

**PROCEDE D'AUTHENTIFICATION DE PAQUETS DE DONNEES RECUS PAR
UNE STATION D'UN SYSTEME DE TELECOMMUNICATION NUMERIQUE**

Domaine technique

- 5 La présente invention appartient au domaine des télécommunications numériques, et concerne plus particulièrement l'authentification de paquets de données émis par des terminaux et reçus par une station.

Etat de la technique

- 10 L'authentification de paquets de données reçus par une station vise à vérifier l'identité du terminal ayant émis ces paquets de données.

De nombreux procédés d'authentification sont connus, généralement applicables à des systèmes de télécommunication de type déterministes et syntonisés. De tels systèmes
15 sont :

- soit basés sur des échanges bidirectionnels entre un terminal et une station par lesquels le terminal et la station se synchronisent et s'authentifient mutuellement ;
- soit basés sur des échanges unidirectionnels entre un terminal et une station de réception, et sur une organisation temporelle et/ou fréquentielle déterministe et connue à
20 l'avance permettant d'obtenir la synchronisation du terminal et de la station.

En outre, dans ce type de système déterministe et syntonisé, l'erreur de fréquence acceptable doit être inférieure, ou de l'ordre de grandeur de la bande passante du système.

- 25 Or, dans un système de télécommunication syntonisé, comme celui présenté dans le document US 2001/004375, les terminaux et la station considèrent une même liste prédéfinie de bandes fréquentielles dans lesquelles les paquets de données peuvent être émis. De ce fait, dans ce type de système, il est possible de vérifier si la séquence prédéfinie de sauts de fréquence a été respectée en comparant directement la bande
30 fréquentielle mesurée à la bande fréquentielle attendue parmi les bandes fréquentielles de la liste prédéfinie.

Ce type de vérification n'est plus possible dans les systèmes de télécommunications non syntonisés car il existe une inadéquation entre les bandes fréquentielles utilisées par

-2-

les terminaux et les bandes fréquentielles théoriques attendues par la station réceptrice. Ceci est d'autant plus vrai lorsque la dérive fréquentielle des moyens de synthèse fréquentielle des terminaux est importante. De tels systèmes non déterministes comprennent des systèmes unidirectionnels dans lesquels les communications sont
5 possibles uniquement du terminal vers la station. Un tel système télécommunication dans lequel la dérive des moyens de synthèse fréquentielle des terminaux est supérieure à la largeur spectrale instantanée des paquets de données émis par lesdits terminaux, est présenté dans le document WO 2011/154466.

10 On comprend donc que les procédés d'authentification développés pour les systèmes de télécommunication déterministes et syntonisés ne sont pas applicables à des systèmes de télécommunications de type non déterministes, non synchronisés et non syntonisés, dans lesquels l'organisation temporelle et fréquentielle des communications entre le terminal et la station ne répond à aucun impératif de prédétermination, de
15 synchronisation ou de syntonisation. En outre, dans ce type de systèmes non syntonisés, l'erreur de fréquence peut être supérieure à la bande passante du système.

Par ailleurs, les procédés d'authentification conventionnels reposent généralement sur l'inclusion dans les paquets de données, outre d'un code d'identification du terminal,
20 de données de contrôle additionnelles dédiées à l'authentification dudit terminal ayant émis lesdits paquets de données.

L'ajout de ces données de contrôle dédiées à l'authentification du terminal contribue à réduire le rapport entre la quantité de données utiles et la quantité de données
25 de contrôle présentes dans chaque paquet de données. Ce rapport sera d'autant plus réduit que la quantité de données utiles présente dans chaque paquet de données est faible, comme c'est par exemple le cas dans les systèmes de télécommunications bas débit.

Exposé de l'invention

30 La présente invention a pour objectif de remédier à tout ou partie des limitations des solutions de l'art antérieur, notamment celles exposées ci-avant, dans le cas de systèmes de télécommunications numériques de type unidirectionnel et non-déterministes. Dans de tels systèmes, chaque terminal émet successivement des paquets de données dans une pluralité de bandes fréquentielles différentes qui ne sont pas prédéterminées, et selon une

-3-

séquence de sauts de fréquence prédéfinie et spécifique du terminal. Par ailleurs, chaque paquet de données incorpore un code d'identification du terminal l'ayant émis.

A cet effet, et selon un premier aspect, l'invention concerne un procédé
5 d'authentification comprenant, pour chaque paquet de données reçu par un système récepteur comprenant au moins une station :

- la mesure, par la station ayant reçu le paquet de données considéré, de la bande fréquentielle dans laquelle le paquet de données considéré a été reçu,
- l'extraction du code d'identification contenu dans le paquet de données considéré,
- 10 - le calcul d'un saut de fréquence, à partir de la bande fréquentielle mesurée du paquet considéré et d'une bande fréquentielle mesurée par le système récepteur pour un précédent paquet de données reçu incorporant un code d'identification identique au code d'identification extrait,
- la détermination, en fonction de la séquence de sauts de fréquence prédéterminée
15 associée au code d'identification extrait du paquet de données considéré, d'un saut de fréquence théorique appliqué depuis le précédent paquet de données reçu, et
- le calcul d'un écart de saut de fréquence en fonction du saut de fréquence théorique et du saut de fréquence calculé.

20 En outre, le procédé d'authentification comprend une étape de détermination si les paquets de données reçus successivement avec un même code d'identification ont été émis par le terminal associé au code d'identification extrait en fonction d'au moins un écart de saut de fréquence calculé pour l'un des paquets de données.

