Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1234

(01/2022)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Sécurité du cyberespace – Lutte contre le spam

Lignes directrices relatives à la lutte contre le spam envoyé par le service de messagerie multimédia

Recommandation UIT-T X.1234

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS (1)	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile (1)	X.1140–X.1149
Sécurité des applications (1)	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le spam	**X.1230–X.1249**
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS (2)	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1319
Sécurité des réseaux électriques intelligents	X.1330–X.1339
Courrier certifié	X.1340–X.1349
Sécurité de l'Internet des objets (IoT)	X.1350–X.1369
Sécurité des systèmes de transport intelligents	X.1370–X.1399
Sécurité de la technologie des registres distribués (DLT)	X.1400–X.1429
Sécurité des applications (2)	X.1450–X.1459
Sécurité de la toile (2)	X.1470–X.1489
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Échange concernant les vulnérabilités/les états	X.1520–X.1539
Échange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Échange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Échange garanti	X.1580–X.1589
Cyberdéfense	X.1590–X.1599
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	X.1640–X.1659
Mise en œuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699
COMMUNICATIONS QUANTIQUES	
Terminologie	X.1700–X.1701
Générateur quantique de nombres aléatoires	X.1702–X.1709
Cadre de sécurité pour les réseaux QKDN	X.1710–X.1711
Conception de la sécurité pour les réseaux QKDN	X.1712–X.1719
Techniques de sécurité pour les réseaux QKDN	X.1720–X.1729
SÉCURITÉ DES DONNÉES	
Sécurité des mégadonnées	X.1750–X.1759
Protection des données	X.1770–X.1789
SÉCURITÉ IMT-2020	X.1800–X.1819

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1234

Lignes directrices relatives à la lutte contre le spam envoyé par le service de messagerie multimédia

Résumé

La présente Recommandation UIT-T X.1234 contient des lignes directrices relatives à la lutte contre le spam par le service de messagerie multimédia (MMS). Elle analyse les scénarios types, les caractéristiques et les méthodes de reconnaissance du spam par MMS et propose un cadre technique, des procédures et un certain nombre de technologies essentielles pour la reconnaissance du spam par MMS, afin d'aider les fournisseurs et les utilisateurs de MMS à lutter contre le spam.

Historique

Édition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	UIT-T X.1234	07-01-2022	17	11.1002/1000/14796

Mots clés

Service de messagerie multimédia (MMS), spam par MMS, cadre technique.

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et on considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets ou par des droits d'auteur afférents à des logiciels, et dont l'acquisition pourrait être requise pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas des renseignements les plus récents, il est vivement recommandé aux développeurs de consulter les bases de données appropriées de l'UIT-T disponibles sur le site web de l'UIT T à l'adresse http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Introduction

Le service de messagerie multimédia (MMS) est un moyen usuel d'échanger des messages comprenant du contenu multimédia entre téléphones mobiles, par le biais d'un réseau cellulaire. Les utilisateurs et les fournisseurs peuvent employer les termes d'image, de vidéo, d'audio, d'animation, et autre pour désigner ce type de message. Porté par le développement des technologies de télécommunication et la popularité des smartphones, le MMS est devenu un moyen courant d'envoyer des messages, en particulier chez les jeunes, tandis que les médias l'utilisent à des fins commerciales pour diffuser des informations et des contenus de divertissement. Facilitant le contact social et offrant une grande richesse de contenu, le service MMS est également apparu comme un moyen, pour les spammeurs, d'envoyer du spam. Ce spam par MMS, qui peut contenir des publicités non sollicitées, des informations frauduleuses ou des virus, est en passe de devenir un problème de grande ampleur et entraîne des pertes de recettes pour les opérateurs de télécommunication, les fournisseurs de service et les utilisateurs dans le monde entier.

La lutte contre le spam par MMS est ainsi devenue un axe important dans le domaine des technologies de lutte contre le spam.

Recommandation UIT-T X.1234

Lignes directrices relatives à la lutte contre le spam envoyé par le service de messagerie multimédia

1 Domaine d'application

La présente Recommandation fixe un cadre technique pour lutter contre le spam par MMS, dans le but de parvenir à régir et réduire le spam par MMS. Ce cadre spécifie des composantes fonctionnelles, des procédures et un certain nombre de technologies clés de la reconnaissance du spam par MMS. La présente Recommandation présente en outre des scénarios types de spam par MMS, ainsi qu'une analyse des différents types de spam par MMS et de leurs caractéristiques générales.

Il convient de noter que toutes les opérations décrites dans la présente Recommandation doivent être autorisées par les utilisateurs et les règlements administratifs. L'ensemble des processus antispam doit être rigoureusement conforme aux dispositions de la législation applicable, afin de ne pas enfreindre le droit à la vie privée de l'abonné.

2 Références

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Au moment de la publication, les éditions indiquées étaient en vigueur. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

[UIT-T X.1231] Recommandation UIT-T X.1231 (2008), *Stratégies techniques de lutte contre le spam*.

