

(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
09 janvier 2020 (09.01.2020)

WIPO | PCT

(10) Numéro de publication internationale
WO 2020/008159 A1

(51) Classification internationale des brevets :

H04L 29/06 (2006.01) H04L 29/08 (2006.01)

H04L 12/26 (2006.01)

(21) Numéro de la demande internationale :

PCT/FR2019/051682

(22) Date de dépôt international :

05 juillet 2019 (05.07.2019)

(25) Langue de dépôt :

français

(26) Langue de publication :

français

(30) Données relatives à la priorité :

18 56240 06 juillet 2018 (06.07.2018) FR

(71) Déposant : QOSMOS TECH [FR/FR] ; IMMEUBLE LE
CARDINET 8 RUE BERNARD BUFFET, 75017 PARIS
(FR).

(72) Inventeur : TOLLET, Jérôme ; 6 boulevard Beaumar-
chais, 75003 PARIS (FR).

(74) Mandataire : PLASSERAUD IP ; 66 rue de la Chaussée
d'Antin, 75440 PARIS CEDEX 09 (FR).

(81) États désignés (sauf indication contraire, pour tout titre de
protection nationale disponible) : AE, AG, AL, AM, AO,

AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA,
CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ,
EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR,
HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR,
KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG,
MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM,
PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC,
SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG,
ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, RU, TJ, TM),
européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES,
FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK,
MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI
(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML,
MR, NE, SN, TD, TG).

Publiée:

— avec rapport de recherche internationale (Art. 21(3))

(54) Title: IDENTIFICATION OF A PROTOCOL OF A DATA STREAM

(54) Titre : IDENTIFICATION DE PROTOCOLE D'UN FLUX DE DONNÉES

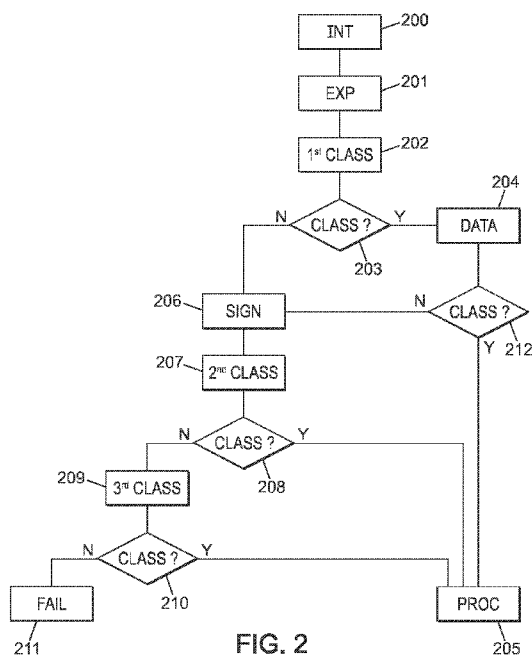


FIG. 2

(57) Abstract: The invention concerns a method for identifying a proto-
col of a data stream exchanged between two entities of a telecommuni-
cation network, the processing method comprising the following steps:
- on receiving (200) data of the data stream, grammatical parsing (202)
of said data stream in order to identify a protocol of the data stream;
- in the event of failure (203) to identify the protocol of the data stream by
grammatical parsing, consulting (206) a signature engine mapping pro-
tocols with corresponding signatures, and sequentially applying (207)
signatures to the data flow in order to identify a data stream protocol.

(57) Abrégé : Identification de protocole d'un flux de données
L'invention concerne un procédé d'identification d'un protocole d'un
flux de données échangé entre deux entités d'un réseau de télécommu-
nication, le procédé de traitement comprenant les étapes suivantes: -sur
réception (200) de données du flux de données, analyse grammaticale
(202) dudit flux de données en vue d'identifier un protocole du flux de
données; -en cas d'échec (203) de l'identification du protocole du flux
de données par l'analyse grammaticale, consultation (206) d'un moteur
de signatures mettant en correspondance des protocoles avec des signa-
tures correspondantes, et application séquentielle (207) des signatures
au flux de données en vue d'identifier un protocole du flux de données.

WO 2020/008159 A1

Identification de protocole d'un flux de données

La présente invention concerne le traitement de données dans des réseaux de télécommunications, et notamment la reconnaissance de protocoles de flux de données.

Elle concerne plus précisément des applications de surveillance et de catégorisation de flux de données transitant sur des réseaux de télécommunications, par exemple des flux internet.

Dans la suite, on entend par flux de données tout ensemble de données échangées entre deux entités réseaux, par exemple entre un client et un serveur, ou entre deux clients (flux dits pair à pair, ou P2P).

Il est connu d'appliquer différentes méthodes de classification de flux de données afin de détecter un format de données, ou un protocole employé pour leur transport, en vue de filtrer les flux de données, de catégoriser un flux afin de permettre de traiter le flux de données en fonction de sa classification.