25 En résumé, pour chaque paquet de données, un écart de saut de fréquence est calculé en fonction du saut de fréquence théorique, de la bande fréquentielle mesurée pour le paquet de données considéré et de la bande fréquentielle mesurée pour le précédent paquet de données reçu avec le même code d'identification. Le procédé d'authentification est donc robuste à l'absence éventuelle de syntonisation entre les
30 terminaux et la station.

Le système récepteur selon l'invention peut être formé soit d'un ensemble constitué d'une ou de plusieurs stations, soit d'un ensemble constitué d'un ou de plusieurs stations en coopération avec un serveur de traitement.

Ainsi, la mesure de la bande fréquentielle d'émission du paquet de données considéré est réalisée dans le référentiel de la station ayant reçu le paquet de données considéré. De ce fait, dans le cas où le système récepteur comprend notamment plusieurs stations, chaque station réalisera les mesures des bandes fréquentielles des paquets qu'il reçoit. Ces mesures de bande fréquentielle sont ainsi obtenues indépendamment des conditions d'émission par le terminal et des différences de conditions de réception entre les stations.

10 En outre, dans certaines conditions extrêmes de réception, on peut observer pendant la réception d'un même paquet, une variation de fréquence dans le référentiel de réception. Cela conduit à une ambiguïté dans le calcul de l'écart de saut de fréquence. Dans ces conditions, la décision d'authentification peut être basée sur le cumul des écarts de plusieurs sauts de fréquence calculés successivement, ou toute autre opération
15 statistique appliquée à une série de valeurs d'écarts de saut de fréquences calculés successivement.

Dans une variante, il est également possible de mettre en place un système d'apprentissage par rapport à l'historique des écarts calculés, et d'ajuster dynamiquement
20 le critère de seuil relatif à la différence maximale acceptable entre les écarts.

De telles dispositions permettent d'écarter des paquets de données émis par un terminal malveillant essayant de se faire passer pour un terminal autorisé. En effet, on comprend que si un terminal malveillant essaie de se faire passer pour un terminal
25 autorisé en utilisant le code d'identification dudit terminal autorisé, mais sans connaître la séquence de sauts de fréquence prédéfinie associée audit terminal autorisé, le ou les écarts de sauts de fréquence calculés seront importants et permettront de déterminer que tout ou partie de ces paquets de données ont été émis par un terminal malveillant.

30 Le procédé d'authentification objet de l'invention est particulièrement adapté aux systèmes de télécommunications non syntonisés, c'est-à-dire dans lesquels les terminaux et la station ne sont pas synchronisés en fréquence. En outre, une telle authentification ne nécessite pas de prérequis notoire sur le système de télécommunication, et est donc

-5-

applicable par extension à tout système de télécommunication, unidirectionnel ou non, syntonisé ou non, synchronisé ou non.

Par ailleurs, il est à noter qu'un tel procédé d'authentification est particulièrement
5 adapté aux systèmes de télécommunications bas débit.

A titre d'exemple illustratif, on considère un terminal émettant systématiquement avec un biais fréquentiel δF par rapport à la station réceptrice, c'est-à-dire que ledit terminal émet dans une bande fréquentielle $F1+\delta F$ lorsqu'il est censé émettre dans une
10 bande fréquentielle $F1$, puis dans une bande fréquentielle $F2+\delta F$ au lieu de $F2$ ($F2$ étant égal à $F1+\Delta F$, ΔF étant le saut de fréquence théorique), etc. Dans ce cas, l'écart de bande fréquentielle, c'est-à-dire l'écart entre la bande fréquentielle dans laquelle le terminal émet et la bande fréquentielle théorique attendue par la station, est toujours sensiblement égal à δF (aux erreurs de mesure près lorsque les conditions environnementales sont
15 équivalentes, en terme de température et de tension). L'écart de saut de fréquence est lui sensiblement nul (aux erreurs de mesure près) puisque le saut de fréquence entre la bande fréquentielle $F1+\delta F$ et la bande fréquentielle $F2+\delta F$ est égal au saut de fréquence théorique ΔF .

20 Dans des modes particuliers de mise en œuvre, le procédé d'authentification comporte l'une ou plusieurs des caractéristiques suivantes, prises isolément ou selon toutes les combinaisons techniquement possibles.

Dans un mode particulier de mise en œuvre, la bande fréquentielle d'un paquet de
25 données est mesurée plusieurs fois au cours de chaque paquet de données, et l'écart de saut de fréquence est calculé en considérant la bande fréquentielle mesurée finale du paquet de données considéré et la bande fréquentielle mesurée finale du précédent paquet de données incorporant le même code d'identification que le paquet de données considéré.

30

De telles dispositions permettent d'éviter certains cas d'échecs d'authentification, dans le cas notamment de terminaux dont la dérive fréquentielle des moyens de synthèse fréquentielle est importante (comme par exemple le système présenté dans le document

WO 2011/154466), et dont la bande fréquentielle utilisée par un terminal peut varier de façon non négligeable au sein d'un même paquet de données.

