



(51) Classification internationale des brevets :
H04L 12/24 (2006.01) **H04L 12/26** (2006.01)
H04L 29/06 (2006.01)

(21) Numéro de la demande internationale :
PCT/FR2011/050541

(22) Date de dépôt international :
17 mars 2011 (17.03.2011)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
10 01062 17 mars 2010 (17.03.2010) FR

(71) Déposant (pour tous les États désignés sauf US) :
THALES [FR/FR]; 45 rue de Villiers, F-92200 Neuilly
Sur Seine (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants (pour US seulement) : **DUBOIS, Renaud** [FR/FR]; 160, Boulevard de Valmy, F-92704 Colombes Cedex (FR). **MOREL, Mathieu** [FR/FR]; 12, rue Jonquoy, F-75014 Paris (FR). **GOMPEL, Paul** [FR/FR]; 80 bis, rue Denfert-Rochereau, F-92100 Boulogne (FR).

(74) Mandataires : **BLOT, Philippe** et al.; Cabinet LAVOIX, 2, place d'Estienne d'Orves, F-75009 Paris (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, BR, BW, BY, BZ, CA, CH, CL, 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, PE, PG, PH, PL, PT, RO, RS, RU, 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, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, 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, ML, MR, NE, SN, TD, TG).

[Suite sur la page suivante]

(54) Title : METHOD OF IDENTIFYING A PROTOCOL GIVING RISE TO A DATA FLOW

(54) Titre : PROCÉDÉ D'IDENTIFICATION D'UN PROTOCOLE À L'ORIGINE D'UN FLUX DE DONNÉES

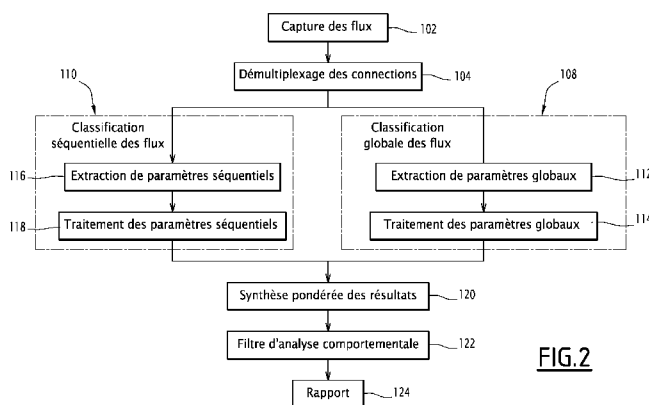


FIG.2

(57) Abstract : Method of identifying a protocol at the origin of a data flow. The method of identifying a protocol giving rise to a packet flow comprises the following steps: - a capture (102) of the flow of the protocol to be identified, - statistical classification of the flow, comprising an extraction of the classification parameters and a comparison of the classification parameters with statistical models constructed during a learning phase. The statistical classification comprises: - a first phase (108) of global statistical classification; and - a step (120) of synthesis of the results of the first and second classification phases (108, 110) so as to identify the protocol giving rise to the flow.

(57) Abrégé : Le procédé d'identification d'un protocole à l'origine d'un flux de paquets comporte les étapes suivantes : une capture (102) du flux du protocole à identifier; une classification statistique du flux, comprenant une extraction des paramètres de classification et une comparaison des paramètres de classification à des modèles statistiques construits lors d'une phase d'apprentissage. La classification statistique comporte : une première phase (108) de classification statistique globale; et une étape (120) de synthèse des résultats des première et seconde phases de classification (108, 110) pour identifier le protocole à l'origine du flux.

102... Capture of the flows
104... Demultiplexing of the connections
110... Sequential classification of the flows
116... Extraction of sequential parameters
118... Processing of the sequential parameters
108... Global classification of the flows
112... Extraction of global parameters
114... Processing of the global parameters
120... Weighted synthesis of the results
122... Behavioural analysis filter
124... Report



Publiée :

- *sans rapport de recherche internationale, sera republiée
dès réception de ce rapport (règle 48.2.g)*