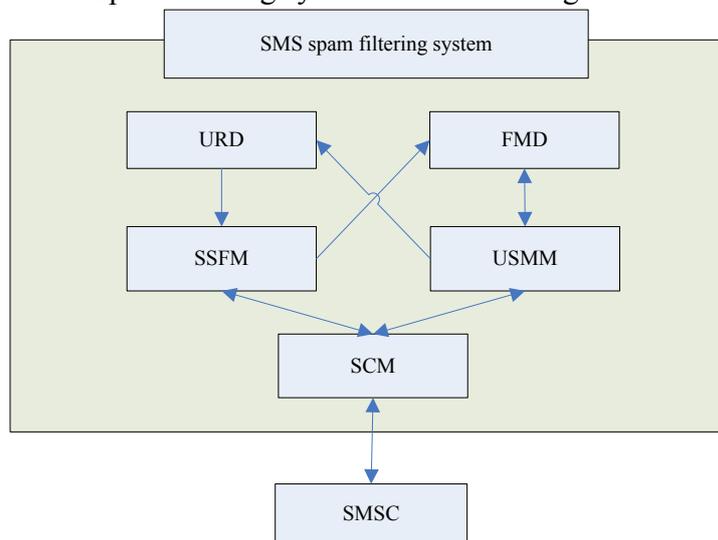


Figure I-2 Structure of the SMS spam filtering system

The SCM is connected to the SMSC directly and is mainly responsible for external entities accessing the filtering system. The SSFM implements SMS spam filtering, while the USMM implements management of the filtering rules and the filtered short messages. The URD is used for storing user-specified filtering rules. The FMD is used for storing short messages filtered out as spam by the SSFM.

I.1.2 3GPP

With respect to the anti-spam study work in SMS and MMS, the following mechanisms have been proposed in 3GPP:

-TCAP & TCAP security [b-3GPP TS 33.200] and [b-3GPP TS 33.204]

Verifying the identity of a sender accurately is a precondition to realize anti-spam technology. With the increasing number of spam messages, in some cases, the SCCP or MAP addresses for mobile-terminated SMS traffic are spoofed, which makes it difficult for operators to apply SMS spam protection rules and may cause inter-operator accounting difference. Therefore, [b-3GPP TS 33.200] and [b-3GPP TS 33.204] respectively describe two mechanisms to prevent address spoofing. The first one which is called TCAP handshake allows verifying if the originating network address has not been spoofed. The second mechanism for protecting all TCAP user messages called TCAPsec, and it can provide more accuracy in authentication than the first one. The benefit for an operator applying TCAPsec will gradually increase when more interconnected operators also apply TCAPsec.

-Routing of MT-SMs via the HPLMN [b-3GPP TR 23.840]

The report [b-3GPP TR 23.840] provides a study into the current core network architecture for inter-PLMN short message delivery. Because User Equipment often does not have the capability for complex spam identification and processing, such functionality is provided by the HPLMN. However, as discussed in this report, if the receiving MS is roaming outside of the HPLMN, then SMs don't pass the HPLMN and therefore the HPLMN cannot intercept such SMs. As a result, the end user has to receive such "Spam" SMs while roaming, incurring a roaming charge for receiving it.

According to the analysis, it is proposed that all MT-SMs shall have the capability to be routed via a SMSC-like logical entity located in the HPLMN of the receiving MS. Before arriving at the VPLMN which the end user will visit, SMs will first pass the receiving MS' HPLMN. Once the SMs enter into the HPLMN, the HPLMN will carry out the relevant anti-spam measures. After that, the SMs will be sent to the receiver.

-Protection against unsolicited communication for IMS [b-3GPP TR 33.937]

The report [b-3GPP TR 33.937] describes several solutions that could be used to protect mobile subscribers from receiving unsolicited communication over IMS. These are the four solutions in this report:

- SPIT/UC protection with supplementary services (SS)
- Contextual information (CI) – an extension to SS
- Methods for authentication of origin networks like the open proxy handshake
- Identification, marking and reacting (IMR)

Supplementary services provide means to identify an Unsolicited Communication (UC) and react on it. For identification purpose, the user or operator has to do prior setting. The prior setting is in terms of order in which SS modules are used, done potentially on operator requirements, and the setting done by the user, e.g., whitelist or blacklist.