Dans ce cas de figure, le comportement de dérive fréquentielle à l'allumage d'un oscillateur d'un terminal émetteur présente un motif particulier unique et parfaitement répétable, modélisable en fonction du temps. Ce motif particulier représente une sorte de « signature » qui dépend de l'assemblage unique des composants électroniques dans le terminal émetteur. En pratique, on peut avantageusement tirer parti de cette signature en considérant la bande fréquentielle mesurée à la fin du paquet de données considéré et la bande fréquentielle mesurée à la fin du précédent paquet de données incorporant le même code d'identification, et présentant donc le même motif de dérive fréquentielle (tout autre paramètre environnemental étant considéré constant). On comprend que les variations de bande fréquentielle sur deux trames successives ou non, et de même longueur sera identique si elles sont mesurées au même moment par rapport à l'allumage des circuits du terminal émetteur.

De ce fait, afin de renforcer le procédé d'authentification objet de l'invention, il est possible de mettre en œuvre des étapes complémentaires en exploitant la dérive fréquentielle de l'oscillateur du terminal émetteur. Ainsi, avantageusement, le procédé d'authentification peut en outre comprendre, pour chaque paquet de données reçu par le système récepteur :

- la mesure, par ce système récepteur, d'un motif de dérive fréquentielle d'un oscillateur ayant servi à générer le paquet de données considéré, et
- la comparaison du motif de dérive fréquentielle mesuré avec un motif de dérive fréquentielle prédéfini associé audit code d'identification extrait dudit paquet de données considéré.

En particulier, dans un contexte d'économie de la batterie du terminal émetteur, il n'est pas souhaitable de mettre l'oscillateur en fonctionnement bien avant l'envoi d'une trame, pour laisser le temps à l'oscillateur de se stabiliser. De ce fait, dans ce contexte d'économie, l'oscillateur est généralement activé juste au moment de l'envoi de la trame et la trame contient donc forcément la « signature » représentative de la dérive fréquentielle de l'oscillateur.

-7-

Par exemple, la bande fréquentielle d'un paquet de données peut être mesurée plusieurs fois au cours de chaque paquet de données. Ces mesures multiples peuvent ainsi servir à établir le modèle du motif particulier unique de comportement de dérive fréquentielle du terminal émetteur, à savoir sa « signature », sur le paquet donné. Ce
5 modèle peut ensuite être comparé à un motif de référence unique et connu du terminal émetteur ayant émis le paquet et relevé par exemple lors de sa fabrication ou de sa mise en service.

En pratique, afin de pouvoir déterminer le saut de fréquence théorique
10 correspondant à deux paquets reçus consécutivement, il est avantageux de s'assurer que ces deux paquets ont été émis consécutivement. Lorsque des trames perdues sont détectées, il est avantageux de recalculer l'écart de saut de fréquence théorique en fonction du nombre de trames perdues.

15 Ainsi, dans un mode particulier de mise en œuvre, le procédé d'authentification comprend, après l'étape d'extraction du code d'identification à partir du paquet de données considéré, une étape d'estimation d'un nombre de paquets de données perdus, lesdits paquets de données perdus correspondant à des paquets de données qui ont été émis par le terminal associé audit code d'identification depuis que le précédent paquet de
20 données incorporant ledit code d'identification a été reçu, mais qui n'ont pas été reçus par le système récepteur, et notamment par la station. Le saut de fréquence théorique pour le paquet de données considéré est alors déterminé en fonction du nombre de paquets de données perdus et de la séquence de sauts de fréquence associée audit code d'identification.

25

De telles dispositions permettent également d'éviter certains cas d'échecs d'authentification. En effet, le saut de fréquence entre deux paquets de données reçus par la station peut correspondre à la somme de plusieurs sauts de fréquence consécutifs, si des paquets de données ont été émis entre lesdits deux paquets de données mais n'ont pas été
30 reçus par la station. L'estimation du nombre de paquets perdus permet alors de déterminer le nombre de sauts de fréquence effectués, et par conséquent d'estimer le saut de fréquence théorique comme étant la somme desdits sauts de fréquence effectués.

-8-

Dans un mode particulier de mise en œuvre, dans lequel les paquets de données incorporent un compteur incrémenté par le terminal à chaque nouvelle émission, le nombre de paquets perdus est estimé en fonction du compteur du paquet de données considéré et du compteur du précédent paquet de données reçu incorporant le même code d'identification que ledit paquet de données considéré.

Dans un mode particulier de mise en œuvre, dans lequel les paquets de données comportent une partie chiffrée au moyen d'un clé tournante incrémentée par le terminal à chaque nouvelle émission, le nombre de paquets perdus est estimé en fonction de la clé tournante utilisée pour le paquet de données considéré et de la clé tournante utilisée pour le précédent paquet de données reçu incorporant le même code d'identification que ledit paquet de données considéré.

Dans un mode particulier de mise en œuvre, dans lequel les paquets de données sont émis par un terminal avec une période prédéfinie, le nombre de paquets perdus est estimé en fonction de ladite période et d'un écart temporel entre la réception du paquet de données considéré et la réception du précédent paquet de données incorporant le même code d'identification que ledit paquet de données considéré.

Dans un mode particulier de mise en œuvre, les paquets de données reçus successivement avec un même code d'identification ne sont considérés comme ayant été émis par le terminal associé audit code d'identification que si chaque écart de saut de fréquence considéré pour l'authentification est de valeur absolue inférieure à une valeur seuil.

25

De préférence, la valeur seuil à utiliser pour le paquet de données considéré est déterminée en fonction d'un écart temporel entre la réception du paquet de données considéré et la réception du précédent paquet de données incorporant le même code d'identification que ledit paquet de données considéré.