A cet effet, des analyseurs de flux peuvent être disposés en interception dans des points d'accès réseau, tels que des bornes Wi-fi, des pare-feu ou de serveurs de proxy par exemple.

Dans un pare-feu, la configuration d'un système de sécurité peut être basée sur la reconnaissance de propriétés de certains protocoles afin d'empêcher certains types de transfert. Un analyseur de flux de données permet ainsi de fournir au pare-feu une classification du flux de données basée sur les protocoles reconnus.

Par exemple, en référence à la figure 1, un système d'analyse de trafic entre deux entités (client et/ou serveur) inclut un premier réseau comprenant une première entité 112 (de type client par exemple) connecté à un second réseau 110 comprenant une deuxième entité 111 (de type serveur par exemple) par un lien de communication 120. Le lien 120 est analysé par un analyseur 300, qui mesure et analyse le trafic dans les deux directions ou dans une seule direction entre le premier réseau 100 et le deuxième réseau 110. Le trafic entre les réseaux 100 et 110 peut être de l'ordre du Gigabit par seconde, Gbps, dans des réseaux d'entreprise, mais peut atteindre la dizaine de Gbps dans le cœur d'un réseau d'un opérateur.

La quantité de données transitant sur un réseau de télécommunications rend par ailleurs l'analyse et la classification coûteuses en termes de ressources.

La capacité de mesure et d'analyse de l'analyseur 300 est déterminée par le nombre N de flux simultanés et le débit T de chaque flux. N affecte directement la quantité de mémoire requise pour gérer le contexte des flux enregistrés, tandis que T impacte directement la puissance de calcul requise pour mettre en œuvre l'analyse et la classification sans perte significative de paquets et sans retarder le flux. T définit la quantité de paquets à traiter dans un laps de temps donné et, ainsi, la quantité de ressources de traitement qui peut être allouée à chaque paquet.

Dans des systèmes connus, la quantité de ressources de traitement augmente proportionnellement avec l'augmentation des flux N. A ressources fixes, une infrastructure de données peut uniquement augmenter N en diminuant T, ou augmenter T en diminuant N. Exprimé autrement, la produit $N \cdot T$ reste sensiblement constant.

Toutefois, en pratique, N et T augmentent tous les deux de manière proportionnelle dans les réseaux informatiques existants.

Afin de tenter de palier à de tels inconvénients, le brevet EP1722509, du même déposant, propose une analyse hiérarchisée reposant sur une reconnaissance de protocole explicite dans un premier temps, et implicite dans un second temps, si la reconnaissance explicite n'est pas possible.

Une reconnaissance explicite est notamment mise en œuvre lorsqu'une couche de niveau donné indique explicitement le protocole utilisé pour la couche de niveau supérieur qu'elle encapsule. Par exemple, la couche Ethernet indique explicitement si la couche supérieure est IPv4 ou IPv6, et IP indique si la couche supérieure est TCP ou UDP. Une telle reconnaissance est aisée et requiert peu de puissance de calcul.

En ce qui concerne les couches de niveau applicatif, elles sont le plus souvent identifiées par une méthode de reconnaissance de type implicite, plus coûteuse en ressources, car elles ne sont pas explicitement indiquées par la couche de transport de niveau inférieur.

En outre, la diversité des encodages de protocoles de ce niveau ainsi que l'émergence du chiffrement des communications requièrent de nouvelles méthodes de reconnaissance de protocole.

Par exemple, l'identification de protocoles tels que SMTP et HTTP est plus aisée et moins consommatrice en ressource que l'identification d'un protocole tel que Bittorrent, dont les données sont chiffrées. Il conviendrait ainsi d'optimiser la classification de flux de données en réduisant la complexité sans réduire la fiabilité.

La présente invention vient améliorer la situation.

Elle propose à cet effet un procédé d'identification d'un protocole d'un flux de données échangé entre deux entités d'un réseau de télécommunication, le procédé de traitement comprenant les étapes suivantes :

- sur réception de données du flux de données, analyse grammaticale du flux de données en vue d'identifier un protocole du flux de données ;
- en cas d'échec de l'identification du protocole du flux de données par l'analyse grammaticale, consultation d'un moteur de signatures mettant en correspondance des protocoles avec des signatures correspondantes, et application séquentielle des signatures au flux de données en vue d'identifier un protocole du flux de données.

Une analyse grammaticale est peu consommatrice en ressources de calculs et permet d'identifier la plupart des protocoles qui ne peuvent être identifiés de manière explicite. La méthode d'analyse basée sur les signatures, plus consommatrices en ressources de calcul, est uniquement mise en œuvre en cas d'échec de l'analyse grammaticale, ce qui permet d'optimiser l'utilisation de ressources lors de l'identification implicite d'un protocole.

Selon un mode de réalisation, l'invention peut comprendre en outre, en cas d'échec de l'identification du protocole du flux de données par consultation du moteur de signatures, l'application d'une méthode statistique de reconnaissance de protocole afin d'identifier le protocole du flux de données.

