

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



(43) Date de la publication internationale
27 décembre 2007 (27.12.2007)

PCT

(10) Numéro de publication internationale
WO 2007/147993 A1

(51) Classification internationale des brevets :
H04L 29/06 (2006.01)

(21) Numéro de la demande internationale :
PCT/FR2007/051349

(22) Date de dépôt international : 29 mai 2007 (29.05.2007)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0652575 21 juin 2006 (21.06.2006) FR

(71) Déposant (pour tous les États désignés sauf US) :
FRANCE TELECOM [FR/FR]; 6 place d'Alleray,
F-75015 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants (pour US seulement) : **STEVENS, Fabrice** [FR/FR]; 3 impasse des Chardonnerets, F-78112 Fourqueux (FR). **CHAKRI, Al Mahdi** [MA/FR]; 104 rue de Saint Denis, Appt 113, F-93400 Saint-ouen (FR). **ANSEL, Pierre** [FR/FR]; 34 rue Paul Vaillant Couturier, F-92140 Clamart (FR).

(74) Mandataire : **FRANCE TELECOM/R & D/PIV/BREVETS**; SIMON Viviane, 38/40 rue du Général Leclerc, F-92794 Issy Moulineaux Cedex 9 (FR).

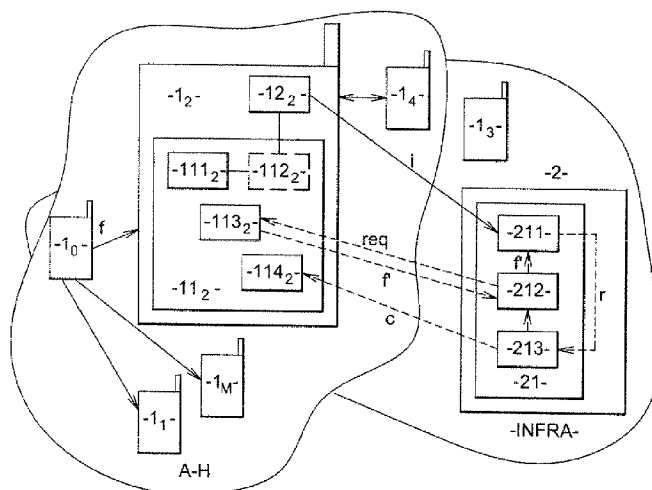
(81) États désignés (sauf indication contraire, pour tout titre de protection nationale disponible) : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) États désignés (sauf indication contraire, pour tout titre de protection régionale disponible) : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL,

[Suite sur la page suivante]

(54) Title: DETECTION AND REACTION TO VIRAL PROPAGATIONS BY AD-HOC NETWORK

(54) Titre : DETECTION ET REACTION AUX PROPAGATIONS VIRALES PAR RESEAU AD-HOC



(57) Abstract: The invention relates to a device and a method of analysis, a device and a method of pre-analysis. In particular, the analysis is a detection of virus propagating in a communication network, in particular an ad-hoc network. In this case, the operator having no knowledge about the traffic, detection cannot be undertaken macroscopically. An object of the invention is a stream (f) analysis device able to communicate with at least one terminal (1₂) exchanging at least one stream (f) with another terminal (1₀) in a communication network (A-H). This analysis device comprises means (211) for analyzing a stream (f) received by a terminal (1₂), said analysis means (211) being able to analyze said stream (f) as function of at least one item of information (i) relating to said stream (f) transmitted by said terminal (1₂) to said analysis device. In a variant of the invention, the analysis device comprises means (213) for controlling a terminal (1₂) that has received this stream (f) as a function of the result (r) of the analysis.

[Suite sur la page suivante]

WO 2007/147993 A1



PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

- avec rapport de recherche internationale
- avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : L'invention concerne un dispositif et un procédé d'analyse, un dispositif et un procédé de pré-analyse. En particulier, l'analyse est une détection de virus se propageant dans un réseau de communication, notamment ad-hoc. Dans ce cas, l'opérateur n'ayant pas connaissance du trafic, la détection ne peut pas être faite de manière macroscopique. Un objet de l'invention est un dispositif d'analyse de flux (f) apte à communiquer avec au moins un terminal (1₂) échangeant au moins un flux (f) avec un autre terminal (1₀) dans un réseau de communication (A-H). Ce dispositif d'analyse comporte des moyens d'analyse (211) d'un flux (f) reçu par un terminal (1₂), lesdits moyens d'analyse (211) étant aptes à analyser ledit flux (f) en fonction d'au moins une information (i) concernant ledit flux (f) transmise par ledit terminal (1₂) audit dispositif d'analyse. Dans une variante de l'invention, le dispositif d'analyse comporte des moyens de commande (213) d'un terminal (1₂) ayant reçu ce flux (f) en fonction du résultat (r) d'analyse.

DETECTION ET REACTION AUX PROPAGATIONS VIRALES PAR RESEAU AD-HOC

L'invention concerne un dispositif et un procédé d'analyse, un serveur l'utilisant, un dispositif et un procédé de pré-analyse, et un terminal l'utilisant. En particulier, l'analyse est une détection de virus se propageant
5 entre terminaux dans un réseau de communication, notamment dans un réseau de communication ad-hoc.

Les techniques de détection de virus, en particulier de propagation de virus dans un réseau de communication, peuvent être, aujourd'hui, divisées
10 en deux familles: les techniques localisées chez l'hôte et les techniques localisées dans le réseau.

Parmi les techniques localisées chez l'hôte existent l'antivirus personnel installé dans le terminal hôte, les coupe-feux (firewall en anglais)
15 personnels... Dans le cas de terminaux, notamment de terminaux mobiles, cette approche présente plusieurs problèmes, notamment:

- des problèmes liés aux capacités de mémoire et de traitement du terminal,
 - des problèmes de non détection (en particulier, lorsque l'antivirus se
20 fonde sur une base de connaissance pour effectuer la détection, seul les virus ayant une signature correspondant à une entrée dans la base de connaissance sont identifiés),
 - le fait que cette technique n'est pas macroscopique et ne permet donc pas de prendre en compte l'évolution du virus dans le réseau.
- 25 Notamment, cette technique ne permettant pas de savoir si le virus se trouve sur de nombreux terminaux et depuis combien de temps il circule dans le réseau, l'éradication complète d'un virus dans le réseau est alors difficile voire impossible à réaliser.

30 Pour permettre une détection macroscopique de virus, les techniques localisées dans le réseau semblent plus appropriées. Parmi ces techniques localisées dans le réseau existent l'antivirus du serveur email capable d'analyse et de détecter les virus dans les emails transitant par le

serveur d'email ainsi qu'éventuellement dans leurs pièces jointes à l'exception des emails cryptés, et aussi, le filtrage d'application, les coupe-feux matériels, les systèmes de détection d'intrusion (IDS pour Intrusion Detection System en anglais), etc. Ces techniques sont déployées dans des réseaux classiques, notamment filaires ou radio, tels que Internet, GSM, GPRS, ou UMTS car elles nécessitent que le réseau possède une infrastructure définie.