Contextual information provides means that can be used together with SS to identify a potential UC when the communication is taking place for the first time between two parties. Thus SS together with CI can be used for initial deployment of IMS with list based solution where the list (white or black) of a user can be populated by CI or by the keypad.

UC-OPH, provides methods for secure communication between networks especially IMS and non-IMS networks. Besides that UC-OPH is dependent on other solutions.

IMR provisions for identifying, marking and reacting against UC based on operator policies and user requirements. The initial step in IMR-based unsolicited communication prevention is to identify that the given communication is unsolicited. Once a given communication is identified as unsolicited it should be marked. Marking could be as simple as a means to notify that a given communication is unsolicited. Having identified and marked a communication as unsolicited the next step is to react on it.

Identification, marking and reaction of UC can be handled in many places, in the network or UE. Moreover, different steps can be centralized or distributed. They can be done as follows:

- Automatically in the network or UE or distributed in the network and UE
- With or without intervention from the user at each or certain steps
- Manual setting in the network and/or UE by the operator and/or user
- At the beginning, during, or end of the communication

The details of how these functions will be realised will be dependent on the eventual selection of supporting methods.

In summary, the four solutions presented in TR are complementary. SS can be enhanced with CI, UC-OPH is the solution for inter-operator purposes and IMR provides a framework that uses SS as modules for identification and, where available, marking.

I.1.3 OMA

The anti-spam study work related to SMS and MMS has the following work items in OMA:

-Client side content screening

With the growing amount of malicious content delivered to mobile terminals, the OMA Categorization Based Content Screening Framework in [b-OMA-AD-Client_Side_CS_FW] defines architecture for content screening framework within the mobile terminal. The scope of this architecture is restricted to client/terminal deployments only. The framework consists of three parts: Scan Engine functional component, OMA and non-OMA enablers, and the framework interfaces to OMA/non-OMA enablers for utilizing content scanning functionality to detect and screen malicious content.

The logical model of the content screening framework in a mobile terminal is shown in Figure I-3. OMA and non-OMA enablers communicate with the scan engine via interface defined by the client side content screening framework.

The general process is as follows. An enabler would directly pass content to the scan engine for analysis before it is presented to the end-user. The scan engine would analyze the content whether the content is found to be malicious or not, and then return the result of the analysis to the calling enabler. The calling enabler screens the content if the content is found to be malicious, it is recommended that screening action be conveyed to the end-user in the form of warning message, notification, and so on. If the content was found to be non-malicious, then the enabler shall not screen the content but continue with its normal flow of operation.