30

Dans un mode particulier de mise en œuvre, dans lequel plusieurs écarts de saut de fréquence sont considérés pour l'authentification, les paquets de données reçus successivement avec un même code d'identification ne sont considérés comme ayant été émis par le terminal associé audit code d'identification que si un critère prédéfini

-9-

d'authentification est vérifié par l'ensemble des écarts de sauts de fréquence considérés pour l'authentification.

En d'autres termes, le diagnostic de validité des paquets peut être retardé jusqu'à ce
5 qu'un critère de validation d'ensemble soit rempli, ce critère statistique validant à posteriori l'ensemble des paquets en attente de validation. Dans ces conditions, le système se trouve parfois en attente d'une validation d'un sous ensemble de paquets.

Dans un mode particulier de mise en œuvre, le critère d'authentification est vérifié
10 si le cumul des écarts de sauts de fréquence considérés pour l'authentification est inférieur à une valeur seuil prédéfinie.

Avantageusement, la vérification du critère d'authentification peut également être basée sur l'espérance, la variance ou toute autre propriété statistique sur les écarts de sauts
15 de fréquence considérés pour l'authentification.

Dans un mode particulier de mise en œuvre, le système récepteur peut comprendre un serveur fédérateur (communément appelé « backbone » dans le contexte de l'invention) coopérant avec une ou plusieurs station(s). Dans ce cas, les opérations du
20 procédé d'authentification sont de préférence réparties entre le serveur et la ou les station(s).

De préférence, la station réalise les mesures de bande fréquentielle des paquets de données qu'il reçoit, et le serveur collecte l'ensemble des paquets de données reçus par
25 chaque station et les bandes fréquentielles mesurées par chaque stations, et réalise au moins les opérations restantes du procédé d'authentification présenté ci-avant.

Selon un second aspect, l'invention concerne un produit programme d'ordinateur comportant un ensemble d'instructions de code de programme qui, lorsqu'elles sont
30 exécutées par un processeur, mettent en œuvre un procédé d'authentification selon l'invention.

Selon un troisième aspect, la présente invention concerne un système récepteur comprenant au moins une station d'un système de télécommunications numérique, adapté

-10-

à recevoir des paquets de données émis par des terminaux, chaque paquet de données incorporant un code d'identification du terminal ayant émis ledit paquet de données, chaque terminal émettant successivement des paquets de données dans une pluralité de bandes fréquentielles différentes selon une séquence de sauts de fréquence prédéfinie
5 spécifique dudit terminal. Ce système récepteur comprend en outre des moyens configurés pour authentifier les paquets de données reçus conformément à un procédé selon l'invention.

Dans une implémentation alternative autorisant un déploiement évolutif (ou
10 scalable), le système récepteur peut comprendre des stations aptes à recevoir les paquets émis par les terminaux et un serveur de fédération (ou backbone). Chaque station comprend de préférence des moyens de communication avec le serveur et des moyens pour réaliser une partie du procédé d'authentification selon l'invention. Le serveur comprend de préférence des moyens pour réaliser l'autre partie du procédé
15 d'authentification des paquets de données reçus conformément à l'invention.

Selon un quatrième aspect, la présente invention concerne un système de télécommunication comprenant :

- des terminaux, chaque terminal étant apte à émettre successivement des paquets de
20 données dans une pluralité de bandes fréquentielles différentes selon une séquence de sauts de fréquence prédéfinie spécifique dudit terminal, chaque paquet de données incorporant un code d'identification du terminal (10) ayant émis ledit paquet de données,
- des stations coopérant avec un serveur fédérateur pour réaliser le procédé d'authentification conformément à l'invention,
- 25 - chaque station étant apte à réaliser les mesures de bande fréquentielle des paquets de données qu'il reçoit ; et
- le serveur étant apte à collecter l'ensemble des paquets de données reçus par chaque station et les bandes fréquentielles mesurées par chaque stations, et étant apte à réaliser au moins les opérations restantes du procédé d'authentification selon
30 l'invention qui ne sont pas réalisés par la station.

Présentation des figures

L'invention sera mieux comprise à la lecture de la description suivante, donnée à titre d'exemple nullement limitatif, et faite en se référant aux figures qui représentent :

-11-

- Figure 1 : une représentation schématique d'un système de télécommunications numériques, et
- Figure 2 : un diagramme illustrant les étapes d'un exemple de mise en œuvre d'un procédé d'authentification selon l'invention.

5

Exposé détaillé d'un mode de réalisation particulier

La figure 1 représente, de façon très schématique, un système de télécommunications comprenant un ou plusieurs émetteurs tels que des terminaux **10** et une ou plusieurs stations **20** (une seule station a été représentée sur la figure 1 pour des
10 raisons de clarté). Dans le contexte de l'invention, on entend de manière générale par « station » tout dispositif adapté à recevoir des paquets de données sous la forme de signaux radioélectriques. La station **20** est par exemple un dispositif particulier tel qu'un point d'accès à un réseau filaire ou non filaire de télécommunications.

15 On entend par « signal radioélectrique » une onde électromagnétique se propageant via des moyens non filaires, dont les fréquences sont comprises dans le spectre traditionnel des ondes radioélectriques (quelques hertz à plusieurs centaines de gigahertz) ou dans des bandes de fréquences voisines.

20 Il est à noter qu'on considère principalement le cas d'une émission de paquets de données par des terminaux **10** vers la station **20**. L'émission éventuelle de paquets de données par la station **20** vers les terminaux **10** sort du cadre de l'invention.