Dans le cas de réseaux ad-hoc, tels que les réseaux Bluetooth ou ZigBee, l'opérateur n'ayant pas connaissance du trafic qui circule, la détection des propagations virales ne peut pas être faite de manière macroscopique. En effet, l'opérateur ne peut pas déployer des équipements effectuant de l'analyse et du filtrage de flux.

La présente invention permet de pallier ou, pour le moins, de réduire tout ou partie de ces inconvénients en proposant de transmettre à l'opérateur des informations concernant les flux échangés entre les terminaux afin de permettre l'analyse des flux échangés, notamment la détection de virus dans les fichiers échangés dans ces flux, quel que soit le type de réseau de communication utilisé.

Un objet de l'invention est un dispositif d'analyse de flux. Ce dispositif d'analyse est apte à communiquer avec au moins un terminal échangeant au moins un flux avec un autre terminal dans un réseau de communication. Ce dispositif d'analyse comporte des moyens d'analyse d'un flux reçu par un terminal, lesdits moyens d'analyse étant aptes à analyser ledit flux en fonction d'au moins une information concernant ledit flux transmis par ledit terminal audit dispositif d'analyse. Ainsi, l'opérateur disposant d'un tel dispositif d'analyse de flux est apte à effectuer une détection macroscopique de propagation de virus quel que soit le type de réseaux: réseaux à infrastructure prédéfinie tels que les réseaux filaires (Internet, Intranet...) ou radio (GSM, UMTS...) mais réseaux sans infrastructure préalablement définie, appelés réseaux ad-hoc (Bluetooth, ZigBee...). Un avantage de cette invention est que cette analyse est réalisée de manière centralisée permettant éventuellement une mise à jour simplifiée de l'analyse effectuée (ce qui est d'autant plus sensible lorsque l'analyse est une détection de virus).

Dans une variante de l'invention, le flux reçu analysé par le dispositif d'analyse est un flux reçu par ledit au moins un terminal dans un réseau ad-hoc. Ainsi seuls les flux non analysés par les techniques classiques
5 sont analysés par le dispositif selon l'invention allégeant à la fois le canal montant entre les terminaux et le dispositif d'analyse et la charge de calcul du dispositif d'analyse.

Dans une variante de l'invention, le dispositif d'analyse de flux
10 comporte en outre des moyens de requête auprès d'un terminal permettant au dispositif d'analyse de requérir la récupération de données comportant tout ou une partie prédéterminée dudit flux, ladite au moins une information concernant ledit flux comportant lesdites données récupérées. Ainsi, le dispositif d'analyse a la capacité de récupérer le flux ou le fichier contenu dans
15 ledit flux afin de faire une analyse complète selon les besoins, notamment en fonction du rapport taux d'erreurs d'analyse/charge de calcul du dispositif d'analyse.

Dans une variante de l'invention, le dispositif d'analyse de flux
20 comporte des moyens de commande, lesdits moyens de commande étant aptes à commander au moins un terminal en fonction du résultat fourni par les moyens d'analyse. Notamment, lorsque l'analyse est une détection de virus, si le résultat de l'analyse indique que le flux est vérolé, la commande permet, par exemple, d'effectuer une ou plusieurs des actions suivantes:

- 25 – de supprimer les données du flux stockées dans le terminal,
- d'interdire l'émission dudit flux par ledit terminal
- de corriger ledit flux afin de supprimer le virus dans ledit terminal, notamment en remplaçant tout ou partie dudit flux par des données de remplacement transmises par le dispositif d'analyse audit terminal.

30 Un autre objet de l'invention est un dispositif de détection de virus dans des flux échangés par au moins un terminal avec au moins un autre terminal dans un réseau de communication, ledit dispositif de détection de virus comportant le dispositif d'analyse de flux susmentionné, et lesdits
35 moyens d'analyse étant aptes à détecter un flux vérolé en fonction d'au moins

une information concernant ledit flux transmis par ledit terminal audit dispositif d'analyse.

Un autre objet de l'invention est un serveur dans un réseau de communication comportant au moins un terminal échangeant au moins un flux avec un autre terminal dans un réseau de communication. Le serveur comporte des moyens d'analyse d'un flux reçu par un terminal, lesdits moyens d'analyse étant aptes à analyser ledit flux en fonction d'au moins une information concernant ledit flux transmis par ledit terminal audit serveur.

Un autre objet de l'invention est un dispositif de pré-analyse de flux apte à communiquer avec au moins un dispositif d'analyse. Le dispositif de pré-analyse comporte:

- Des moyens de détection de réception d'un flux par un terminal, ledit terminal échangeant au moins un flux avec un autre terminal dans un réseau de communication;
- Des moyens de communication aptes à émettre au moins une information concernant ledit flux reçu audit dispositif d'analyse.

Un autre objet de l'invention concerne un terminal de communication apte à communiquer avec au moins un dispositif d'analyse, ledit terminal étant apte à échanger au moins un flux avec un autre terminal dans un réseau de communication. Le terminal comporte:

- Des moyens de détection de réception d'un flux par ledit terminal;
- Des moyens de communication aptes à émettre lesdites au moins une information concernant ledit flux reçu audit dispositif d'analyse.

Un autre objet de l'invention concerne un procédé d'analyse de flux échangés entre au moins un terminal et un autre terminal dans un réseau de communication, comportant au moins l'étape suivante consistant à analyser un flux reçu par ledit au moins un terminal en fonction d'une information concernant ledit flux.

Dans une variante de l'invention, l'analyse dudit flux en fonction desdites au moins une information concernant ledit flux comporte une sous

étape consistant à comparer la fréquence de réception d'au moins une information concernant ledit flux d'un type donné sur une plage de temps prédéterminé par rapport à un seuil prédéterminé dont le résultat constitue une condition prédéterminée pour au moins une étape suivante dudit procédé d'analyse. Par type d'information est entendu qu'un type d'information regroupe toutes les informations concernant des flux identiques ou similaires en ce qui concerne l'analyse. Les flux sont identiques ou similaires lorsque les résultats d'analyse seraient identiques si l'analyse était effectuée sur le flux complet. Dans le cas d'une analyse permettant la détection de virus, les informations concernant des flux reçus contenant un fichier par le même virus sont regroupées dans un type, éventuellement y compris lorsque le fichier est légèrement modifié lors de sa propagation mais conserve ses propriétés virales.

Un autre objet de l'invention est un programme d'ordinateur d'analyse comprenant des instructions de code de programme pour l'exécution des étapes du procédé d'analyse susmentionné.

Un autre objet de l'invention est un procédé de pré-analyse de flux échangé entre un terminal et un autre terminal dans un réseau de communication, comportant les étapes suivantes consistant à:

- Détecter la réception d'un flux par ledit terminal,
- Emettre lesdites au moins une information concernant ledit flux à un dispositif d'analyse de flux.

Un autre objet de l'invention est un programme d'ordinateur de pré-analyse comprenant des instructions de code de programme pour l'exécution des étapes du procédé de pré-analyse susmentionné lorsque ledit programme est exécuté sur un ordinateur.