[UIT-T X.1247] Recommandation UIT-T X.1247 (2016), *Cadre technique de lutte contre le spam publicitaire sur les applications mobiles*.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 service de messagerie multimédia MMS [UIT-T X.1231]: type de service de messagerie postérieur au service de messages courts (SMS) qui permet de transférer divers messages multimédias contenant des données textuelles, graphiques, audio, vidéo, etc., via un réseau mobile, hertzien ou fixe.

3.1.2 spam acheminé par le service de messagerie multimédia (MMS) [UIT-T X.1247]: spam envoyé par MMS.

3.1.3 spammeur [UIT-T X.1231]: entité ou personne qui crée et envoie des spams.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit le terme suivant:

3.2.1 fonctions d'identification du spam par MMS (MMSSIF): système de lutte contre le spam par MMS, qui est indépendant d'un centre de service de messagerie multimédia (CSMM) et comprend

les composantes fonctionnelles suivantes: fonction de surveillance, fonction d'acquisition de données, fonction de prétraitement, fonction de reconnaissance, fonction de vérification, fonction de distribution et fonction de gestion de système.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

ASR reconnaissance automatique de la parole (*automatic speech recognition*)

MMS service de messagerie multimédia (*multimedia messaging service*)

MMSC centre du service de messagerie multimédia (*multimedia messaging service centre*)

MMSSIF fonction d'identification du spam envoyé par le service de messagerie multimédia (*multimedia messaging service spam identification function*)

SMS service de messages courts (*short message service*)

UICC carte à circuit intégré universelle (*universal integrated circuit card*)

URL localisateur uniforme de ressources (*uniform resource location*)

5 Conventions

La présente Recommandation utilise les conventions suivantes:

Le terme "**devrait**" indique une exigence qui est recommandée mais qui n'est pas absolument nécessaire. Cette exigence n'est donc pas indispensable pour déclarer la conformité.

Le terme "**pourra**" indique une exigence optionnelle qui est admissible, sans pour autant être en quoi que ce soit recommandée.

Dans le corps de la présente Recommandation, le mot "**peut**" apparaît à quelques occasions. Il doit alors être interprété comme "**est en mesure de**".

6 Vue d'ensemble

Le terme de service de messagerie multimédia (MMS) désigne un type de service de messagerie postérieur au service de messages courts (SMS), qui permet de transférer divers messages multimédias contenant des données textuelles, audio et vidéo via des réseaux mobiles ou IP. Porté par le développement rapide des technologies Internet et des télécommunications et la popularité croissante des smartphones, le MMS, outil pratique et ludique de contact social, est devenu un moyen répandu d'envoyer des messages, en particulier chez les jeunes et pour les médias, ces derniers l'utilisant à des fins commerciales pour diffuser des informations et des contenus de divertissement.

Malheureusement, les spammeurs ont également adopté cette technologie pour envoyer du spam par MMS. Ce spam par MMS, qui peut contenir des publicités non sollicitées, des informations frauduleuses ou des virus, est en passe de devenir un problème de grande ampleur et entraîne des pertes de recettes pour les opérateurs de télécommunication, les fournisseurs de services et les utilisateurs dans le monde entier. La recherche de techniques efficaces pour lutter contre le spam par MMS est ainsi devenue un défi important dans le domaine de la lutte contre le spam.

7 Scénarios et caractéristique du spam par MMS

Comme l'indique la Figure 7-1, la procédure d'envoi d'un MMS comporte trois étapes principales: (1) l'expéditeur prépare du contenu MMS et l'envoie au centre MMSC dont relève sa carte à circuit intégré universelle (UICC); (2) le centre MMSC reçoit le contenu MMS envoyé par l'expéditeur et décide si ce MMS doit être envoyé au centre MMS suivant ou directement au destinataire; (3) le destinataire reçoit le MMS d'un centre MMSC qui peut être différent du centre MMSC utilisé par l'expéditeur.

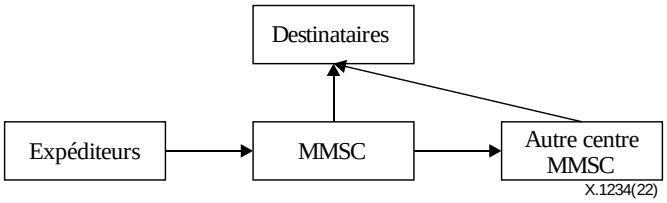


Figure 7-1 – Procédure d'envoi d'un MMS

Les spammeurs emploient la procédure ci-dessus pour envoyer du spam aux utilisateurs, entraînant pour ces derniers une nuisance et des pertes potentielles. Le contenu de ces spam peut être publicitaire, frauduleux, etc. Voici quelques scénarios typiques de spam par MMS:

1) Spam frauduleux: ces MMS visent à tromper les destinataires en leur présentant de fausses informations ou en leur faisant croire qu'ils ont peut-être gagné un cadeau. Si le destinataire répond en suivant les instructions, il devra payer pour un service à valeur ajouté fourni par la société fraudeuse à l'origine du message ou y sera abonné.