Une telle méthode est également consommatrice en ressources de calcul, et n'est pas totalement fiable. Elle est donc avantageusement mise en œuvre en cas d'échec des deux premières méthodes. Elle permet de plus de reconnaître des protocoles chiffrés tels que Bittorrent, qui ne peuvent être

reconnus par les deux méthodes précédentes.

Selon un mode de réalisation, le protocole identifié peut être un protocole de niveau applicatif.

5 Les protocoles de niveau applicatif, et plus généralement les protocoles des couches 5 à 7 du modèle OSI, ne sont pas indiqués explicitement par les couches de niveau inférieur, et le procédé leur est donc avantageusement appliqué selon ce mode de réalisation.

10 Selon un mode de réalisation, en cas de succès de l'identification du protocole du flux de données par l'analyse grammaticale, le procédé peut comprendre en outre une étape d'identification de données de protocoles par l'application d'un algorithme simple passe à des éléments contextuels du flux de données selon le protocole identifié.

15 Un tel algorithme est peu consommateur en ressources, et permet ainsi, pour un protocole identifié donné, de différencier les données qu'ils transportent entre différents types de données de protocole.

20 En complément, en cas d'échec de l'identification de données de protocoles par l'application de l'algorithme simple passe, le procédé peut comprendre en outre la consultation d'un moteur de signatures mettant en correspondance des données de protocoles avec des signatures correspondantes, et l'application séquentielle des signatures au flux de données en vue d'identifier les données de protocole du flux de données.

25 Ainsi, la méthode d'analyse basée sur les signatures, plus consommatrices en ressources de calcul, est uniquement mise en œuvre en cas d'échec de l'analyse grammaticale, ce qui permet d'optimiser l'utilisation de ressources lors de l'identification implicite de données de protocole.

Selon un mode de réalisation, le procédé peut comprenant en outre une étape de traitement du flux de données sur la base du protocole identifié du flux de données.

Ainsi, un traitement différencié par protocole peut être appliqué.

30 En complément, traiter le flux de données peut comprendre l'une au moins des étapes parmi :

- appliquer une politique de qualité de service dépendant du protocole identifié ;
- ou

- autoriser ou interdire le flux de données sur la base du protocole identifié.

Un deuxième aspect de l'invention concerne un produit programme informatique comportant des instructions pour la mise en œuvre du procédé selon le premier aspect de l'invention, lorsque ce programme est exécuté par un processeur.

Un troisième aspect de l'invention concerne un dispositif d'identification d'un protocole d'un flux de données échangé entre deux entités d'un réseau de télécommunication, le dispositif comprenant :

- une interface configurée pour recevoir des données du flux de données ;

- un processeur configuré pour :

- mener une analyse grammaticale du flux de données en vue d'identifier un protocole du flux de données ;

- en cas d'échec de l'identification du protocole du flux de données par l'analyse grammaticale, consulter un moteur de signatures mettant en correspondance des protocoles avec des signatures correspondantes, et appliquer séquentiellement les signatures au flux de données en vue d'identifier un protocole du flux de données.

D'autres caractéristiques et avantages de l'invention apparaîtront à l'examen de la description détaillée ci-après, et des dessins annexés sur lesquels:

- la figure 1 illustre une architecture générale d'un système selon un mode de réalisation de l'invention;

- la figure 2 est un diagramme présentant les étapes d'un procédé de traitement selon un mode de réalisation de l'invention ;

- la figure 3 illustre la structure d'un dispositif de traitement de données selon un mode de réalisation de l'invention.

L'invention peut être mise en œuvre dans un dispositif d'identification de protocole tel que l'analyseur 300 illustré sur la figure 1. Le dispositif d'identification sera présenté plus en détails en référence à la figure 3.

La figure 2 présente les étapes d'un procédé d'identification de protocole selon un mode de réalisation de l'invention.

A une étape 200, un ou plusieurs paquets d'un flux sont reçus par le dispositif d'identification, par exemple suite à une interception des paquets par l'analyseur 300 sur le lien de communication 200.

5 A une étape 201, un paquet de données reçu peut être identifié pour être associé à un flux existant ou pour créer une nouvelle entrée dans une table répertoriant les flux de données en cours. Par exemple, une adresse IP (et éventuellement un numéro de port) d'une entité source et une adresse IP (et éventuellement un numéro de port) d'une entité destinataire peuvent être prises en compte pour identifier le flux correspondant au paquet. Une telle technique
10 est bien connue et ne sera pas explicitée davantage.

L'entité source ou destinataire peut désigner indifféremment un client ou un serveur. Le client peut être un ordinateur portable ou de bureau, une tablette tactile, un Smartphone ou encore tout dispositif électronique comprenant une interface permettant de communiquer dans le réseau 100 ou
15 110, tel que le réseau Internet par exemple. Selon l'invention, les deux entités communicantes peuvent être dans deux réseaux distincts comme illustré sur la figure 1 ou peuvent appartenir au même réseau.