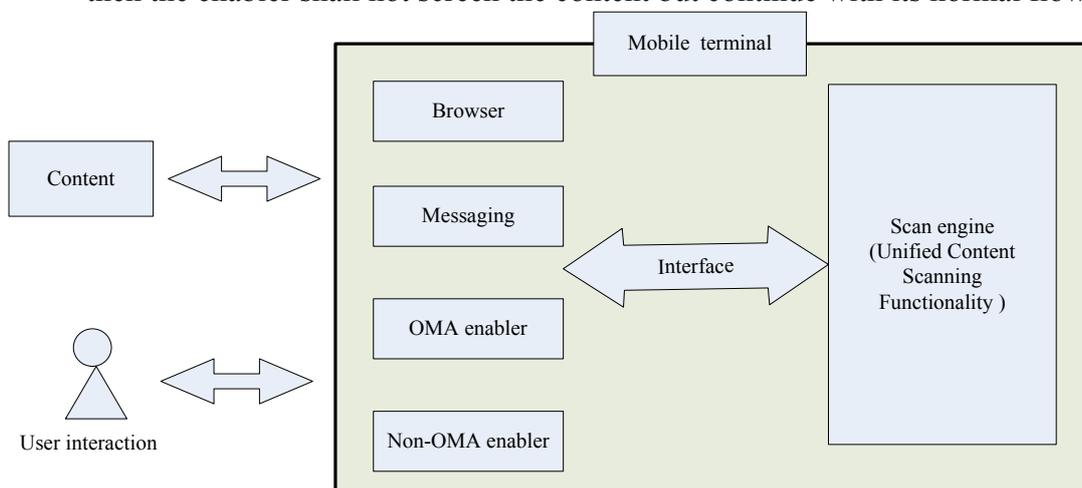


Figure I-3 Client Side Content Screening Framework

-Categorization based content screening

The aim of the Categorization Based Content Screening (CBCS) Enabler in [b-OMA-TS-CBCS] is to screen Content before delivering it to the user, based on Content Categories. The CBCS Enabler can be applied to any Content regardless of the Enabler or protocol that is used to deliver the Content.

The CBCS Enabler consists of two components in [b-OMA-AD-CBCS]: a Content Categorization Component which categorizes Content or Content References, and a Content Screening Component which applies Screening Rules to determine whether the Content should be categorized, modified in any way and delivered.

The Content Categorization Component is mainly responsible for mapping Content and/or Content references (e.g., URI) in the incoming request to a set of Content Categories, and then return the results of category according to a categorization scheme. Examples of existing categorization schemes are the Minimum Recommended Age (MRA), or the Recording Industry Association of America™'s (RIAA) Parental Advisory warning in [b-OMA-TS-CBCS].

The screening step of the Content Screening Component may use following information:

- A Content Category
- The Content source (for example, the URI or the Content owner)
- A CBCS user profile (such as the user's MSISDN, age, preferred and banned type of Content)
- Screening rules

As a result of applying the rules, the content may pass, be blocked, be subject to modification, or be combined with a warning.

-Mobile spam reporting

The purpose of the SpamRep Enabler in [b-OMA-RD-SpamRep] is to provide a mechanism that allows users to designate received content as spam, and then to send a report to an external entity containing information about that content that may be used by the external entity to prevent further instances of unwanted content from reaching users.

The architectural of the SpamRep which was described in [b-OMA-AD-SpamRep] is very simple and consists of only a SpamRep server and a SpamRep client in Figure I-4. In order to submit a spam report or request an action, the SpamRep client interacts with users and possibly various messaging systems. The SpamRep client may be implemented in a mobile device, but messaging servers may implement it as well in order to communicate with a SpamRep server. The SpamRep server is a network entity which receives spam reports and action requests from SpamRep clients. It may interact with various messaging and anti-spam systems.

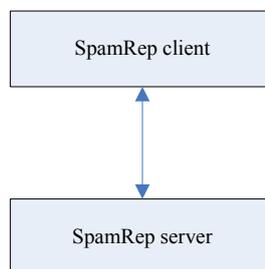


Figure I-4 SpamRep Architectural Diagram

For the Anti-Spam, subscriber's feedback is a very effective, proven method for identifying Spam as long as the feedback contains sufficient information to identify the message source and/or Content.

The Mobile Spam reporting focuses on the Spam Report format and the interface for the delivery of this report. The user's device will be provisioned with the address of the report collection node in the operator's network.

The Mobile Spam reporting defines a common mechanism for Users to report content received by various means as Spam. User creates of Spam Report, reporting Spam to the SpamRep Server By-Reference I, By-Value or By-fingerprint, SpamRep Client may interact message client and integrate the part of the message into a Spam Report. It specifies types and format of messages sent by the User to the SpamRep Server, message system may transfer the Spam report to the SpamRep Server .

The user may queries the SpamRep Server about the status of Spam Reports,and SpamRep Server notifying the Reporter the status of spam report automatically.

A SpamRep Client may inform the SpamRep Server that it has reason to believe that the messaging infrastructure may be blocking and/or quarantining messages inappropriately, and request the SpamRep Server to interact the message box of message system and release any quarantined messages.

When the Spam Report has been processed and per policy, SpamRep Server may notify the Reporter the status of spam report automatically.