2) Spam contenant un cheval de Troie: le MMS contient un fichier média contenant un cheval de Troie. Si le destinataire ouvre ce fichier et que son téléphone mobile est vulnérable, l'expéditeur du spam obtient les droits d'administration les plus élevés sur le système du téléphone et peut dérober toutes les données privées du téléphone à l'insu de son propriétaire.

3) Spam contenant un virus: ce MMS peut contenir un fichier de configuration qui ressemble à un fichier normal mais qui est en réalité piégé. Lorsque le destinataire clique sur le fichier pour exécuter la configuration, le virus entreprend de détruire le système du téléphone de différentes manières, habituellement en supprimant rapidement les fichiers ou en les désagrégeant.

4) Publicité non sollicitée: les spams publicitaires par MMS peuvent contenir des offres immobilières ou financières, des propositions de formation, etc. Ils sont envoyés au destinataire sans son autorisation ou sans que celui-ci soit abonné au service. Certains de ces messages sont volontairement trompeurs et peuvent contenir un lien publicitaire camouflé dans l'image ou la vidéo envoyée. Lorsque le destinataire clique sur l'image ou la vidéo, son navigateur web ouvre une page publicitaire.

8 Lignes directrices relatives au cadre technique

8.1 Structure générale

Comme l'indique la Figure 8-1, l'expéditeur envoie un message MMS au centre MMSC et le destinataire télécharge le message MMS depuis un centre MMSC; par conséquent, les centres MMSC stockent tous les messages MMS. Il est donc recommandé de déployer des fonctions d'identification du spam par MMS (MMSSIF) adjacentes aux centres MMSC.

Aucune technologie antispam ne pouvant garantir une précision de 100% et les fonctions MMSSIF nécessitant d'être configurées et gérées hors ligne manuellement, il est nécessaire d'installer des opérateurs de service, comme indiqué à la Figure 8-1.

Il convient en outre de modifier le processus opératoire du centre MMSC initial, de façon qu'il envoie les messages MMS aux fonctions MMSSIF au lieu de les transférer directement au destinataire ou au centre MMSC suivant après réception. Les fonctions MMSSIF évaluent si le message MMS est du spam et transmettent en conséquence des suggestions au centre MMSC. Le centre MMSC décide, en fonction de ces suggestions, s'il poursuit l'envoi du message MMS concerné au destinataire ou au centre MMSC suivant.

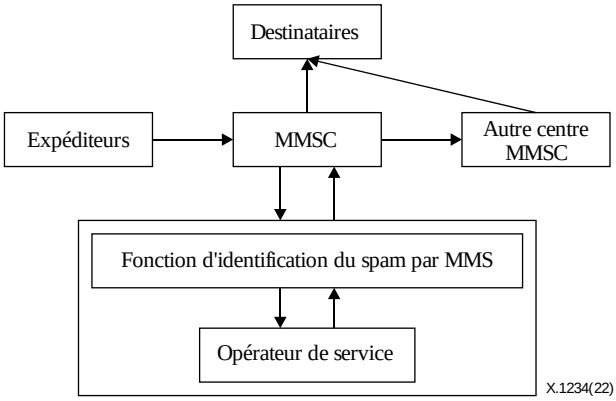


Figure 8-1 – Structure générale de lutte contre le spam par MMS

8.2 Structure de référence des fonctions MMSSIF

La structure de référence des fonctions MMSSIF comprend principalement sept modules correspondant à différentes fonctions: surveillance, acquisition de données, prétraitement, reconnaissance, vérification, distribution et gestion du système. Il est recommandé d'associer différents modules, qui devraient se coordonner en fonction des règles ou politiques définies par les accords pertinents.

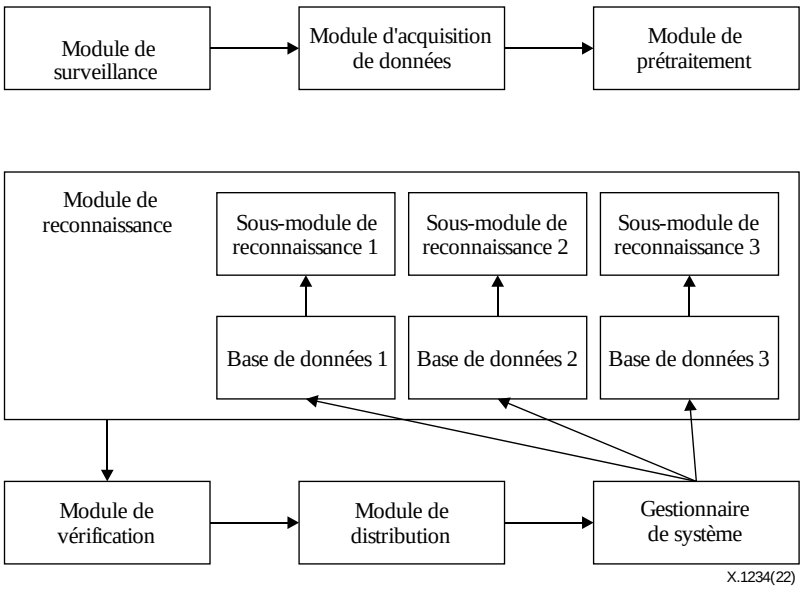


Figure 8-2 – Structure de référence des fonctions MMSSIF

Sur la Figure 8-2, le module de surveillance reçoit un MMS d'un centre MMSC et obtient l'en-tête de ce MMS, qui comprend l'objet, le numéro de téléphone de l'expéditeur, le nombre de pièces jointes, l'URL de ces pièces jointes, etc.