Les terminaux **10** émettent des paquets de données à destination de la station **20**
25 dans une ressource fréquentielle partagée, dite « macrocanal » (ou bande de multiplexage des signaux correspondant à la bande de réception de la station) dans le jargon des réseaux de télécommunication, de largeur spectrale ΔM .

Les paquets de données sont émis par les terminaux **10** dans des bandes
30 fréquentielles de largeur spectrale ΔB prédéfinie inférieure à ΔM . De préférence, la largeur spectrale ΔM du macrocanal est significativement supérieure à la largeur spectrale ΔB , afin de pouvoir multiplexer un grand nombre de terminaux **10**. Par exemple, la largeur spectrale ΔM est au moins cent fois supérieure à la largeur spectrale ΔB .

-12-

Chaque terminal **10** émet des paquets de données de manière récurrente à destination de la station **20**. Des paquets de données émis successivement par un même terminal **10** sont émis dans des bandes fréquentielles différentes selon une séquence de sauts de fréquence prédéfinie spécifique dudit terminal **10**. En outre, chaque paquet de données incorpore un code d'identification du terminal **10** ayant émis ledit paquet de données.

Dans une variante, un serveur fédérateur **40**, communément appelé « backbone » dans le contexte des réseaux de télécommunication, peut être associé à ces stations **20** comme illustré sur la figure 3.

De ce fait, par la suite, le terme « émetteur » se rapportera à un terminal **10**, et le terme « système récepteur » se rapportera indifféremment à une station ou à un ensemble formé d'au moins une station en coopération avec un serveur fédérateur (backbone).

En outre, dans la description suivante, les terminaux sont désignés par la même référence **10**. Lorsqu'il est nécessaire de distinguer un terminal d'un autre terminal, la référence correspondante est accompagnée d'un indice alphabétique spécifique au terminal considéré. Par exemple, un terminal quelconque considéré de manière générale sera désigné par **10**, tandis que les terminaux **10a**, **10b**, **10c**, etc. correspondront à des terminaux particuliers.

Suivant un exemple non limitatif, un terminal **10a** est configuré pour émettre dans des bandes fréquentielles successives définies par une bande fréquentielle de base F_a et une séquence S_a comportant $(N-1)$ sauts de fréquence successifs $S_a = \{\Delta F_{a1}, \Delta F_{a2}, \dots, \Delta F_{a_{N-1}}\}$. Ainsi, le terminal **10a** émet d'abord un paquet de données dans la bande fréquentielle F_a , puis dans la bande fréquentielle $(F_a + \Delta F_{a1})$, puis dans la bande fréquentielle $(F_a + \Delta F_{a1} + \Delta F_{a2})$, etc. L'ensemble des sauts de fréquence de la séquence S_a est par exemple choisi tel que :

$$\sum_{n=1}^{N-1} \Delta F_{a_n} = 0$$

de sorte que, après avoir appliqué l'ensemble des sauts de fréquence de la séquence S_a , le terminal **10a** émet à nouveau, théoriquement, dans la bande fréquentielle de base F_a .

De manière analogue, un terminal **10b** se voit associer une bande fréquentielle de base F_b et une séquence S_b spécifique de $(M-1)$ sauts de fréquence successifs $S_b = \{\Delta F_{b1}, \Delta F_{b2}, \dots, \Delta F_{bM-1}\}$, un terminal **10c** se voit associer une bande fréquentielle de base F_c et une séquence S_c spécifique de $(P-1)$ sauts de fréquence successifs $S_c = \{\Delta F_{c1}, \Delta F_{c2}, \dots, \Delta F_{cP-1}\}$, etc.

Les longueurs M , N , P , et de façon générale toute longueur de séquence peut être choisie indépendamment et arbitrairement. En particulier, elles peuvent être choisies arbitrairement grandes, de façon à ce que la séquence ne présente pas ce cycle répétitif apparent.

La séquence de sauts de fréquence de chaque terminal **10** (c'est à dire la séquence S_a du terminal **10a**, la séquence S_b du terminal **10b**, la séquence S_c du terminal **10c**, etc.) peut être obtenue soit la station **20**, soit par le serveur **40** (backbone). Par exemple, la station **20** peut comprendre une mémoire électronique **30** dans laquelle est mémorisée une table de correspondance associant, à chaque code d'identification possible, la séquence de sauts de fréquence correspondante. Bien entendu, cette table de correspondance peut être mémorisée dans le serveur **40**.

20

Une implémentation préférentielle est celle où chaque station **20** effectue la réception et la mesure de la bande fréquentielle, et le serveur **40** collecte l'ensemble des paquets et les mesures fréquentielles mesurées par la ou les stations **20**, et effectue l'opération d'authentification en utilisant l'ensemble des résultats de manière comparative pour consolider et fiabiliser le diagnostic.

Dans l'exemple ci-dessus, les séquences de sauts de fréquence sont cycliques, de façon apparente ou non. Rien n'exclut, suivant d'autres exemples, d'avoir des séquences de sauts de fréquences non cycliques, par exemple générées au moyen d'un registre à décalage à rétroaction linéaire, ou LFSR (acronyme de l'anglais « Linear Feedback Shift Register »), dont le ou les polynômes générateurs prédéfinis peuvent être obtenus par la station **20**.

Dans la suite de la description, on se place de manière non limitative dans un système de télécommunications numériques tel que décrit dans la demande internationale WO 2011/154466, dans lesquels les paquets de données sont à bande étroite (largeur spectrale ΔB de l'ordre de quelques hertz à quelques centaines de hertz) et la dérive en
5 fréquence des moyens de synthèse fréquentielle des terminaux est supérieure à la largeur spectrale ΔB .