Les protocoles de couches basses du flux de données peuvent être déterminés à l'étape 201 par reconnaissance explicite. Comme indiqué
20 précédemment, une reconnaissance explicite requiert peu de puissance de calcul en ce que le protocole d'une couche d'un niveau donné peut être indiqué explicitement par la couche du niveau qui lui est directement inférieur.

Ainsi, il peut par exemple être déterminé que le protocole IPv4 ou IPv6 est utilisé à partir de données de la couche Ethernet. De même la couche
25 IP indique si le protocole UDP ou TCP est utilisé.

A partir de l'étape 202, le procédé selon l'invention a pour but d'identifier un protocole qui n'est pas signalé explicitement par les couches de niveaux inférieurs. Une telle identification est donc implicite. A titre d'exemple, la reconnaissance d'un protocole des couches du niveau 5 à 7 du niveau OSI,
30 et en particulier du niveau 7 (application), est considérée.

A une étape 203, le dispositif d'identification met en œuvre une analyse grammaticale des données du flux de données, contenues dans le paquet ou les paquets du flux de données, en vue d'identifier un protocole du

flux de données. En effet, certains protocoles de niveau applicatif ont une grammaire aisément identifiable en mettant en œuvre une faible puissance de calcul. C'est par exemple le cas des protocoles SMTP et HTTP. De tels protocoles ont des éléments contextuels utiles à leur reconnaissance. Par exemple, ils utilisent tous les deux un processus de « *handshake* » pour l'établissement du flux. D'autres protocoles tels que SSL ou SIP peuvent également être identifiés par reconnaissance de leur grammaire. Il est à noter que statistiquement, 90% des protocoles d'application des flux à classifier peuvent être reconnus par utilisation de l'étape 203. Utiliser en priorité une telle méthode de reconnaissance en premier permet ainsi de reconnaître un grand nombre de protocoles avec une faible puissance de calcul.

A l'étape 203, il est vérifié si le protocole du flux de données a été identifié avec succès par l'analyse grammaticale.

En cas de succès de l'identification du protocole du flux de données par l'analyse grammaticale, le procédé peut comprendre en outre une étape 204 d'identification de données de protocoles (« *protocol data* » en anglais) par l'application d'un algorithme simple passe (« *one pass* » ou « *single pass* » en anglais) à des éléments contextuels du flux de données selon le protocole identifié. L'algorithme simple passe peut dépendre du protocole identifié.

L'identification des données de protocole peut être considérée comme l'identification d'une application ou sous-application d'une couche supérieure à la couche du protocole identifié à l'étape 203. Par exemple, si le protocole identifié comme étant HTTP, la sous-application de couche supérieure, ou données de protocoles, peuvent être des données FacebookTM par exemple.

L'application de l'algorithme simple passe peut consister en l'injection d'éléments contextuels du flux (par exemple, pour HTTP, les éléments contextuels peuvent être des éléments tels que l'URL, User Agent, etc) dans un moteur de règles. On appelle élément contextuel du flux tout élément d'en-tête ou de charge utile (payload) du flux de données. L'utilisation d'un algorithme simple passe est peu coûteux en ressources de calcul et le temps de traitement est fixe et ne dépendant pas du nombre d'entrées.

En réponse à l'injection des éléments contextuels, le moteur de

règles peut renvoyer un ensemble de règles qui peuvent être testées sur les données du protocole identifié à l'étape 102 afin d'identifier les données de protocole. Par exemple, après avoir identifié le protocole HTTP à l'étape 202, les données de protocole peuvent être identifiées comme étant des données FacebookTM.

A une étape 212, il est vérifié si les données de protocoles ont été identifiées à l'étape 204 au moyen de l'algorithme simple passe. En cas de succès, le procédé se poursuit avec l'étape 205. En cas d'échec, le procédé passe à l'étape 206 décrite ci-après.

Les étapes 204 et 205 sont optionnelles et le procédé peut passer directement de l'étape 203 à 205 en cas d'identification positive à l'étape 203.

Une fois le protocole identifié, et éventuellement les données de protocole, le procédé peut comprendre l'application d'une étape 205 de traitement du flux de données en fonction du protocole identifiée, et éventuellement en fonction des données d'application. Le traitement du flux peut par exemple consister à appliquer une politique de qualité de service dépendant du protocole identifié ou à autoriser ou interdire le flux de données sur la base du protocole identifié, ou peut plus généralement consister à classer le flux en fonction du protocole identifié. La classification peut être transmise à un dispositif de traitement extérieur au dispositif d'identification de protocole.