Le module d'acquisition de données reçoit les messages correspondant à l'en-tête MMS envoyés par le module de surveillance, puis il télécharge toutes les pièces jointes à partir des URL.

Le module de prétraitement reçoit tous les messages de ce MMS envoyés par le module d'acquisition de données, à savoir l'en-tête et la totalité des pièces jointes, puis il normalise les messages en leur appliquant des règles. Les messages peuvent provenir de l'en-tête ou du corps du MMS, et les types de ces messages peuvent être textuels, graphique, vidéo, audio, etc., de sorte qu'il est recommandé d'employer des règles composées, par exemple "la source + le type de message + le message".

Le module de reconnaissance reçoit les messages de normalisation envoyés par le module de prétraitement et analyse si le MMS en question est du spam en appliquant des technologies telles que les listes noires, la reconnaissance de texte, la reconnaissance d'image, la reconnaissance vidéo, etc.

Le module de vérification reçoit le résultat putatif envoyé par le module de reconnaissance et y ajoute une évaluation telle que des déterminations manuelles pour réduire la possibilité de faux positifs.

Le module de distribution reçoit le résultat de la reconnaissance envoyé par le module de vérification et traite le MMS qui aura été jugé comme étant du spam, par exemple en le bloquant, en envoyant un avertissement aux spammeurs, etc. Il transmet également le MMS concerné, le journal de distribution et le numéro de téléphone de l'expéditeur au module de gestion du système.

Le module de gestion du système reçoit les dossiers envoyés par le module de distribution et sauvegarde le journal des opérations et le journal du système. Il transfère en outre le numéro de téléphone du spammeur, des mots clés et des images aux différentes bases de données du module de reconnaissance afin de les mettre à jour.

8.3 Composantes fonctionnelles des fonctions MMSSIF

8.3.1 Module de surveillance

Les fonctions du module de surveillance consistent:

- à surveiller l'arrivée d'un nouveau MMS envoyé par le centre MMSC;
- à recevoir le flux de données complet du MMS;
- à analyser le flux de données et obtenir l'en-tête du MMS;
- à transférer l'objet, le numéro de téléphone de l'expéditeur, le nombre et les URL des pièces jointes, et le corps du MMS au module d'acquisition de données.

8.3.2 Module d'acquisition de données

Les fonctions du module d'acquisition de données consistent:

- à recevoir les messages transmis par le module de surveillance et à localiser les URL des pièces jointes;
- à télécharger toutes les pièces jointes;
- à transférer tous les messages du MMS au module de prétraitement, y compris l'en-tête et le corps du MMS, en incluant toutes les pièces jointes.

8.3.3 Module de prétraitement

Les fonctions du module de prétraitement consistent:

- à recevoir tous les messages transmis par le module d'acquisition de données;

- à vérifier toutes les pièces jointes et à évaluer leur nature (texte, image, audio, ou vidéo), car le protocole actuel de transport des MMS stipule que seuls du texte, des images, du contenu audio ou des vidéos peuvent être joints à un MMS;
- à classer les messages selon différents types et à normaliser les messages en leur appliquant des règles, qui peuvent être composées (par exemple "la source + le type de message + le message");
- à transférer le MMS d'origine, tous les messages de normalisation et le numéro de téléphone de l'expéditeur au module de reconnaissance.

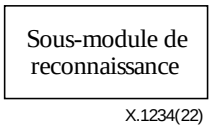
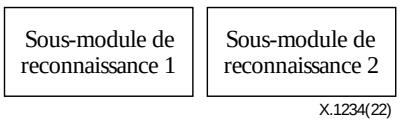
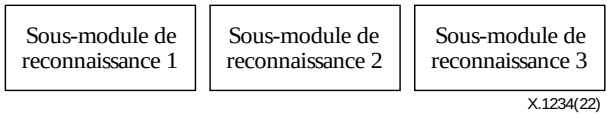
8.3.4 Module de reconnaissance

Les fonctions du module de reconnaissance consistent:

- à analyser si le MMS constitue du spam;
- à envoyer le résultat de reconnaissance au module de vérification.

Il existe trois principaux types de technologies de reconnaissance, qui s'appliquent aux différentes parties d'un MMS. La première s'appuie sur le numéro de téléphone, comme dans le cas des listes noires et des listes blanches. La deuxième s'appuie sur le texte, comme dans le cas de la reconnaissance de texte. La dernière s'appuie sur les pièces jointes, comme dans le cas de la reconnaissance d'image ou de vidéo, par exemple. Selon les exigences spécifiques et les caractéristiques du fournisseur de services, le module de reconnaissance peut déployer un sous module différent en fonction du type de technologies.