Les caractéristiques et avantages de l'invention apparaîtront plus clairement à la lecture de la description, faite à titre d'exemple, et des figures s'y rapportant qui représentent :

– Figure 1, une représentation schématique d'un système de communication mettant œuvre les dispositifs de pré-analyse et d'analyse selon l'invention,

5 – Figures 2a et 2b, une représentation schématique du procédé mis en œuvre par le système illustrant notamment une première phase d'une variante de l'invention, respectivement du procédé de pré-analyse selon l'invention et du procédé d'analyse selon l'invention,

10 – Figure 3, une représentation schématique du procédé d'analyse illustrant, notamment, une deuxième phase d'une variante de l'invention,

 – Figure 4, une représentation schématique d'un mode de réalisation des moyens d'analyse du dispositif d'analyse selon l'invention,

 – Figure 5, une représentation schématique du procédé d'analyse illustrant, notamment, une troisième phase d'une variante de l'invention.

15 Dans la suite de la description, l'invention sera plus particulièrement expliquée dans le cas où l'analyse comporte la détection de virus dans un flux se propageant dans un réseau pour une meilleure compréhension de celle-ci. L'invention peut néanmoins être mise en œuvre dans tout type d'application pour laquelle une analyse macroscopique des flux se propageant dans un
20 réseau est utile.

 Par analyse d'un flux est entendu, analyse des données transportées par ce flux ainsi que, le cas échéant, toutes autres informations transportées par le flux telles que les informations utiles à la lecture de ce flux:
25 par exemple, champ d'identification des terminaux émetteur et destinataires(s), type de flux, type des données transportées... Dans une variante de l'invention l'analyse du flux comportera uniquement l'analyse des données transportées par ce flux (par exemple, du fichier ou de la trame).

30 La figure 1 illustre un système de communication dans lequel une variante de l'invention est implémentée. Le système de communication comporte plusieurs terminaux de communication $1_0, 1_1, 1_2, 1_3, 1_4, \dots, 1_M$ (M entier > 0) et un opérateur, représenté dans le cadre de cet exemple par un serveur 2. L'opérateur, par le biais du serveur 2, est connecté dans un premier
35 réseau de communication INFRA à un ensemble de ces terminaux $1_0, 1_2, 1_3,$

1₄, etc. de communications du système de communication via une interface de communication. L'interface de communication 12₂ du terminal 1₂ avec le serveur 2 est représentée sur la figure. Ce premier réseau INFRA est un réseau à infrastructure préalablement défini, par conséquent l'interface 12₂ du terminal 1₂ est, par exemple, une interface de type GSM, GPRS, UMTS, IP.

Les interfaces 12₀, 12₃, 12₄ des autres terminaux 1₀, 1₃, 1₄ avec ce serveur 2 ne sont pas représentés mais doivent être considérées comme ayant des fonctions identiques ou équivalentes à l'interface 12₂.

Dans une variante de l'invention, un ensemble des terminaux 1₀, 1₁, 1₁, 1₂, 1₄, ... 1_M du système de communication a la capacité de s'associer à un deuxième réseau A-H. Ce deuxième réseau A-H est soit un autre réseau à structure préalablement défini, soit un réseau ad-hoc tel que représenté sur la figure 1. Ces terminaux sont alors dotés d'une interface (non représentée sur la figure 1) de communication avec le réseau A-H, par exemple une interface Bluetooth.

Au moins une fraction des terminaux 1₀, 1₃, 1₄ en liaison avec le serveur 2 de l'opérateur comporte un dispositif de pré-analyse 11₂ (illustré sur la figure 1 uniquement pour le terminal 1₂, ce qui ne signifie pas que les autres terminaux n'en comportent pas). Ce dispositif d'analyse comporte dans une variante de l'invention, un agent embarqué par le terminal 1₂. Cet agent comporte, par exemple, un programme d'ordinateur apte à remonter des informations i à l'opérateur 2.

Lorsqu'un terminal 1₀ transmet un flux f au terminal 1₂ dans le réseau A-H, le serveur 2 n'a pas connaissance de l'échange et, par conséquent est dans l'incapacité de fournir une analyse du flux f. C'est pourquoi, le dispositif de pré-analyse 11₂ du terminal 1₂ comporte des moyens de détection 111₂. Ces moyens de détection 111₂ détectent la réception d'un flux f par le terminal 1₂. Lorsqu'un flux f reçu a été détecté, les moyens de communication du dispositif de pré-analyse transmettent au serveur 2 une information i concernant le flux f via l'interface 12₂ du terminal.

Dans une variante non illustrée de l'invention, le dispositif de pré-analyse 11₂ est externe au terminal. Dans ce cas, le terminal 1₂ et le dispositif de pré-analyse 11₂ sont connectés pour permettre aux moyens de détection 111₂ de détecter la réception d'un flux f par le terminal 1₂. Le dispositif d'analyse 112 transmet alors l'information i au serveur 2 soit directement via ses moyens de communications (non représentés), soit via l'interface de communication dans le premier réseau INFRA d'un terminal connecté à ce dispositif de pré-analyse. Ainsi, un utilisateur ayant une famille d'objets/terminaux communicants, certains connectés au serveur 2 et d'autres non, dispose du dispositif d'analyse de flux mis à disposition par son opérateur (soit gratuitement, soit par abonnement) pour analyser non seulement les flux de ses objets connectés au serveur 2 mais aussi pour les autres. En outre, l'utilisation d'un dispositif de pré-analyse hors terminaux permet à l'utilisateur d'utiliser un seul dispositif de pré-analyse pour l'ensemble de ses objets communicants.

Dans une variante de l'invention, afin d'éviter une surcharge du premier réseau INFRA, le dispositif de pré-analyse comporte des moyens de réduction 112₂ du flux f reçu. L'information réduite ainsi obtenue est transmise au serveur 2 comme information i concernant ce flux. Cette information réduite peut être une réduction du flux f complet ou seulement d'une ou plusieurs parties de ce flux f, par exemple d'un ou plusieurs fichiers transportés par le flux f. La réduction est obtenue, notamment, par compression ou condensé. Par exemple, l'information i transmise au serveur 2 est soit une partie du flux, soit un condensé (hash en anglais) de tout ou partie du flux (notamment du fichier transporté par le flux), soit une compression de tout ou partie du flux. Les moyens de réduction 112₂ calculent le condensé, par exemple, à l'aide d'un algorithme de hashage tel que SHA-1, SHA-256. L'information ainsi réduite présente un volume moindre que le flux complet et évite la surcharge du canal montant entre les terminaux et le dispositif d'analyse.

Le serveur 2 de l'opérateur comporte un dispositif d'analyse 21. Ce dispositif d'analyse 21 comporte des moyens d'analyse 211 de flux. Ces moyens d'analyse 211 analyse un flux f en fonction d'au moins l'information i concernant ce flux transmise par un terminal 1₂.