A SpamRep Client may inform the SpamRep Server that it has reason to believe that the messaging infrastructure may be blocking and/or quarantining messages inappropriately, and/or that the SpamRep Server should release any quarantined messages. The SpamRep Client sends a Release Quarantine request to the SpamRep Server. On receipt, the SpamRep Server may relay that request to the logical entity (e.g., Messaging Server) over MSS-2, where the quarantined messages are managed. The SpamRep Server may identify the Spam message Box type and user's subscription, and send an "Update Spam message status" request to the Messaging System by reusing the interface of Message Box (e.g. MMS Box, PoC Box). The Messaging System responds with a status message to the SpamRep Server. The SpamRep Server responds with a status message, optionally indicating any actions of the Messaging System.

-Secure Content Identification Mechanism

The objective of Secure Content Identification Mechanism (SCIDM) Enabler in [b-OMA-RD-SCIDM] is to leverage available identification mechanisms to identify all kinds of content including both premier and user generated content for various applications. That is, this mechanism provides a basic service: a standardized trusted content ID which is a more trusted representation of the content than simply a content name.

The model of the SCIDM framework is shown in Figure I-5 in [b-OMA-AD-SCIDM]. Content Identity Manager (CIM) acts as the SCIDM server residing in the network, in charge of managing content registration, responding to content identity query verification requests, and issuing content ID certificates. The identification client is used to interact with CIM for content identification. The registration client is used for content registration by the content registrant.

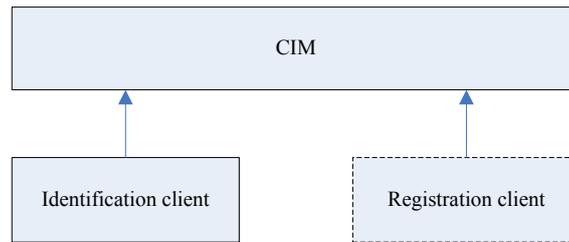


Figure I-5 SCIDM architectural diagram

Secure identification and authentication of digital content of this mechanism would allow secure content transactions between all entities in the service environment, resulting in a more trustworthy transaction environment.

I.2 International activities on countering messaging spam

I.2.1 ITU WSIS thematic meeting on countering messaging spam

ITU WSIS thematic meeting on countering spam was held in Geneva, 7-9 July 2004. Around 200 participants took part in the meeting, representing a range of government policy-makers and regulators, international and intergovernmental organizations, consumer groups, representatives of Internet service providers, ICT companies, academics, civil society organizations and others. Dr. Robert Horton, Acting Chair, Australian Communications Authority chaired the Workshop.

In the meeting, many issues were discussed, including the scope of the problem, technical solutions, consumer education and awareness, spam legislation and enforcement, multilateral and bilateral cooperation, frameworks for international action, and so on.

[Editor's Note]: Have to add more meeting information.

I.3 List of industry alliances and initiatives for countering messaging spam

I.3.1 Countering messaging spam Alliance of ISC (Internet Society of China)

This Alliance was established by Internet Society of China in July 17, 2008. The leaders of Ministry of Industry and Information Technology of China attended the establishing meeting. The main internet service providers, internet content providers and so on. A self-discipline convention statement is published in this meeting. All of the members in this alliance promised to constrain their actions to anti spam messaging in their operating process.

12321 is a running spam reporting centre in China, everybody could report spam information to this centre by web (www.12321.cn), by Wap (wap.12321.cn), by call(010-12321), by SMS(12321) or by email(abuse@12321.cn). On the website of 12321, the newest spam information will be published in time. The 12321 spam message reporting centre is a part of Countering messaging spam Alliance of ISC.

[Editor's Note]: Have to add more activities information.

Appendix II

Current status analysis of messaging spam

(This appendix does not form an integral part of this Recommendation)

Mobile phones have become a fundamental part of personal communications, far more pervasive than personal computers, inherently more portable than other communications devices and enabling an “always on” user experience. Mobile devices now provide not only the communication channel between friends, family and colleagues but also an immediate and personalized channel for businesses to address consumers directly.