Tableau 8-1 – Modèle de configuration du module de reconnaissance

Modèle	Description
Modèle 0	 Le modèle 0 compte un seul sous-module et emploie un type de technologie de reconnaissance.
Modèle 1	 Le modèle 1 est une forme qui associe un sous-module 1 et un sous module 2 configurés ensemble. Le sous-module 1 et le sous-module 2 peuvent être de deux types quelconques choisis parmi les trois types.
Modèle 2	 Le modèle 2 est une forme qui associe un sous-module 1, un sous-module 2 et un sous-module 3 configurés ensemble.

Des modes de calcul différents peuvent s'appliquer au résultat de reconnaissance dans le modèle 1 et le modèle 2. Par exemple, dans le modèle 1, le sous-module de reconnaissance 1 met en œuvre une reconnaissance de texte et le sous-module 2 une reconnaissance d'image. Le sous-module de reconnaissance 1 détermine qu'un MMS est du spam, mais le sous-module de reconnaissance 2 ne le reconnaît pas comme du spam. La reconnaissance du spam nécessite donc de déployer une stratégie

globale au niveau du module de reconnaissance. Il est recommandé de configurer la stratégie en fonction de la situation et des besoins réels.

8.3.5 Module de vérification

Les fonctions du module de vérification consistent:

- à recevoir les résultats putatifs envoyés par le module de reconnaissance;
- à effectuer une évaluation supplémentaire, par exemple une détermination manuelle.

8.3.6 Module de distribution

Les fonctions du module de distribution des données consistent:

- à recevoir le résultat envoyé par le module de vérification;
- à traiter le MMS en fonction du résultat de reconnaissance, qui permet de décider si le MMS est du spam;
- à envoyer la décision de distribution au module de gestion du système si le MMS est reconnu comme étant du spam;
- à envoyer le MMS d'origine au centre MMSC s'il n'est pas reconnu comme étant du spam.

8.3.7 Module de gestion du système

Les fonctions du module de gestion du système consistent:

- à sauvegarder le journal des opérations et le journal système;
- à mettre à jour les bases de données;
- à recevoir les commentaires des utilisateurs.

8.4 Modèle de référence

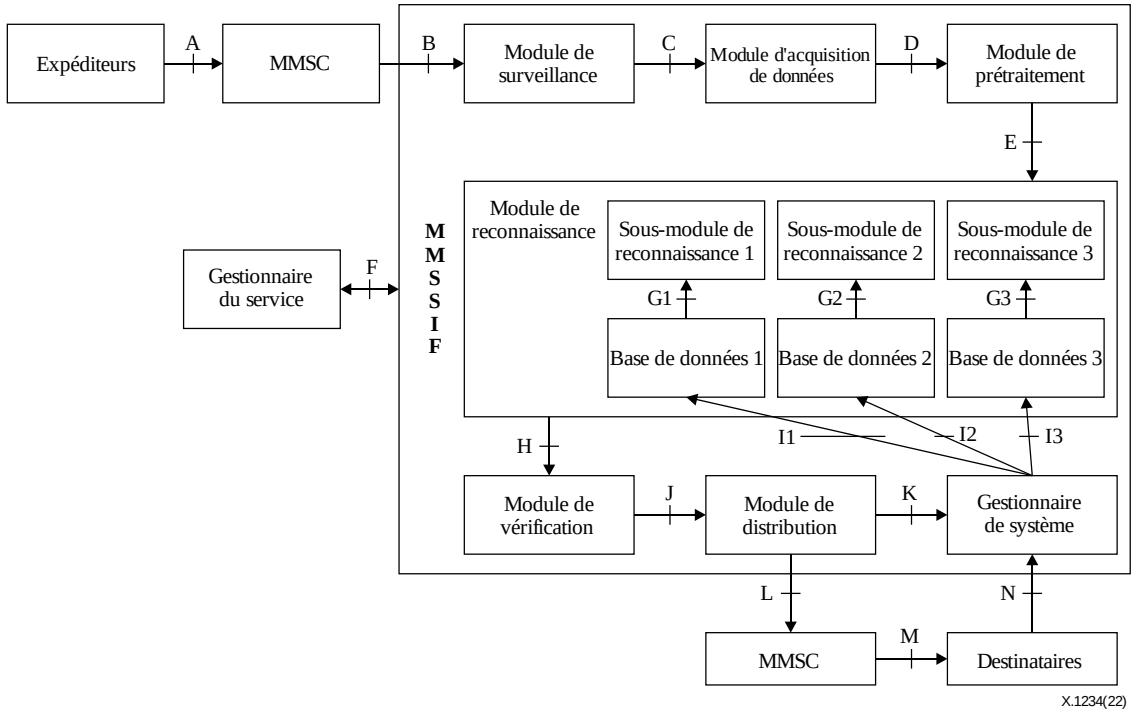


Figure 8-3 – Modèle de référence pour la lutte contre le spam par MMS

L'interface A est située entre les expéditeurs et le centre MMSC. Elle assure la transmission des MMS au centre MMSC. Cette interface est déjà en place lorsque le fournisseur de service commence à

assurer le service de messagerie multimédia aux utilisateurs. Elle n'a pas besoin de changer dans ce modèle.