Par conséquent, le terminal **10a**, lorsqu'il émet théoriquement dans la bande fréquentielle de base F_a , émet en pratique dans une bande fréquentielle $F'a$ qui peut être
10 séparée de la bande fréquentielle de base F_a d'une largeur spectrale supérieure à ΔB . De manière analogue, les sauts de fréquence $\{\Delta F'a_1, \Delta F'a_2, \dots, \Delta F'a_{N-1}\}$ pourront différer des sauts de fréquence $\{\Delta F_a1, \Delta F_a2, \dots, \Delta F_a_{N-1}\}$. Cependant, l'erreur entachant le saut de fréquence est bien moindre que celle entachant la bande fréquentielle. En effet, dans un système non syntonisé dans lequel la station réalisant les mesures de bande fréquentielle
15 présente une précision en fréquence de 10ppm par exemple, non corrigé ni compensé par un mécanisme de synchronisation, l'erreur de fréquence induite pour la bande fréquentielle de base F_a autour de 1GHz est de 10kHz, alors que l'erreur de fréquence sur un saut de 10kHz n'est que de 0.1Hz. Par conséquent, la valeur du saut de fréquence est parfaitement discriminante, alors que la fréquence F_a elle-même ne l'est pas.

20

On comprend donc qu'un avantage du procédé d'authentification de la présente invention réside dans le fait que, ni la station **20** ni le serveur **40** (backbone), bien qu'ils aient accès aux séquences de sauts de fréquence de chaque terminal **10**, ne savent ni n'ont besoin de discriminer directement dans quelle bande fréquentielle un terminal **10** a émis
25 un paquet à des fins d'authentification. Ce procédé d'authentification diffère fondamentalement des procédés déterministes tels que décrit dans le document US2001/0004375, qui se base sur la mesure et la discrimination de fréquence afin d'authentifier les paquets.

30 Dans un mode particulier de réalisation, la station **20** comporte un module de réception analogique et un module de réception numérique.

Le module de réception analogique est adapté à recevoir un signal global correspondant à l'ensemble des signaux radioélectriques reçus dans le macrocanal. Il

-15-

comporte à cet effet un ensemble de moyens, considérés comme connus de l'homme de l'art (antennes, filtres analogiques, amplificateurs, oscillateurs locaux, mélangeurs, etc.), adaptés à traduire fréquemment le signal global.

- 5 Le module de réception analogique présente en sortie un signal analogique correspondant au signal global ramené autour d'une fréquence intermédiaire inférieure à la fréquence centrale de la bande de multiplexage, pouvant être nulle.

- 10 Le module de réception numérique comporte, de manière conventionnelle, un ou plusieurs convertisseurs analogique/numérique (A/N) adaptés à échantillonner le ou les signaux analogiques fournis par le module de réception analogique de sorte à obtenir un signal numérique.

- 15 Le module de réception numérique comporte en outre une unité de traitement du signal numérique en sortie des convertisseurs A/N. L'unité de traitement effectue, à partir du signal numérique, une détection de paquets de données émis par des terminaux 10 et présents dans le signal global. L'unité de traitement exécute également les étapes d'un procédé 50 d'authentification des paquets de données détectés, décrit plus en détail ci-après.

20

Dans une variante préférentielle, le procédé d'authentification 50 peut être réparti entre une unité de calcul allouée par le serveur 40 et une unité de calcul de la station 20.

- 25 L'unité de traitement comporte par exemple un processeur et une mémoire électronique dans laquelle est mémorisé un produit programme d'ordinateur, sous la forme d'un ensemble d'instructions de code de programme qui, lorsqu'elles sont exécutées par le processeur, mettent en œuvre tout ou partie des étapes d'un procédé 50 d'authentification. Dans une variante, l'unité de traitement comporte des circuits logiques programmables, de type FPGA, PLD, etc., et/ou circuits intégrés spécialisés (ASIC), 30 adaptés à mettre en œuvre tout ou partie des étapes dudit procédé 50 d'authentification.

La figure 2 représente un mode préféré de mise en œuvre d'un procédé 50 d'authentification des paquets de données reçus par la station 20.

-16-

Le procédé **50** d'authentification comporte des étapes qui sont exécutées par le système récepteur pour chaque paquet de données reçu, dont les principales sont :

- **51** mesure de la bande fréquentielle dans laquelle le paquet de données considéré a été reçu,
- 5 - **52** extraction du code d'identification à partir dudit paquet de données considéré,
- **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,
- 10 - **56** calcul d'un écart de saut de fréquence en fonction du saut de fréquence théorique, de la bande fréquentielle mesurée pour le paquet de données considéré et de la bande fréquentielle mesurée pour le précédent paquet de données reçu incorporant le même code d'identification que ledit paquet de données considéré.

Au cours de l'étape **51** de mesure, la station **20** mesure la bande fréquentielle du
15 paquet de données considéré, désignée ci-après par « Fe » puis extrait le code d'identification au cours de l'étape **52** d'extraction, ci-après désigné par « Ce ».

Pour la description du mode de mise en œuvre illustré par la figure 2, on se place de manière non limitative dans le cas où le code d'identification Ce extrait du paquet de
20 données considéré correspond au code d'identification associé au terminal **10a**.