Just as PC users struggle with Spam filling their inboxes, unwanted text messages are becoming a growing nuisance in the mobile world and will continue to do so. The problem is smaller in scale on the mobile network but remains substantial, with mobile operators reporting that the average user already receives about five Spam SMS messages per week. The graphical interest of multimedia messages could multiply the problem exponentially.

Mobile messaging provides an ideal model for targeted advertising campaigns but is also open to abuse through indiscriminate advertising, proliferation of scam schemes and falsification of message parameters.

Global SMS Spam levels are on the rise. Operators are under pressure to maintain the quality of service on their networks to ensure satisfaction levels remain high for their customers. The challenge of controlling Spam coming in from other countries is a major issue as extremely low SMS prices means Spammers can target consumers outside their own nation.

The low cost of sending and receiving text messages is one of the most important factors behind high Spam levels in Southeast Asia and China. SMS prices in the Asia/Pacific region are the lowest in the world. In China, the average subscriber receives between six and ten SMS Spam messages a day. Many analysts have revised their SMS forecasts for Asia/Pacific as many operators offer big bundle SMS deals to retain their existing subscribers and acquire new customers.

[Editor’s Note]: Have to add some MMS status description. The description in this clause only includes the SMS.

Bibliography

- [b-ITU-T Resolution 51] ITU-T Resolution 51(Oct. 2004), *Combating spam*
- [b-ITU-T Resolution 52] ITU-T Resolution 52(Oct. 2004), *Countering spam by technical means*
- [b-ITU-T Resolution 52] ITU-T Resolution 52(Oct. 2008), *Countering and combating spam*
- [b-3GPP TS 33.200] 3GPP TS 33.200, *3G Security; Network Domain Security (NDS); Mobile Application Part (MAP) application layer security*
- [b-3GPP TS 33.204] 3GPP TS 33.204, *3G Security; Network Domain Security (NDS); Transaction Capabilities Application Part (TCAP) user security*
- [b-3GPP TR 23.840] 3GPP TR 23.840, *Technical Specification Group Core Network and Terminals; Study into routeing of MT-SMs via the HPLMN*
- [b-3GPP TR 33.937] 3GPP TR 33.937, *Technical Specification Group Services and System Aspects; Study of Mechanisms for Protection against Unsolicited Communication for IMS (PUCI)*
- [b-3GPP TR 33.cde s3-091238] 3GPP TR 33.cde s3-091238 (1000), *Study of Different SPAM Protection Mechanisms: Protection against SMS and MMS SPAM*
- [b-OMA-AD-Client_Side_CS_FW] OMA-AD-Client_Side_CS_FW-V1_0-20070614-A, *Client Side Content Screening Framework Architecture*
- [b-OMA-RD-Client_Side_CS_FW] OMA-RD-Client_Side_CS_FW-V1_0-20070614-A, *Client Side Content Screening Framework Requirements*
- [b-OMA-TS-Client_Side_CS_FW] OMA-TS-Client_Side_CS_FW-V1_0-20070614-A, *Client Side Content Screening Framework Specification*
- [b-OMA-AD-CBCS] OMA-TS-CBCS-V1_0-20090710-C, *Categorization Based Content Screening Framework Architecture*”, “*Categorization Based Content Screening*
- [b-OMA-RD-CBCS] OMA-RD-CBCS-V1_0-20081014-C, *Categorization Based Content Screening Framework Requirements*
- [b-OMA-TS-CBCS] OMA-TS-CBCS-V1_0-20090710-C, *Categorization Based Content Screening*
- [b-OMA-AD-SpamRep] OMA-AD-SpamRep-V1_0-20100420-C, *Mobile Spam Reporting Architecture*
- [b-OMA-RD-SpamRep] OMA-RD-SpamRep-V1_0-20090811-C, *Mobile Spam Reporting Requirements*
- [b-OMA-AD-SCIDM] OMA-AD-SCIDM-V1_0-20090728-C, *Secure Content Identification Mechanism Architecture*
- [b-OMA-RD-SCIDM] OMA-RD-SCIDM-V1_0-20081216-C, *Secure Content Identification Mechanism Requirements*
-