Dans une variante de l'invention, ce dispositif d'analyse 21 comporte des moyens de commande 213. Ces moyens de commande 213 commandent au moins un terminal 1_2 ayant reçu le flux f en fonction du résultat r fourni par les moyens d'analyse 211.

Dans une variante de l'invention, le dispositif d'analyse 21 associé à l'opérateur est externe au serveur 2 et communique avec les terminaux 1_0 , 1_3 , 1_4 soit directement, soit via le serveur 2, pour recevoir l'information i , et notamment transmettre au moins une commande c qui est exécutée par des moyens de traitement 114₂.

Les figures 2a et 2b illustrent respectivement le procédé de pré-analyse et le procédé d'analyse selon l'invention.

Un terminal 1_0 envoie un flux f aux terminaux 1_2 , 1_4 , ... 1_M environnants, dans notre exemple, dans le deuxième réseau A-H. Une fraction de ces terminaux dont le terminal 1_2 embarque un agent mettant en œuvre un procédé de pré-analyse. Le procédé de pré-analyse comporte une étape consistant à détecter la réception de flux par le terminal 1_2 . Dans le cas de notre exemple, seuls les flux reçus dans un réseau spécifié: le deuxième réseau, sont détectés, notamment, des réseaux sans infrastructure préalablement définie tels que les réseaux ad-hoc. L'agent ayant constaté la réception du flux f lors de cette étape de détection transmet une information i concernant ce flux à un dispositif d'analyse.

Cette information i comporte soit tout ou au moins une partie du flux f reçu, soit une réduction de tout ou partie du flux f reçu. Dans le cas où i ne comporte pas tout le flux f reçu, une variante de l'invention prévoit que le procédé de pré-analyse comporte une étape de calcul de l'information $i(f)$ concernant le flux déclenché lors de la détection de la réception d'un flux f . Ce calcul est soit l'extraction d'au moins une partie du flux f , soit une réduction du flux f par exemple par hachage.

L'information i est analysée dans un procédé d'analyse. Dans une variante de l'invention suivant le résultat r_1 , r_2 de cette analyse des commandes c sont transmises à au moins un terminal ayant reçu le flux f .

5 Dans le cas où l'analyse comporte la détection de virus dans le flux complet ou dans un ou plusieurs fichiers transportés par le flux: le mobile "attaquant" (terminal 1_0) est infecté, et essaie d'envoyer des fichiers dans un flux f aux mobiles environnants (terminaux 1_2 , 1_4 , ... 1_M). Il envoie avec succès le flux f comportant un fichier à l'utilisateur 1_2 via son interface ad-hoc (non
10 représentée), et envoie un fichier infecté par le même virus ux utilisateurs 1_4 et 1_M de la même manière.

Les terminaux 1_2 et 1_4 embarquent l'agent mettant ainsi en œuvre le procédé de pré-analyse décrit plus haut. Cet agent constate la réception du
15 flux f comportant le fichier, et calcule un condensé de ce fichier, par exemple à l'aide d'un algorithme de hachage (ex : SHA-1, SHA-256) pour fournir une information i comportant ce condensé. Il envoie alors l'information i comportant ce condensé au serveur 2, i.e. l'équipement de l'opérateur mettant en œuvre le procédé d'analyse chargé de l'analyse de ces remontées
20 d'information.

Dans une variante de l'invention, si le résultat de l'analyse est que le fichier est vérolé, le serveur 2 envoie une commande c en réponse à l'agent, l'informant directement que le fichier correspondant est un virus. Cette
25 commande c comporte :

- soit une commande d'action par rapport au virus, auquel cas le terminal, voire l'agent, dispose d'au moins un traitement exécutable à la réception de cette commande d'action (par exemple supprimer le fichier, présentation à l'utilisateur de l'information de la réception d'un
30 fichier vérolé, etc.) ;
- soit le traitement à exécuter par le terminal, voire l'agent embarqué sur le terminal, tels que :
 - Informer l'utilisateur de la réception d'un virus
 - Procéder directement à la suppression du fichier,
 - 35 ○ Interdire la transmission du fichier à un autre terminal,

- Assainir le fichier.

Dans une variante de l'invention, à la première phase correspondant à la mise en œuvre des procédés de pré-analyse et d'analyse décrit plus haut est ajoutée une deuxième phase dans laquelle la fréquence d'apparition d'information i concernant un type de flux sur une plage de temps prédéterminée est calculée pour avoir une vision macroscopique de la propagation lente d'un flux f . Un type de flux regroupe soit un seul et même flux reçu par un ou plusieurs terminaux, soit un flux reçu par un ou plusieurs terminaux éventuellement légèrement modifié. Par légèrement modifié est entendu que la modification du flux n'entraîne pas d'altération de ses propriétés au regard d'une analyse du flux complet (par exemple, lorsque l'analyse est la détection de virus dans un fichier, le fichier légèrement modifié est toujours porteur du même virus, i.e. d'un virus ayant les mêmes effets).

Le procédé d'analyse met alors à jour la fréquence $Freq$ correspondant au type de flux concerné par l'information i , comme le montre la figure 3. Puis le procédé d'analyse compare cette fréquence $Freq$ avec un seuil prédéterminé S .

Dans une variante de l'invention, l'envoi de commandes à au moins un terminal 1_2 ayant reçu le flux f est conditionné au fait que le flux f se propage dans le réseau A-H à une fréquence $Freq$ supérieure à un seuil S .

Dans une variante de l'invention, l'identité Id Term du terminal 1_2 sur lequel la réception du flux f a déclenché la transmission de l'information $i(f)$ est transmise avec l'information i au serveur 2. Une mise à jour de la liste des terminaux $List$ Id ayant reçu un type de flux correspondant au flux f est alors mise à jour en y ajoutant l'identité du terminal 1_2 .

La figure 4 montre un mode de réalisation de ce procédé. Les moyens d'analyse 211 comportent :

- des moyens de calcul et de mise à jour 2111, permettant de calculer la fréquence $Freq$ d'apparition du flux f concerné par l'information i ou au moins d'un flux du même type que le flux f concerné par l'information i , et

- des moyens de comparaison 2113 de cette fréquence Freq à un seuil prédéterminé S.

Dans une variante de l'invention, les moyens d'analyse 211 comportent une table 2112 pour la mise à jour. Dans l'exemple illustré par la figure 4, l'information i est le hash du fichier transporté par le flux f reçu (un type de flux dans cet exemple regroupe un seul et même flux reçu par un ou plusieurs terminaux sans modification) et la Freq est le nombre d'occurrences, i.e. le nombre de fois où l'information i a été remontée au serveur 2. Cette table comporte en outre, dans une variante non illustrée, pour au moins un type de flux la liste des identifiants List Id d'au moins une partie des terminaux ayant reçu ce flux f et ayant directement ou grâce à un dispositif de pré-analyse distinct fait remonter l'information i au serveur 2.