En cas d'échec de l'identification du protocole du flux de données par l'analyse grammaticale à l'étape 202, le procédé selon l'invention comprend une étape 206 de consultation d'un moteur de signatures mettant en correspondance des protocoles avec des signatures correspondantes. A une étape 207, les signatures sont appliquées séquentiellement au flux de données en vue d'identifier le protocole de niveau applicatif du flux de données. Une telle application séquentielle est plus coûteuse en termes de ressources, et est ainsi avantageusement appliquée uniquement en cas d'échec de l'analyse grammaticale à l'étape 202.

Statistiquement, une telle méthode par recherche de signatures permet d'accéder à la moitié des 10% de protocoles applicatifs qui n'ont pu être identifiés par la méthode d'analyse grammaticale (soit 5% des protocoles). Bien que plus coûteuse en ressources de calcul, la méthode par recherche de

signatures demeure néanmoins fiable.

Les étapes 206 et 207 peuvent également être appliquées aux données de protocole en cas d'échec d'identification à l'étape 204. Dans ce cas, les données de protocoles sont comparées avec des signatures pour leur

identification.

A une étape 208, il est vérifié si le protocole du flux de données a été identifié avec succès par la méthode de recherche de signatures.

En cas de succès, le procédé reprend à l'étape 205 décrite précédemment.

En cas d'échec, un mode de réalisation de l'invention peut prévoir une étape additionnelle 209 d'application d'une méthode statistique de reconnaissance de protocole afin d'identifier le protocole applicatif du flux de données (ou les données de protocole). Une telle méthode permet notamment d'identifier des protocoles chiffrés, tels que Bittorrent. Une telle méthode est coûteuse en puissance de calculs (recherche séquentielle) et n'est pas totalement fiable. Elle permet toutefois d'identifier 1 à 2% des protocoles ou des données de protocole qui n'ont pas été identifiés par les méthodes mises en œuvre précédemment.

A une étape 210, il est vérifié si le protocole du flux de données a été identifié avec succès par la méthode statistique.

En cas de succès, le procédé reprend à l'étape 205 décrite précédemment.

En cas d'échec (statistiquement dans 3% des cas environs), le procédé s'achève sans pouvoir identifier le protocole applicatif du flux de données. Un traitement prédéfini peut être appliqué à une étape 211 en cas d'échec. Par exemple, par mesure de précaution, le flux de données peut être bloqué.

L'invention prévoit ainsi l'application incrémentale de méthodes de reconnaissances de protocole, de la méthode la plus fiable et la moins coûteuse en puissance de calcul, à la méthode la moins fiable et la plus consommatrice en ressources. Elle optimise ainsi la recherche du protocole de niveau applicatif.

La figure 3 représente un dispositif d'identification de protocole 301 selon un mode de réalisation de l'invention.

Le dispositif d'identification 301 peut être implémenté dans l'analyseur 300 situé en interception entre les réseaux 100 et 110 de la figure 1.
5 De manière plus général, il est apte à recevoir des données de flux de données transitant entre deux entités réseau.

Le dispositif d'identification comprend une mémoire vive 305 et un processeur 304, ainsi qu'une mémoire 301 pour stocker des instructions permettant la mise en œuvre des étapes du procédé décrit ci-avant en
10 référence à la figure 2. Le processeur peut comprendre des sous-entités 304.1 à 304.3 respectivement dédiées aux trois méthodes de reconnaissance décrites ci-avant.

La mémoire 301 peut en outre stocker des données utilisées par le processeur pour la mise en œuvre du procédé, notamment :

- 15 - le moteur de signatures mettant en correspondance des signatures avec des protocoles correspondants ;
- les ensembles de règles associées à des protocoles données, pour la reconnaissance de données de protocole ;
- des règles de méthodes statistiques de reconnaissance de protocole.

20 Le dispositif d'identification 301 comporte en outre une interface d'entrée 302 destinée à recevoir les données de flux de données circulant sur le lien de communication 200 ou dans un réseau donné.

Le dispositif d'identification 301 comprend en outre une interface de sortie 303 apte à fournir un résultat d'identification de protocole, ou une
25 commande déterminée à partir du protocole identifié.

Bien entendu, la présente invention ne se limite pas à la forme de réalisation décrite ci-avant à titre d'exemple ; elle s'étend à d'autres variantes.