L'interface B est située entre le centre MMSC et le module de surveillance. Il s'agit d'une nouvelle interface qui sert à transmettre le MMS au module de surveillance au lieu de le transférer directement au destinataire ou au centre MMSC suivant.

L'interface C est située entre le module de surveillance et le module d'acquisition de données. Elle est utilisée pour transmettre l'en-tête du MMS, le numéro de téléphone de l'expéditeur, l'URL, etc., issus de l'analyse par le module de surveillance.

L'interface D est située entre le module d'acquisition de données et le module de prétraitement. Elle est utilisée pour transmettre tous les messages: en-tête du MMS, corps du MMS, objet, totalité des pièces jointes, etc.

L'interface E est située entre le module de prétraitement et le module de reconnaissance. Elle est utilisée pour transmettre les messages de normalisation, par exemple "la source + le type de message + le message". Cette interface doit prendre en charge les protocoles FTP et HTTP.

L'interface F est située entre l'opérateur de service et les fonctions MMSSIF. Elle est utilisée pour transmettre les règles de configuration et les statistiques relatives aux spams.

L'interface G est située entre la base de données et le sous-module. Il ne s'agit pas d'une interface spécifique. L'interface G représente une classe d'interfaces situées entre les différentes bases de données et le sous-module de reconnaissance correspondant. Elle est utilisée pour transmettre le numéro de téléphone, le texte, l'image, etc., suspect qui sont identifiés dans la base de données pour reconnaître le spam.

L'interface H est située entre le module de reconnaissance et le module de vérification. Elle est utilisée pour transmettre le résultat putatif et le MMS d'origine.

L'interface I est située entre le module de gestion du système et la base de données. Comme l'interface G, l'interface I n'est pas spécifique et elle représente une classe d'interfaces situées entre les différentes bases de données et le module de gestion du système.

L'interface J est située entre le module de vérification et le module de distribution. Elle est utilisée pour transmettre le résultat de reconnaissance et le MMS d'origine.

L'interface K est située entre le module de distribution et le module de gestion du système. Elle est utilisée pour transmettre le numéro de téléphone de l'expéditeur, le résultat de la reconnaissance, la décision de distribution et le MMS d'origine.

L'interface L est située entre le module de distribution et le centre MMSC. Elle est utilisée pour transmettre le MMS d'origine, quand celui-ci n'a pas été reconnu comme du spam.

L'interface M est située entre le centre MMSC et les destinataires. Elle est utilisée pour transmettre les MMS aux destinataires. Cette interface est déjà en place lorsque le fournisseur de service commence à assurer le service de messagerie multimédia aux utilisateurs et n'a pas besoin de changer dans ce modèle.

L'interface N est située entre les destinataires et le module de gestion du système. Elle est utilisée pour transmettre les commentaires envoyés par les destinataires.

9 Procédures de travail

La Figure 9-1 montre que douze procédures doivent être appliquées en vue de contrer le spam par MMS. Ces procédures constituent un système adaptatif, qui contribue à l'optimisation de la qualité de fonctionnement du système.

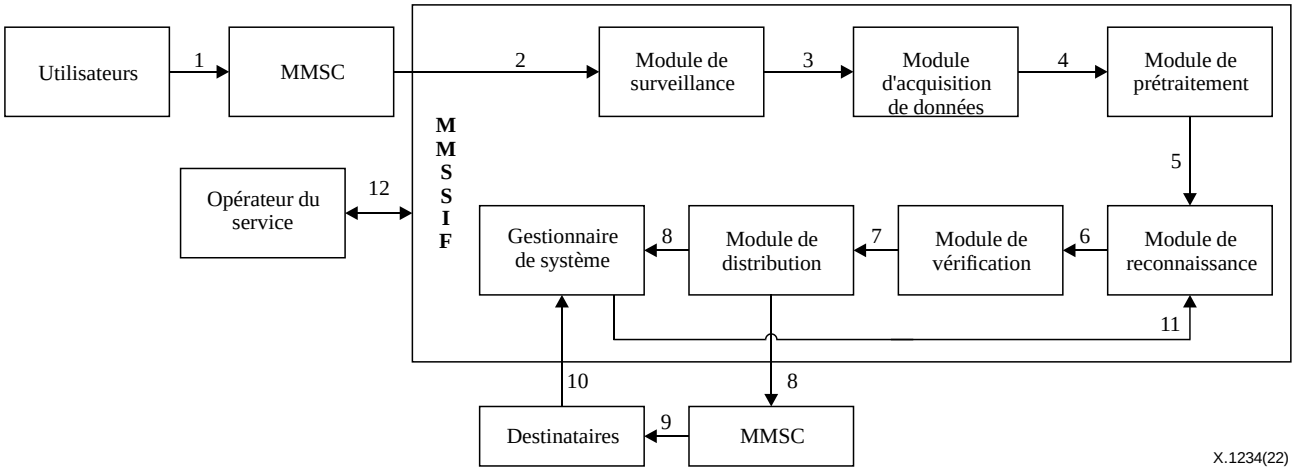


Figure 9-1 – Procédures de traitement destinées à contrer le spam par MMS

Procédure 1: Envoi du MMS au centre MMSC

L'expéditeur prépare le contenu du MMS, le numéro de téléphone du destinataire puis envoie le MMS au centre MMSC.