La mise à jour de la fréquence est effectuée d'une des manières suivantes :

Une première méthode comporte le stockage dans une file d'attente associée à un type, des éléments e contenant les estampilles temporelles t_e de réception des informations i. On ne conserve dans la file que les estampilles qui appartiennent à une fenêtre temporelle déterminée de longueur T_F (période d'étude). La fenêtre temporelle pour laquelle on conserve les estampilles temporelles peut être définie soit à partir de l'heure courante t, soit à partir de l'estampille temporelle de l'élément le plus récent introduit dans la file d'attente.

Dans le premier cas, on ne conserve que les éléments e de la file d'attente dont les estampilles temporelles vérifient

$$t - t_e < T_F$$

Dans le deuxième cas, on ne conserve que les éléments e de la file d'attente dont les estampilles temporelles vérifient

$$t_{i+n} - t_e < T_F$$

Le décompte du nombre d'éléments dans chaque file d'attente donne donc une mesure, pour un type donné, du nombre de fichiers transférés dans une fenêtre de temps T_F .

5 Une deuxième méthode comporte l'utilisation d'une moyenne glissante telle que la moyenne EWMA, moyenne glissante pondérée exponentielle (Exponential Weighted Moving Average en anglais).

10 L'intérêt de l'invention étant de déceler les envois répétés d'un flux f ou d'au moins une partie d'un contenu d'un flux f (un fichier notamment) sur une longue durée, la période d'étude sera typiquement de plusieurs jours.

15 Dans le cas de la détection de virus, lorsque la valeur du nombre d'occurrences (la valeur de la fréquence $Freq$) dépasse un seuil S , le dispositif d'analyse conclut que le flux f correspondant à cette information i est suspicieux, et soit agit directement en envoyant une commande c , soit entame une troisième phase pour cette information i .

20 L'intérêt de ne mettre à jour que les fréquences $Freq$ d'apparition d'une information i est que :

- les données stockées sont réduites (d'autant plus si l'information i est une information réduite),
- ces fréquences mettent en évidence des phénomènes de propagation lente de flux, et
- 25 – cela ne nécessite pas le stockage de données individuelles ni même du contenu du flux (en particulier dans le cas d'information réduite obtenue par une fonction non réversible telle que les fonctions de hachage), évitant ainsi des problèmes de violation de règles de droits de vie privé et des libertés individuelles ou publiques telles que les règles de la
- 30 CNIL (Commission Nationale de l'Informatique et des Libertés) en France.

Le calcul des fréquences d'apparition d'une information i ne permet pas de détecter la propagation lente de fichiers légèrement modifiés, car

35 l'information i résultant serait différente. Toutefois, en pratique, tous les virus

développés jusqu'à présent sur téléphone mobile consistent en la propagation de la même pièce jointe, et par conséquent sont détectables par notre mécanisme.

5 Néanmoins, afin de détecter la propagation lente de fichiers légèrement modifiées, une variante de l'invention propose de mettre à jour non pas la fréquence de l'information i mais la fréquence d'un type $\text{Freq}(\text{type}(f))$ de flux concerné par l'information i . En effet, un flux f concerné par une information i_1 peut être de même type qu'un flux f' concerné par une
10 information i_n , car le flux f' est le flux f légèrement modifié. Dans ce cas, i_1 et i_n servent à la mise à jour de la même fréquence Freq correspondant à un type de flux $\text{type}(f)$.

 Dans une variante de l'invention, l'invention propose, outre la
15 première phase précitée ou les deux phases précitées, une troisième phase dans laquelle le procédé d'analyse comporte la récupération du flux en tout ou partie, notamment des fichiers contenus dans ledit flux, concernés par les informations décelées dans la phase précédente, et l'analyse de ces fichiers comme le montre la figure 5. Cette récupération, dans un mode de réalisation
20 particulier est effectuée si une ou plusieurs conditions prédéterminées sont remplies. La récupération des données permet éventuellement de compléter l'analyse faite sur l'information concernant un flux dans des circonstances déterminées. Le fait de limiter la récupération des données à ces circonstances permet de limiter les données sur le canal montant. En effet,
25 par exemple:

- soit cette récupération est effectuée lorsqu'une information concernant un flux donné se propageant dans un réseau de communication est analysée pour la première fois par le dispositif d'analyse. Elle permet éventuellement de s'assurer immédiatement de l'exactitude des
30 résultats avant d'agir en conséquence.
- Soit cette récupération est effectuée en fonction de la fréquence d'analyse d'informations concernant ledit flux. Cela permet d'éviter la remontée systématique du flux lors de la première analyse de l'information concernant le flux et une charge de calcul d'analyse tout

en s'octroyant la capacité de traitement des données récupérées lorsqu'une propagation d'un flux est visible.

- 5 Ainsi, pour une information $i_0(f)$ concernant un flux f , lorsque le résultat r de l'analyse de la phase 1 est un résultat donné r_1 et/ou lorsque la fréquence Freq mise à jour est supérieure au seuil prédéterminé S , si les moyens d'analyse 211 représentés sur la figure 1 (notamment la table 2112 de la figure 4) ne disposent pas de l'identifiant du terminal 1_2 ayant reçu le flux
- 10 f ,
- Lorsqu'un dispositif de pré-analyse 11_n remonte une information i_n concernant un flux f' reçu, vérifier si cette information i_n correspond à une information identique dans l'ensemble des informations $\{i_j\}$ préalablement reçue.
 - 15 ○ Si ce n'est pas le cas, continuer le traitement comme dans la première phase.
 - Si c'est le cas, initier une demande $\text{Req}(f', \text{IdTerm})$ de récupération de données comportant tout ou une partie du flux f' auprès du client IdTerm ayant transmis l'information i_n . Cette
 - 20 étape peut ou non faire intervenir l'utilisateur (i.e., par exemple, lui demander son autorisation).
 - Répéter l'étape précédente jusqu'à récupération d'un de ces flux.
 - Analyser alors les données récupérées, par exemple par des tests par un antivirus, ou par une analyse manuelle plus précise par des
 - 25 personnes (reverse engineering...).

La figure 1 montre un mode de réalisation de la récupération de données. Le dispositif d'analyse 21 comporte des moyens de requête 212 auprès d'un terminal permettant au dispositif d'analyse 21 de requérir req la

30 récupération de données comportant tout ou une partie prédéterminée du flux f .

Le terminal 1_2 comporte des moyens de réponse 113_2 à la requête en récupération. Ces moyens de réponse 113_2 sont soit dans le dispositif de

35 pré-analyse 11_2 , soit externe à celui-ci. Ils reçoivent du dispositif d'analyse 21

une demande req de récupération de données comportant tout ou partie du flux f' en fonction du résultat r fourni par les moyens d'analyse 211 et transmettent aux moyens de requête 212 les données, dans notre exemple le flux f' .

5

Ce point met en évidence un autre intérêt de l'invention. L'analyse directement en fonction du flux complet ou le fichier n'est alors effectuée que lorsqu'il y a intérêt à l'analyse soit par ce que ce type de flux se propage pour la première fois, soit parce que sa propagation commence à être importante voire, soit parce que sa propagation est suspecte (dans le cas d'une détection de virus), soit parce que le résultat r de l'analyse du flux en fonction de l'information i est égal à un résultat donné $r1$ montrant qu'il y a un intérêt à une analyse plus poussée du flux. Cela limite donc les calculs du dispositif d'analyse.