REVENDICATIONS

1. Procédé d'identification d'un protocole d'un flux de données échangé entre deux entités (111 ; 112) d'un réseau de télécommunication, le procédé de traitement comprenant les étapes suivantes :
 - sur réception (200) de données du flux de données, analyse grammaticale (202) dudit flux de données en vue d'identifier un protocole du flux de données ;
 - en cas d'échec (203) de l'identification du protocole du flux de données par l'analyse grammaticale, consultation (206) d'un moteur de signatures mettant en correspondance des protocoles avec des signatures correspondantes, et application séquentielle (207) des signatures au flux de données en vue d'identifier un protocole du flux de données.
2. Procédé selon la revendication 1, comprenant en outre, en cas d'échec (208) de l'identification du protocole du flux de données par consultation du moteur de signatures, l'application (209) d'une méthode statistique de reconnaissance de protocole afin d'identifier le protocole du flux de données.
3. Procédé selon la revendication 1 ou 2, dans lequel le protocole identifié est un protocole de niveau applicatif.
4. Procédé selon l'une des revendications précédentes, dans lequel, en cas de succès (203) de l'identification du protocole du flux de données par l'analyse grammaticale, le procédé comprend en outre une étape d'identification (204) de données de protocoles par l'application d'un algorithme simple passe à des éléments contextuels du flux de données selon le protocole identifié.
5. Procédé selon la revendication 4, dans lequel, en cas d'échec de l'identification de données de protocoles par l'application de l'algorithme simple passe, le procédé comprend en outre la consultation (206) d'un moteur de signatures mettant en correspondance des données de protocoles avec des signatures correspondantes, et l'application séquentielle (207) des signatures au flux de données en vue d'identifier les données de protocole du flux de

données.

5 6. Procédé selon l'une des revendications précédentes, comprenant en outre une étape de traitement (205) du flux de données sur la base du protocole identifié du flux de données.

7. Procédé selon la revendication 6, dans lequel le traitement (205) du flux de données comprend l'une au moins des étapes parmi :
- appliquer une politique de qualité de service dépendant du protocole identifié ;
10 ou
- autoriser ou interdire le flux de données sur la base du protocole identifié.

8. Produit programme informatique comportant des instructions pour la mise en œuvre du procédé selon l'une des revendications 1 à 7, lorsque ce programme
15 est exécuté par un processeur.

9. Dispositif d'identification d'un protocole d'un flux de données échangé entre deux entités d'un réseau de télécommunication, le dispositif comprenant :
- une interface (302) configurée pour recevoir des données du flux de données ;
20 - un processeur (304) configuré pour :
- mener une analyse grammaticale du flux de données en vue d'identifier un protocole du flux de données ;
- en cas d'échec de l'identification du protocole du flux de données par l'analyse grammaticale, consulter un moteur de signatures mettant
25 en correspondance des protocoles avec des signatures correspondantes, et appliquer séquentiellement les signatures au flux de données en vue d'identifier un protocole du flux de données.

30

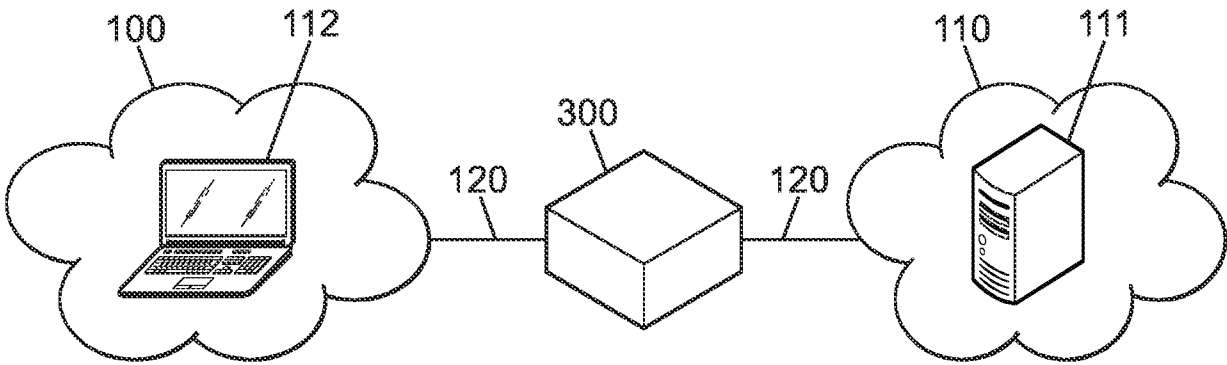
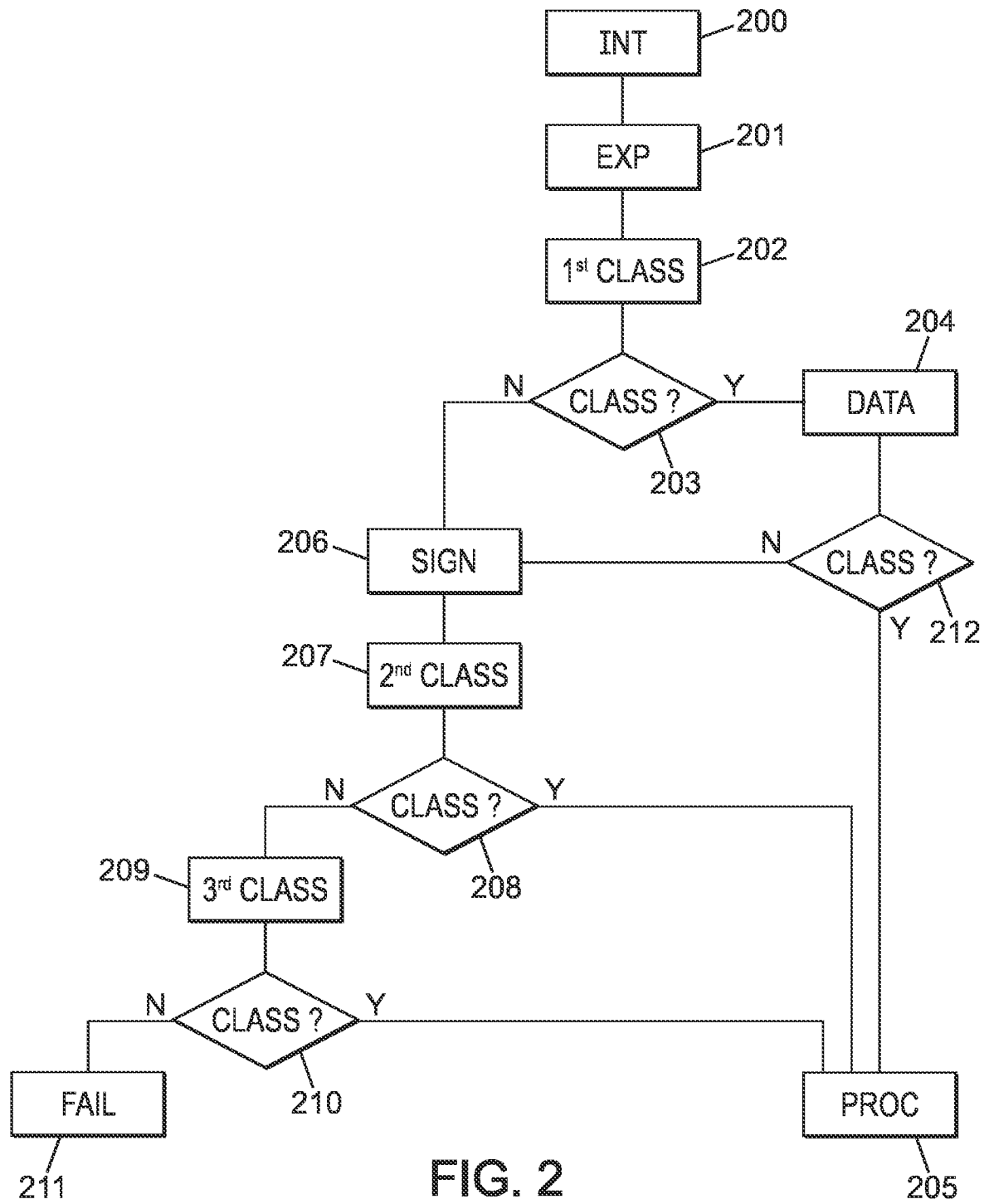


