(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
3 janvier 2014 (03.01.2014)

WIPO | PCT

(10) Numéro de publication internationale
WO 2014/001708 A1

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

(21) Numéro de la demande internationale : PCT/FR2013/051480

(22) Date de dépôt international : 25 juin 2013 (25.06.2013)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1256015 25 juin 2012 (25.06.2012) FR

(71) Déposant : **SIGFOX** [FR/FR]; 425 Rue Jean Rostand, F-31670 Labege (FR).

(72) Inventeurs : **FOURTET, Christophe**; 115 Chemin de la Moissagaise, F-82170 Pompignan (FR). **SELLIER, Laurence**; 2 Rue du Moulin Bayard, F-31000 Toulouse (FR).

(74) Mandataires : **PALIX, Stéphane** et al.; Cabinet Laurent & Charras, Le Contemporain, 50 Chemin de la Bruyère, F-69574 Dardilly Cédex (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, 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, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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, 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))*

[Suite sur la page suivante]

(54) **Title** : METHOD FOR AUTHENTICATING DATA PACKETS RECEIVED BY A STATION OF A DIGITAL TELECOMMUNICATIONS SYSTEM

(54) **Titre** : PROCEDE D'AUTHENTIFICATION DE PAQUETS DE DONNEES RECUS PAR UNE STATION D'UN SYSTEME DE TELECOMMUNICATIONS NUMERIQUE

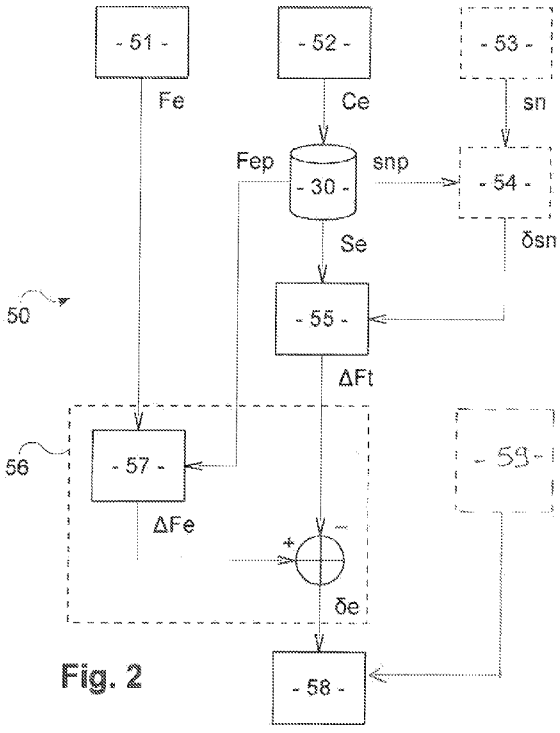


Fig. 2

(57) **Abstract** : The present invention relates to a method for authenticating data packets transmitted by terminals (10) and received by a station (20), each terminal (10) sequentially transmitting data packets in a plurality of different frequency bands according to a predefined sequence of frequency hops that is specific to said terminal, characterised in that it comprises, for a data packet received by the station (20), the steps of: i) measuring (51) the frequency band in which the data packet in question was received; ii) extracting (52) an identification code from said data packet in question; iii) determining (55) a theoretical frequency hop in accordance with the sequence of frequency hops associated with said identification code extracted from the data packet in question; and iv) calculating (56) a frequency hop deviation in accordance with the theoretical frequency hop and the frequency bands measured for the data packet in question and for the preceding data packet. The authentication method (50) comprises a step (58) of determining whether the data packets received sequentially with a single identification code were transmitted by the terminal (10) associated with said identification code in accordance with at least one frequency hop deviation.

(57) **Abrégé** :

[Suite sur la page suivante]

WO 2014/001708 A1

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues (règle 48.2.h))*

La présente invention concerne un procédé (50) d'authentification de paquets de données émis par des terminaux (10) et reçus par une station (20), chaque terminal (10) émettant successivement des paquets de données dans une pluralité de bandes fréquentielles différentes selon une séquence de sauts de fréquence prédéfinie spécifique dudit terminal, caractérisé en ce qu'il comporte, pour un paquet de données reçu par la station (20), des étapes de i)(51) mesure de la bande fréquentielle dans laquelle le paquet de données considéré a été reçu, ii) (52) extraction d'un code d'identification à partir dudit paquet de données considéré,iii) (55) détermination d'un saut de fréquence théorique en fonction de la séquence de sauts de fréquence associée audit code d'identification extrait du paquet de données considéré, et iv) (56) calcul d'un écart de saut de fréquence en fonction du saut de fréquence théorique et des bandes fréquentielles mesurée pour le paquet de données considéré et pour le précédent paquet de données. Le procédé (50) d'authentification comporte une étape (58) de détermination si les paquets de données reçus successivement avec un même code d'identification ont été émis par le terminal (10) associé à ce code d'identification en fonction d'au moins un écart de saut de fréquence.