15

Dans une variante de l'invention, si le résultat r de l'analyse des données récupérées sur le flux f' est égale à un résultat donné $r1$ (indiquant dans le cas d'une détection de virus que le fichier est vérolé), une réaction est initiée par une commande c correspondant à une ou plusieurs des réactions suivantes données à titre d'exemples:

20

- Informer tout ou partie des terminaux (notamment des agents) du résultat $r1$ de l'analyse (i.e. de la détection d'un virus dans notre exemple d'application) pour le flux f et, éventuellement, ses versions légèrement modifiées f' . Ces agents pourront alors avertir l'utilisateur lors de la réception du fichier correspondant, ou directement procéder à sa suppression, comme décrit précédemment.
- Fournir à tout ou partie des terminaux (notamment des agents) les moyens d'agir sur le flux f et, éventuellement, ses versions légèrement modifiées f' : par exemple, dans le cas d'une détection de virus, des moyens d'assainir soit en fournissant le remède à exécuter par les terminaux soit des données de remplacement pour remplacer les parties vérolées du flux.

25

30

La partie des terminaux informés ou recevant les moyens d'agir est déterminée soit par localisation physiques ou réseaux des terminaux

35

par rapport au(x) terminal (ux) ayant reçu le flux f, soit en fonction de la station de base de connexion (ceux connectés à la même station sont informés).

- 5
- Mettre à jour, dans le dispositif d'analyse, des données de résultats d'analyse concernant ce type de flux permettant ainsi, lorsqu'un nouveau flux de même type est reçu postérieurement par un terminal, de ne pas nécessiter une nouvelle analyse poussée mais d'obtenir ces informations des l'analyse de la première phase.

10

Si, par contre, les moyens d'analyse 211 représentés sur la figure 1 disposent de l'identifiant du terminal 1₂ ayant reçu le flux f soit parce que transmis avec l'information i et, éventuellement, conservé dans une mémoire tampon des moyens d'analyse 211, soit stocké notamment dans la table 2112

15

- de la figure 4:
- Demander à ce terminal 1₂ ou à l'un des terminaux de la liste List Id de la table 2112 l'envoi des données comportant tout ou une partie du flux f, jusqu'à-ce que l'un d'entre eux l'envoie.
 - Analyser alors les données récupérées comme décrit ci-dessus.

20

Dans une variante de l'invention, si le résultat r de l'analyse des données récupérées sur le flux f est égal à un résultat donné r1 (indiquant dans le cas d'une détection de virus que le fichier est vérolé), une réaction est initiée par une commande c correspondant à une ou plusieurs des réactions

25

mentionnées ci-dessus données à titre d'exemples (les terminaux sont notamment ceux contenus dans la liste list Id).

25

Un mode de réalisation du procédé d'analyse est un programme d'ordinateur mis en œuvre, par exemple, par le serveur 2 qui, lorsqu'il est exécuté, effectue toutes ou parties des étapes décrites précédemment suivant la variante implémentée.

30

L'invention permet ainsi de détecter et, éventuellement, de réagir le cas échéant aux propagations virales dans des réseaux sans infrastructure préalablement définie tels que les réseaux ad-hoc.

35

Dans une variante d'application, le premier et le deuxième réseau sont deux réseaux à infrastructure distincts. Cela permet éventuellement à une personne ayant plusieurs objets communicants dont une partie est
5 supervisée par un premier opérateur et une autre partie par un deuxième opérateur de bénéficier de l'analyse d'un seul opérateur pour tous ses objets.

Dans une autre variante d'application, le premier et le deuxième réseau sont un seul et même réseau à infrastructure. Ainsi, lorsque l'opérateur
10 n'a pas déployé les équipements de l'art antérieur pour l'analyse des flux ou pour les parties de son réseau pour lesquelles ces équipements n'ont pas été déployés, l'utilisateur bénéficie toujours de l'analyse grâce à l'invention.

REVENDICATIONS

1. Dispositif d'analyse de flux (f), ledit dispositif d'analyse étant apte à communiquer avec au moins un terminal (1₂) échangeant au moins un flux (f) avec un autre terminal (1₀) dans un réseau de communication (A-H),
5 caractérisé en ce que ledit dispositif d'analyse comporte des moyens d'analyse (211) d'un flux (f) reçu par un terminal (1₂), lesdits moyens d'analyse (211) étant aptes à analyser ledit flux (f) en fonction d'au moins une information (i) concernant ledit flux (f) transmise par ledit terminal (1₂) audit dispositif d'analyse.
- 10 2. Dispositif d'analyse de flux (f) selon l'une quelconque des revendications précédentes, caractérisé en ce que ledit flux (f) reçu est un flux reçu par ledit au moins un terminal (1₂) dans un réseau ad-hoc.
3. Dispositif d'analyse de flux (f) selon l'une quelconque des revendications précédentes, caractérisé en ce que ledit dispositif d'analyse
15 comporte en outre des moyens de requête (212) auprès d'un terminal (1₂) permettant au dispositif d'analyse de requérir la récupération de données (f') comportant tout ou une partie prédéterminée dudit flux (f), ladite au moins une information (i) concernant ledit flux comportant lesdites données récupérées.
4. Dispositif d'analyse de flux (f) selon l'une quelconque des revendications précédentes, caractérisé en ce que ledit dispositif d'analyse
20 comporte des moyens de commande (213), lesdits moyens de commande (213) étant aptes à commander au moins un terminal (1₂) ayant reçu ledit flux (f) en fonction du résultat (r) fournis par les moyens d'analyse (211).
5. Dispositif de détection de virus dans des flux (f) échangés par au moins
25 un terminal (1₂) avec au moins un autre terminal (1₀) dans un réseau de communication (A-H), ledit dispositif de détection de virus comportant le dispositif d'analyse (21) de flux selon l'une quelconque des revendications précédentes, et lesdits moyens d'analyse (211) étant aptes à détecter un flux (f) vérolé en fonction d'au moins une information (i) concernant ledit flux
30 transmis par ledit terminal (1₂) audit dispositif d'analyse (21).
6. Serveur dans un réseau de communication (A-H) comportant au moins un terminal (1₂) échangeant au moins un flux (f) avec un autre terminal (1₀) dans un réseau de communication (A-H), caractérisé en ce qu'il comporte des moyens d'analyse (211) d'un flux (f) reçu par un terminal, lesdits moyens

d'analyse (211) étant apte à analyser ledit flux (f) en fonction d'au moins une information (i) concernant ledit flux (f) transmis par ledit terminal (1₂) audit serveur.

7. Dispositif de pré-analyse de flux, ledit dispositif de pré-analyse étant apte à communiquer avec au moins un dispositif d'analyse (21), caractérisé en ce que ledit dispositif de pré-analyse comporte:

- Des moyens de détection (111₂) de réception d'un flux (f) par un terminal (1₂), ledit terminal (1₂) échangeant au moins un flux (f) avec un autre terminal (1₀) dans un réseau de communication (A-H);
- Des moyens de communication aptes à émettre au moins une information (i) concernant ledit flux (f) reçu audit dispositif d'analyse (21).