A partir du code d'identification Ce, l'unité de calcul, situé soit dans la station **20** soit dans le serveur **40** (backbone), obtient la séquence de sauts de fréquence associée audit code d'identification Ce, préalablement mémorisée dans la mémoire
25 électronique **30**, et obtient la séquence Sa de sauts de fréquence associée au terminal **10a**.

L'unité de calcul obtient également des informations relatives au précédent paquet de données reçu avec le code d'identification Ce, c'est-à-dire dans le cas présent reçu du terminal **10a**. Ces informations ont été préalablement mémorisées dans la base de données
30 du réseau, suite à l'exécution des étapes du procédé **50** d'authentification pour un précédent paquet de données reçu du terminal **10a**.

Notamment, l'unité de calcul obtient la bande fréquentielle mesurée pour le précédent paquet de données au cours de l'étape **51** de mesure et mémorisée dans la mémoire électronique **30**, désignée ci-après par « Fep ».

5 Dans le mode particulier de mise en œuvre illustré par la figure 2, on se place de manière non limitative dans le cas où chaque terminal **10** incorpore dans un paquet de données émis un compteur qui est incrémenté à chaque nouvelle émission par ledit terminal. Par exemple, lorsque le terminal **10a** émet un paquet de données dans la bande fréquentielle de base Fa, le compteur est égal à 0, lorsqu'il émet le paquet de données
10 suivant (dans la bande fréquentielle $Fa + \Delta F1a$), le compteur est égal à 1, etc. Dans ce cas, le procédé **50** d'authentification peut comporter une étape **53** d'extraction du compteur du paquet de données considéré, désigné ci-après par « sn ».

Dans ce cas, les informations, obtenues par la station **20** à partir du code
15 d'identification Ce dans la mémoire électronique **30**, comprennent également le compteur du précédent paquet de données reçu avec le code d'identification Ce, désigné ci-après par « snp ».

Dans le mode particulier de mise en œuvre illustré par la figure 2, le procédé **50**
20 d'authentification comporte en outre une étape **54** d'estimation du nombre de paquets perdus, désigné ci-après par « δsn ». Les paquets de données perdus correspondent, dans le cas présent, à des paquets de données qui ont été émis par le terminal **10a** depuis que le précédent paquet de données reçu du terminal **10a** a été reçu, mais qui n'ont pas été reçus par la station **20**.

25

Le nombre δsn de paquet de données perdus peut être estimé en fonction du compteur sn extrait du paquet de données considéré et du compteur snp extrait du précédent paquet de données reçu avec le même code d'identification Ce. Par exemple, si le compteur sn est égal à n (modulo N) et si le compteur snp est égal à (n-d) (modulo N,
30 $d \geq 1$), alors le nombre δsn de paquets perdus est égal à (d-1) et peut être égal à zéro.

Au cours de l'étape **55**, la station **20** calcule un saut de fréquence théorique, désigné ci-après par « ΔFt », en fonction de la séquence Sa de sauts de fréquence obtenue à partir du code d'identification Ce extrait du paquet de données considéré. Le saut de fréquence

théorique ΔFt correspond au saut de fréquence théoriquement appliqué depuis l'émission du précédent paquet de données reçu avec le même code d'identification C_e .

Le saut de fréquence théorique ΔFt , dans l'exemple illustré par la figure 2, est également calculé en fonction des compteurs sn (égal à n) et snp (égal à $(n-d)$). Dans le cas considéré de paquets de données reçus du terminal **10a**, le saut de fréquence théorique ΔFt est par exemple calculé selon l'expression suivante :

$$\Delta Ft = \sum_{k=sn-\delta sn}^{sn} \Delta Fa_k$$

Par exemple, si $sn = 4$ et $(sn-\delta sn) = 4$ (c'est-à-dire qu'aucun paquet de données n'a été perdu) le saut de fréquence théorique ΔFt est égal à ΔFa_4 . Si $sn = 4$ et $(sn-\delta sn) = 3$ (c'est-à-dire qu'un paquet de données a été perdu) le saut de fréquence théorique ΔFt est égal à $(\Delta Fa_3 + \Delta Fa_4)$, etc.

Au cours de l'étape **56**, la station **20** calcule un écart de saut de fréquence, désigné ci-après par « δe ».

Dans le mode particulier de mise en œuvre illustré par la figure 2, le procédé **50** d'authentification comporte une étape **57** de calcul d'un saut de fréquence réel, désigné ci-après par « ΔFe ». Le saut de fréquence réel ΔFe est calculé en fonction de la bande fréquentielle mesurée Fe et de la bande fréquentielle mesurée Fep , par exemple selon l'expression $\Delta Fe = Fe - Fep$. Dans ce cas, l'écart de saut de fréquence δe est calculé comme étant une distance entre le saut de fréquence théorique ΔFt et le saut de fréquence réel ΔFe , par exemple selon l'expression $\delta e = \Delta Fe - \Delta Ft$.

Rien n'exclut, suivant d'autres exemples, de calculer différemment l'écart de saut de fréquence δe . Dans une variante non illustrée par des figures, le procédé **50** d'authentification comporte une étape de calcul d'une bande fréquentielle théorique dans laquelle le paquet de données considéré aurait dû être reçu, désignée ci-après par « Ft ». La bande fréquentielle théorique Ft est calculée en fonction du saut de fréquence théorique ΔFt et de la bande fréquentielle mesurée Fep , par exemple selon l'expression $Ft = Fep + \Delta Ft$. Dans ce cas, l'écart de saut de fréquence δe est calculé comme étant une distance entre la bande fréquentielle mesurée Fe et la bande fréquentielle théorique Ft , par exemple selon l'expression $\delta e = Fe - Ft$.