FIG. 1

2/3



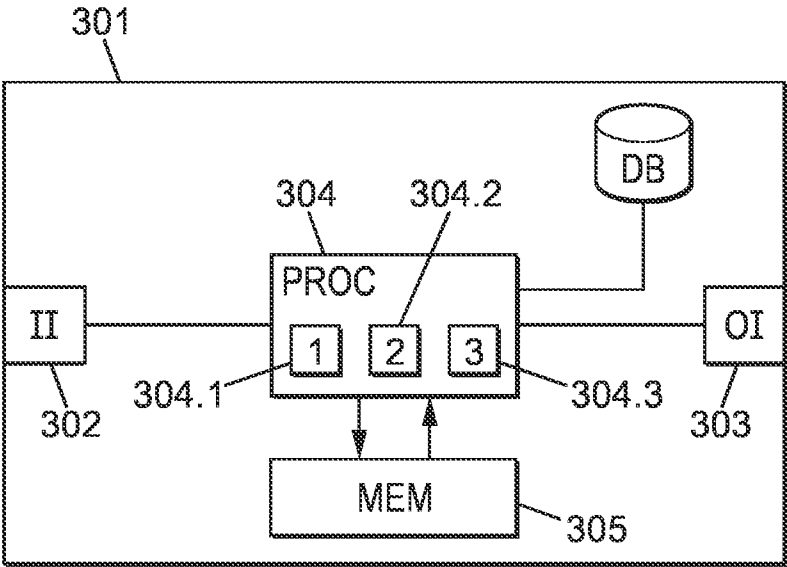


FIG. 3

INTERNATIONAL SEARCH REPORT

International application No.