Procédure 2: Transfert du MMS au module de surveillance

Le centre MMSC reçoit le message MMS envoyé par le centre MMSC et le transfère directement au module de surveillance.

Procédure 3: Obtention de l'en-tête du MMS

Le module de surveillance surveille en permanence l'envoi de nouveaux MMS par le centre MMSC. Dès la détection d'un nouveau MMS, il reçoit l'intégralité du flux de données du MMS et analyse celui-ci afin de récupérer l'en-tête du MMS, qui comprend l'objet, le numéro de téléphone de l'expéditeur et le nombre de pièces jointes ainsi que leur URL. Le module de surveillance envoie ensuite tous les messages au module d'acquisition de données.

Procédure 4: Téléchargement de toutes les pièces jointes

Le module d'acquisition de données reçoit les messages transférés par le module de surveillance, il localise l'URL des pièces jointes et télécharge ces dernières. Lorsqu'il a obtenu la totalité des messages du MMS, le module d'acquisition de données les transfère au module de prétraitement.

Procédure 5: Normalisation des messages du MMS

Le module de traitement vérifie toutes les pièces jointes et évalue leur nature (texte, image, audio, ou vidéo), après réception des messages transférés par le module d'acquisition de données. Si tous les messages sont licites, le module de prétraitement les classe selon leur type et les normalise en fonction des règles. Il transfère ensuite le MMS d'origine, tous les messages de normalisation et le numéro de téléphone de l'expéditeur au module de reconnaissance.

Procédure 6: Analyse du MMS

Le module de reconnaissance analyse si le MMS constitue du spam, en exécutant différentes technologies qui sont déployées dans le système pratique. Il transfère ensuite le résultat putatif au module de vérification. Hormis dans le cas de technologies spécifiques, le module de reconnaissance doit disposer de stratégies globales pour pouvoir obtenir le résultat putatif final.

Procédure 7: Évaluation complémentaire

Le module de vérification effectue une évaluation complémentaire après réception des résultats putatifs transmis par le module de reconnaissance, puis il envoie le résultat de reconnaissance au module de distribution.

Procédure 8: Distribution du MMS

Le module de distribution traite le MMS en fonction du résultat de la reconnaissance. Si le MMS a été reconnu comme étant du spam, le module de distribution traite le MMS suivant les règles établies, par exemple en le bloquant, en envoyant un avertissement aux spammeurs, etc. Il transmet également le MMS d'origine, le journal de distribution et le numéro de téléphone de l'expéditeur au module de gestion du système. Le destinataire ne reçoit pas ce MMS. Si le MMS n'est pas reconnu comme spam, le module de distribution le transmet dans son état d'origine au centre MMSC.

Procédure 9: Envoi du MMS au destinataire

Le centre MMSC envoie le MMS au destinataire. Il peut parfois le transférer à un autre centre MMSC, puis l'envoyer au destinataire. Cette procédure est identique à la procédure antérieure, avant le déploiement de fonctions MMSSIF.

Procédure 10: Commentaires des destinataires

Les destinataires, en tant que victimes potentielles de spam, peuvent envoyer volontairement des commentaires au module de gestion du service. La participation des destinataires sera utile pour lutter efficacement et rationnellement contre le spam. Par conséquent, il est recommandé que le module de gestion du système utilise les commentaires des destinataires pour la mise au point de solutions ou de stratégies de lutte contre le spam.

Procédure 11: Mise à jour des bases de données

Le module de gestion du système sauvegarde le journal des opérations, le journal système et le MMS d'origine. Il actualise également les bases de données pour consigner les nouveaux échantillons, le numéro de téléphone, les mots clés, etc.

Procédure 12: Ajustement des mesures prises pour lutter contre le spam

En fonction des statistiques sur les spams ainsi que du rapport sur l'analyse des spams communiqués par les fonctions MMSSIF, l'opérateur du service évalue l'efficacité des fonctions MMSSIF, en vue d'éventuelles améliorations. En fonction des résultats de cette évaluation, les mesures et les stratégies pourront être adaptées et les mécanismes de collaboration du module de reconnaissance pourront être modifiés par l'opérateur du service.

10 Lignes directrices concernant les technologies clés

Le système de messagerie multimédia MMS permet de transférer divers types de messages multimédia, qui peuvent contenir des images, du texte, du contenu audio ou vidéo, etc. Par conséquent, les technologies clés de reconnaissance destinées à lutter contre le spam par MMS sont principalement la reconnaissance d'image, la reconnaissance de texte, la reconnaissance vidéo, la reconnaissance audio, etc.