8. Dispositif de pré-analyse de flux (f) selon la revendication précédente, caractérisé en ce que ledit dispositif de pré-analyse comporte en outre des moyens de réduction (112₂) dudit flux (f) permettant ainsi de fournir des informations réduites, les informations (i) concernant ledit flux (f) comportant lesdites informations réduites.

9. Terminal de communication apte à communiquer avec au moins un dispositif d'analyse, ledit terminal étant apte à échanger au moins un flux (f) avec un autre terminal (1₀) dans un réseau de communication (A-H), caractérisé en ce que ledit terminal comporte:

- Des moyens de détection (111₂) de réception d'un flux (f) par ledit terminal;
- Des moyens de communication (12₂) apte à émettre lesdites au moins une information (i) concernant ledit flux (f) reçu audit dispositif d'analyse (21).

10. Procédé d'analyse de flux (f) échangés entre au moins un terminal (1₂) et un autre terminal (1₀) dans un réseau de communication (A-H), caractérisé en ce qu'il comporte au moins l'étape suivante consistant à analyser un flux (f) reçu par ledit au moins un terminal en fonction d'une information (i) concernant ledit flux (f).

11. Procédé d'analyse de flux (f) selon la revendication 10, caractérisé en ce que l'analyse dudit flux (f) en fonction desdites au moins une information (i) concernant ledit flux (f) comporte une sous étape consistant à comparer la fréquence (Freq) de réception d'au moins une information (i) concernant ledit

flux (f) d'un type donné sur une plage de temps prédéterminé par rapport à un seuil (S) prédéterminé dont le résultat (r) constitue une condition prédéterminée pour au moins une étape suivante dudit procédé d'analyse.

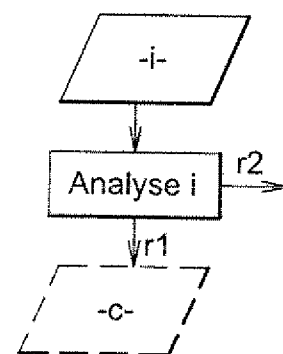
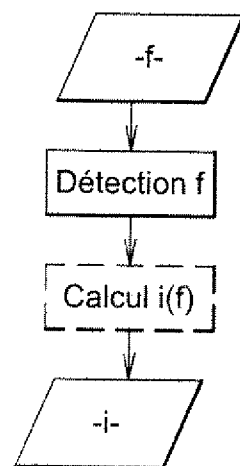
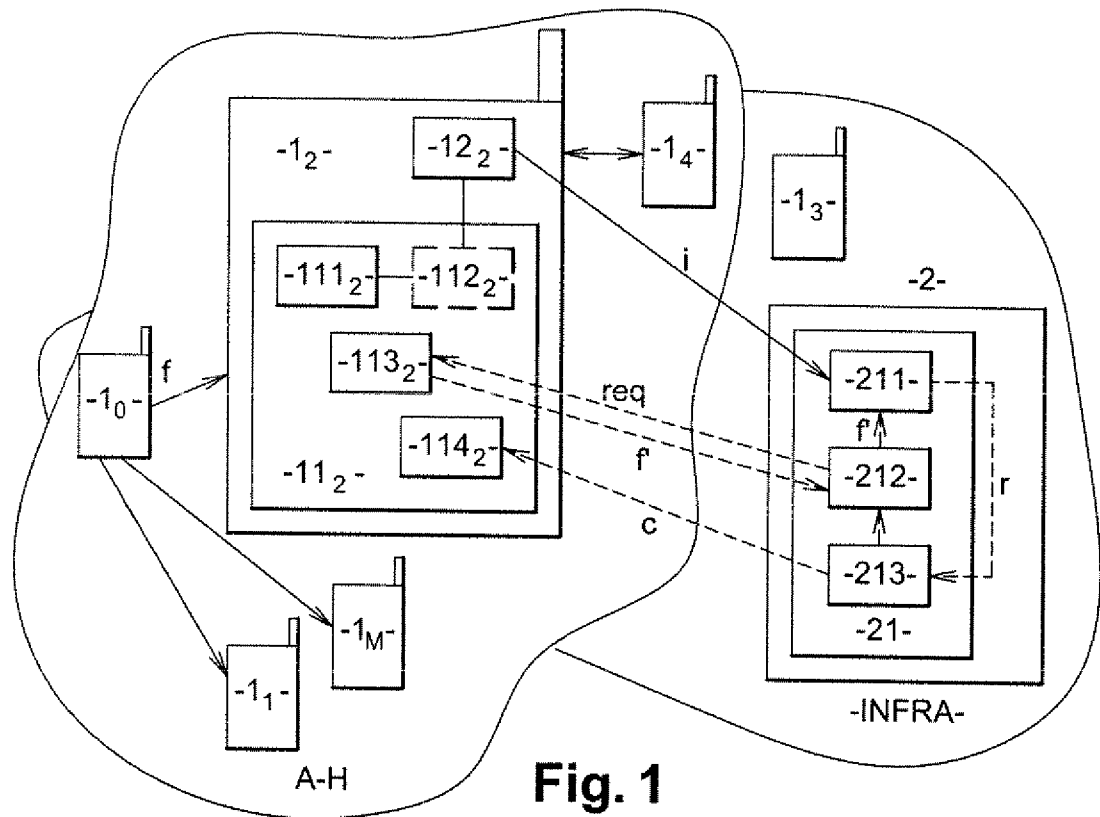
5 12. Programme d'ordinateur d'analyse comprenant des instructions de code de programme pour l'exécution des étapes du procédé selon l'une quelconque des revendications 10 ou 11 lorsque ledit programme est exécuté sur un ordinateur

10 13. Procédé de pré-analyse de flux (f) échangé entre un terminal et un autre terminal (10) dans un réseau de communication (A-H), caractérisé en ce qu'il comporte les étapes suivantes consistant à:

- Détecter la réception d'un flux (f) par ledit terminal,
- Emettre lesdites au moins une information (i) concernant ledit flux (f) à un dispositif d'analyse de flux (f).

15 14. Programme d'ordinateur de pré-analyse comprenant des instructions de code de programme pour l'exécution des étapes du procédé selon la revendication 13 lorsque ledit programme est exécuté sur un ordinateur.