PCT/FR2019/051682**A. CLASSIFICATION OF SUBJECT MATTER****H04L 29/06**(2006.01)i; **H04L 12/26**(2006.01)i; **H04L 29/08**(2006.01)i

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

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 practicable, search terms used)

EPO-Internal, INSPEC, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2006106583 A1 (FDIDA ALFORTVILLE [FR] ET AL) 18 May 2006 (2006-05-18)	1-6,8,9
Y	paragraphs [0002], [0003], [0009], [0011], [0014], [0022] - [0026], [0029], [0039], [0058], [0060], [0096] - [0098]; figure 2	7
X	US 2013238782 A1 (ZHAO YAO [US] ET AL) 12 September 2013 (2013-09-12)	1-6,8,9
A	paragraphs [0036] - [0047]; figures 1,4	7
X	EP 2916512 A1 (MITSUBISHI ELEC R&D CT EUROPE [NL]; MITSUBISHI ELECTRIC CORP [JP]) 09 September 2015 (2015-09-09)	1-6,8,9
Y	paragraphs [0001] - [0007], [0011] - [0031], [0034] - [0048], [0058] - [0097], [0101] - [0106], [0111] - [0123]; figures 5,6	7

☐ 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 application or patent 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

03 September 2019

Date of mailing of the international search report

10 September 2019

Name and mailing address of the ISA/EP

European Patent Office
p.b. 5818, Patentlaan 2, 2280 HV Rijswijk
Netherlands

Telephone No. (+31-70)340-2040

Facsimile No. (+31-70)340-3016

Authorized officer

Valero, Monica

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/FR2019/051682

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
US	2006106583	A1	18 May 2006	AU	2003267510	A1	03 March 2004
				CN	1703890	A	30 November 2005
				EP	1574000	A2	14 September 2005
				ES	2408158	T3	18 June 2013
				FR	2842970	A1	30 January 2004
				JP	4203012	B2	24 December 2008
				JP	2005537705	A	08 December 2005
				KR	20050033637	A	12 April 2005
				US	2006106583	A1	18 May 2006
				WO	2004017595	A2	26 February 2004
US	2013238782	A1	12 September 2013	CN	104160681	A	19 November 2014
				EP	2823624	A1	14 January 2015
				JP	5889445	B2	22 March 2016
				JP	2015518296	A	25 June 2015
				KR	20140133917	A	20 November 2014
				US	2013238782	A1	12 September 2013
				WO	2013134005	A1	12 September 2013
EP	2916512	A1	09 September 2015	CN	106063222	A	26 October 2016
				EP	2916512	A1	09 September 2015
				JP	6173613	B2	02 August 2017
				JP	2017502625	A	19 January 2017
				US	2016337333	A1	17 November 2016
				WO	2015133557	A1	11 September 2015

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°

PCT/FR2019/051682

A. CLASSEMENT DE L'OBJET DE LA DEMANDE INV. H04L29/06 H04L12/26 H04L29/08 ADD.		
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		
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, INSPEC, WPI Data		
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 2006/106583 A1 (FDIDA ALFORTVILLE [FR] ET AL) 18 mai 2006 (2006-05-18)	1-6,8,9
Y	alinéas [0002], [0003], [0009], [0011], [0014], [0022] - [0026], [0029], [0039], [0058], [0060], [0096] - [0098]; figure 2	7
X	----- US 2013/238782 A1 (ZHAO YAO [US] ET AL) 12 septembre 2013 (2013-09-12)	1-6,8,9
A	alinéas [0036] - [0047]; figures 1,4	7
X	----- EP 2 916 512 A1 (MITSUBISHI ELEC R&D CT EUROPE [NL]; MITSUBISHI ELECTRIC CORP [JP]) 9 septembre 2015 (2015-09-09)	1-6,8,9
Y	alinéas [0001] - [0007], [0011] - [0031], [0034] - [0048], [0058] - [0097], [0101] - [0106], [0111] - [0123]; figures 5,6	7
☐ 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 "&" document qui fait partie de la même famille de brevets		
Date à laquelle la recherche internationale a été effectivement achevée		Date d'expédition du présent rapport de recherche internationale
3 septembre 2019		10/09/2019
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, Fax: (+31-70) 340-3016		Fonctionnaire autorisé Valero, Monica

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°

PCT/FR2019/051682

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2006106583 A1	18-05-2006	AU 2003267510 A1	03-03-2004
		CN 1703890 A	30-11-2005
		EP 1574000 A2	14-09-2005
		ES 2408158 T3	18-06-2013
		FR 2842970 A1	30-01-2004
		JP 4203012 B2	24-12-2008
		JP 2005537705 A	08-12-2005
		KR 20050033637 A	12-04-2005
		US 2006106583 A1	18-05-2006
		WO 2004017595 A2	26-02-2004
US 2013238782 A1	12-09-2013	CN 104160681 A	19-11-2014
		EP 2823624 A1	14-01-2015
		JP 5889445 B2	22-03-2016
		JP 2015518296 A	25-06-2015
		KR 20140133917 A	20-11-2014
		US 2013238782 A1	12-09-2013
		WO 2013134005 A1	12-09-2013
EP 2916512 A1	09-09-2015	CN 106063222 A	26-10-2016
		EP 2916512 A1	09-09-2015
		JP 6173613 B2	02-08-2017
		JP 2017502625 A	19-01-2017
		US 2016337333 A1	17-11-2016
		WO 2015133557 A1	11-09-2015