10.1 Liste de filtrage antispam

Les listes de filtrage antispam sont les listes noires, les listes blanches et les listes "ambigües". Les fournisseurs de services devraient configurer les fonctions MMSSIF pour qu'elles consignent les activités suspectes ou, à titre d'option, les configurer de manière automatique (par exemple, blocage des MMS suspects, envoi des MMS normaux) pour qu'elles utilisent une liste noire ou une liste blanche. Les fournisseurs de services devraient également tenir les listes à jour pour assurer la disponibilité des fonctions MMSSIF et leur fonctionnement stable. Lorsque des anomalies sont détectées pour un numéro de téléphone non listé, le numéro de téléphone devrait être transféré au service de vérification manuelle qui procèdera à une évaluation complète.

10.2 Reconnaissance d'image

La technologie de reconnaissance d'image extrait en premier lieu une caractéristique permettant de représenter l'image, puis établit une base de données des valeurs propres (eigenvalue) des images. La détection du spam devient alors un problème de classification binaire dans l'espace des caractéristiques, problème qui peut être résolu par apprentissage automatique classique. Ou, plus simplement, si la valeur propre de l'image d'un message MMS est identifiée dans la base de données, le message est reconnu comme étant du spam. Cette méthode est tributaire de la qualité de la base de données des valeurs propres des images.

10.3 Reconnaissance de texte

La reconnaissance de texte consiste principalement en une reconnaissance de mots clés et une reconnaissance sémantique. La reconnaissance de mots clés établit en premier lieu une base de données de mots clés. Si le texte contenu dans un message MMS contient au moins un mot clé recensé dans la base de données, le message est reconnu comme étant du spam. La fonction de reconnaissance de texte peut ensuite construire des modèles logiques booléens et un modèle d'espace vectoriel; après apprentissage, on obtient un modèle de reconnaissance qui peut améliorer la précision de la reconnaissance de texte. Cette méthode dépend de la qualité de la base de données de mots clés.

Les spammeurs ne sont pas à court d'idée pour échapper à la détection. Par exemple, ils falsifient des courriers électroniques normaux et en randomisent le contenu pour éviter la détection des filtres à spam. Par conséquent, si l'on s'appuie sur la reconnaissance de mots-clés, il est très efficace d'avoir recours à une reconnaissance sémantique pour effectuer une reconnaissance secondaire (par exemple, un traitement de la langue naturelle fondée sur une reconnaissance sémantique partielle), laquelle peut fortement réduire le taux de faux positifs.

10.4 Reconnaissance vidéo

En règle générale, la reconnaissance vidéo commence par l'établissement d'une base de données d'échantillons, après quoi la fonction compare chaque élément vidéo d'un message MMS avec les échantillons vidéo pour évaluer s'il s'agit ou non d'un spam. L'identification peut également reposer sur l'extraction de trames clés de la vidéo concernée. Le principe de fonctionnement est le suivant: décodage de la vidéo, traitement en tant qu'ensemble d'images, échantillonnage d'images de l'ensemble, identification des images échantillonnées par une technologie de reconnaissance d'image, puis obtention du résultat de la reconnaissance vidéo à partir du résultat de l'analyse globale des images échantillonnées.

10.5 Reconnaissance audio

Une reconnaissance audio peut être mise en œuvre conjointement à la technologie de reconnaissance vocale automatique (ASR). L'objectif de la technologie ASR est de permettre à des ordinateurs de "dicter" le discours continu complet ou la prononciation de mots clés ou de phrases par des locuteurs différents, et de convertir la "voix" en "texte". Pour identifier des données audio similaires ou identiques, la technologie extrait en outre des caractéristiques spectrales et calcule une empreinte sonore courte et robuste. L'ASR peut ainsi "reconnaître" certains mots clés dans un flux audio et déterminer si ce flux constitue du spam.

10.6 Commentaires des utilisateurs finals

Les commentaires des utilisateurs finals, les conseils de mise en œuvre associés et d'autres informations spécifiées dans le § 8.5 de [UIT-T X.1231] et à l'Annexe A de [UIT-T X.1247] s'appliquent.

Certains utilisateurs finals suppriment directement le spam reçu par MMS et ils sont peu à effectuer un signalement via le canal officiel de retour d'information destiné aux clients. L'efficacité de cette méthode dépend de la bonne volonté et de l'implication des utilisateurs finals. La participation active des utilisateurs finals sera encouragée pour lutter efficacement et rationnellement contre le spam.

Bibliographie

[b-UIT-T X.1240] Recommandation UIT-T X.1240 (2008), *Technologies intervenant dans la lutte contre le spam par courrier électronique.*

[b-UIT-T X.1241] Recommandation UIT-T X.1241 (2008), *Cadre technique pour lutter contre les spams par courrier électronique.*

[b-UIT-T X.1242] Recommandation UIT-T X.1242 (2009), *Système de filtrage du spam du service de messages courts (SMS) fondé sur des règles spécifiées par l'utilisateur.*

[b-UIT-T X.1245] Recommandation UIT-T X.1245 (2010), *Cadre de lutte contre le spam dans les applications multimédias IP.*

[b-UIT-T X.1246] Recommandation UIT-T X.1246 (2015), *Technologies intervenant dans la lutte contre le spam vocal dans les organisations de télécommunication.*

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation et mesures et tests associés
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2022