1/2



2 / 2

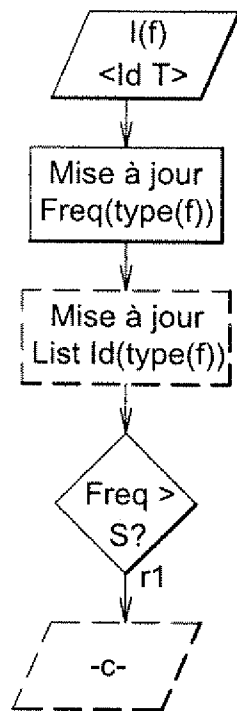


Fig. 3

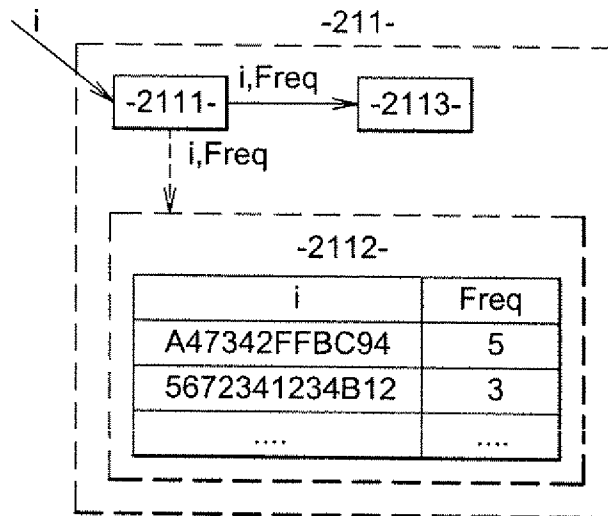


Fig. 4

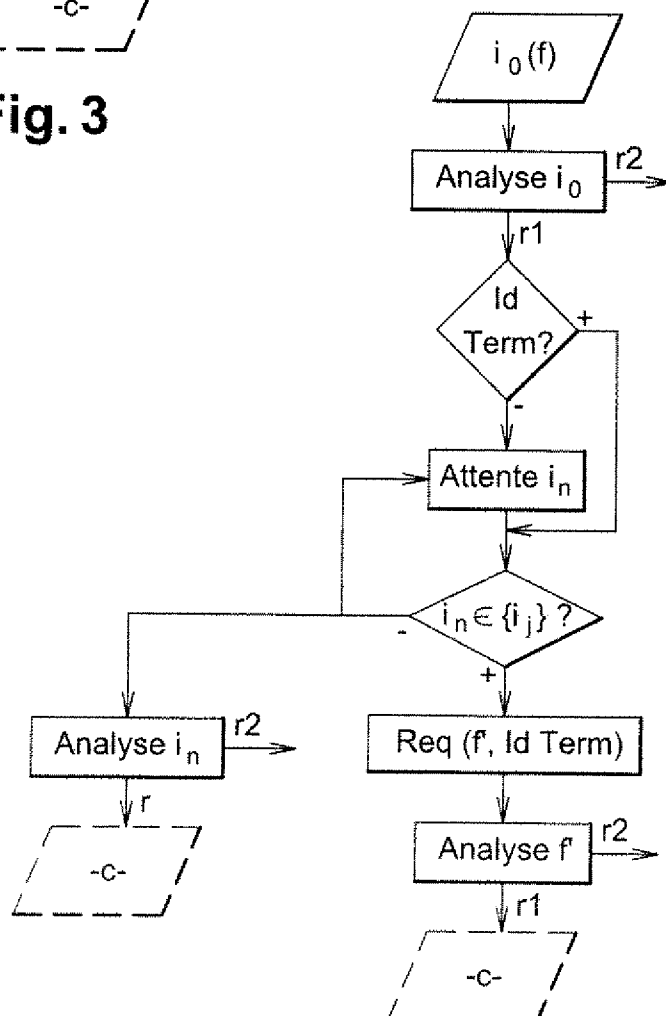


Fig. 5

INTERNATIONAL SEARCH REPORT

International application No

PCT/FR2007/051349

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, IBM-TDB, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2003/027552 A1 (KOUZNETSOV VICTOR [US]) 6 February 2003 (2003-02-06) paragraph [0026] - paragraph [0058]; figure 1	1-14
A	US 2004/209609 A1 (KOUZNETSOV VICTOR [US] ET AL KOUZNETSOV VICTOR [US] ET AL) 21 October 2004 (2004-10-21) paragraph [0007] - paragraph [0008] paragraph [0027] - paragraph [0046] claim 1	1-14
A	WO 02/19066 A2 (SECURE OYJ F [FI]; SAMMAN BEN [FR]) 7 March 2002 (2002-03-07) page 3, line 9 - page 8, line 14	1-14



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

A document defining the general state of the art which is not considered to be of particular relevance

E earlier document but published on or after the international filing date

L document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

O document referring to an oral disclosure, use, exhibition or other means

P document published prior to the international filing date but later than the priority date claimed

T later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

X document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

Y document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

& document member of the same patent family

Date of the actual completion of the international search

8 novembre 2007

Date of mailing of the international search report

14/11/2007

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Raposo Pires, João

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/FR2007/051349

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003027552	A1	06-02-2003	AU 2002329645 A1 24-02-2003
		CA 2455860 A1 20-02-2003	
		WO 03015371 A2 20-02-2003	
US 2004209609	A1	21-10-2004	CA 2517553 A1 04-11-2004
		EP 1629346 A2 01-03-2006	
		JP 2006524396 T 26-10-2006	
		KR 20060008902 A 27-01-2006	
		WO 2004095177 A2 04-11-2004	
WO 0219066	A2	07-03-2002	AU 8982301 A 13-03-2002
		GB 2366692 A 13-03-2002	
		US 2003177397 A1 18-09-2003	

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°

PCT/FR2007/051349

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. H04L29/06

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
H04L G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)

EPO-Internal, IBM-TDB, INSPEC

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	US 2003/027552 A1 (KOUZNETSOV VICTOR [US]) 6 février 2003 (2003-02-06) alinéa [0026] - alinéa [0058]; figure 1	1-14
A	US 2004/209609 A1 (KOUZNETSOV VICTOR [US] ET AL KOUZNETSOV VICTOR [US] ET AL) 21 octobre 2004 (2004-10-21) alinéa [0007] - alinéa [0008] alinéa [0027] - alinéa [0046] revendication 1	1-14
A	WO 02/19066 A2 (SECURE OYJ F [FI]; SAMMAN BEN [FR]) 7 mars 2002 (2002-03-07) page 3, ligne 9 - page 8, ligne 14	1-14

☐ Voir la suite du cadre C pour la fin de la liste des documents



Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

- *A* document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- *E* document antérieur, mais publié à la date de dépôt international ou après cette date
- *L* document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
- *O* document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
- *P* document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

T document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

X document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

Y document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

Z document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

8 novembre 2007

Date d'expédition du présent rapport de recherche internationale

14/11/2007

Nom et adresse postale de l'administration chargée de la recherche internationale

Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Raposo Pires, João

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°

PCT/FR2007/051349

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2003027552 A1	06-02-2003	AU 2002329645 A1	24-02-2003
		CA 2455860 A1	20-02-2003
		WO 03015371 A2	20-02-2003
US 2004209609 A1	21-10-2004	CA 2517553 A1	04-11-2004
		EP 1629346 A2	01-03-2006
		JP 2006524396 T	26-10-2006
		KR 20060008902 A	27-01-2006
		WO 2004095177 A2	04-11-2004
WO 0219066 A2	07-03-2002	AU 8982301 A	13-03-2002
		GB 2366692 A	13-03-2002
		US 2003177397 A1	18-09-2003