De préférence, en particulier lorsque la dérive fréquentielle des moyens de synthèse fréquentielle des terminaux **10** est importante, la bande fréquentielle du paquet de données considéré est mesurée plusieurs fois au cours dudit paquet de données considéré.

5 Par exemple, au cours de l'étape **51** de mesure, la bande fréquentielle est mesurée L fois, de sorte à obtenir des bandes fréquentielles mesurées respectivement Fe_1 (première mesure), Fe_2 , ..., Fe_L (dernière mesure). De même, pour le précédent paquet de données, plusieurs mesures sont effectuées de sorte à obtenir des bandes fréquentielles mesurées respectivement Fep_1 (première mesure), Fep_2 , ..., Fep_L (dernière mesure). Dans ce cas,

10 l'écart de saut de fréquence δe est avantageusement calculé en considérant la bande fréquentielle mesurée Fe_L du paquet de données considéré et la bande fréquentielle mesurée Fep_L du précédent paquet de données incorporant le même code d'identification que ledit paquet de données considéré. Dans le cas illustré par la figure 2, cela revient à calculer le saut de fréquence réel ΔFe selon l'expression $\Delta Fe = Fe_L - Fep_L$.

15

Rien n'exclut cependant, lorsque la bande fréquentielle du paquet de données considéré est mesurée plusieurs fois au cours d'un même paquet de données, de considérer suivant d'autres exemples des moments équivalents du paquet de données considéré et du précédent paquet de données. Par exemple, le saut de fréquence réel ΔFe

20 peut être calculé en considérant les premières mesures (selon l'expression $\Delta Fe = Fe_1 - Fep_1$) ou une autre mesure quelconque (selon l'expression $\Delta Fe = Fe_i - Fep_i$).

Lorsque la dérive fréquentielle des moyens de synthèse fréquentielle des terminaux **10** est importante, il est possible d'identifier le terminal à partir de la signature de sa

25 dérive fréquentielle à l'allumage. En effet, de façon connue de l'homme de l'art, le comportement de dérive en fréquence à l'allumage d'un dispositif électronique synthétisant une fréquence radioélectrique présente un motif unique qui dépend de l'assemblage unique des composants électroniques qui le composent. À partir de l'ensemble des mesures Fe_i , on peut reconstituer ce motif unique, par une opération

30 mathématique, une interpolation par exemple, et le comparer au motif de dérive théorique stocké en base de donnée pour ce dispositif.

Le procédé **50** d'authentification comporte en outre 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 audit code d'identification en fonction d'au moins un écart de saut de fréquence δe calculé pour l'un desdits paquets de données.

De préférence, plusieurs écarts de saut de fréquence, calculés pour différents
5 paquets de données reçus avec un même code d'identification, sont considérés au cours de l'étape **58** de détermination, afin d'améliorer la robustesse de l'authentification. Dans la suite de la description, on se place dans le cas où M écarts de saut de fréquence (respectivement $\delta e_1, \delta e_2, \dots, \delta e_M$) sont considérés au cours de l'étape **58** de détermination.

10 Dans un mode particulier de mise en œuvre de l'étape **58** de détermination, les paquets de données reçus successivement avec le même code d'identification ne sont considérés comme ayant été émis par le terminal **10** associé audit code d'identification que si chaque écart de saut de fréquence $\delta e_1, \delta e_2, \dots, \delta e_M$ est de valeur absolue inférieure à une valeur seuil. La valeur seuil est par exemple prédéfinie en fonction des dérives
15 fréquentielles maximales constatées en fonction des conditions environnementales (température) pour les moyens de synthèse fréquentielle des terminaux **10**.

A titre d'exemple numérique, on reprend l'exemple cité plus haut, c'est-à-dire que l'on considère un système non syntonisé dans lequel :

- 20 - la station réceptrice présente une précision fréquentielle initiale de 10ppm (« parts per million »), non compensé par un mécanisme de synchronisation, l'erreur de fréquence induite pour $F_a=1\text{GHz}$ est de 10kHz,
- le terminal émet des paquets d'occupation spectrale $\Delta B=100\text{Hz}$, et
- la variation en température est typiquement de 10ppm sur la plage autorisée, ou 0.1ppm
25 par degré.

Dans ce cas de figure, d'un paquet à l'autre, une variation typique de 10°C des conditions de température autour de la température de travail va induire entre deux paquets un écart de saut de $0.1\text{Hz} + 1\text{kHz}$. La valeur de seuil à appliquer dans ce cas est
30 autour de 1kHz. Dans des conditions particulières d'implémentation, une variation extrême des conditions de température va induire entre deux paquets un écart de saut de $0.1\text{Hz} + 10\text{kHz}$. L'écart de saut n'est donc plus discriminant en soi, il est donc préférable d'adapter le système d'authentification et d'appliquer une analyse globale sur un grand ensemble de paquets reçus successivement par le réseau. Dans ce cas, l'analyse peut se

-21-

faire sur le comportement statistique de l'ensemble des paquets reçus, en particulier sur l'ensemble des écarts de saut, dont l'espérance et la variance lorsqu'ils présentent des valeurs statistiques réalistes, vont valider l'ensemble des paquets reçus jusqu'à la réalisation du critère statistique. Par contre, si un écart ou si une série d'écarts de saut de
5 fréquence $\delta e_1, \delta e_2, \dots, \delta e_M$ est trop important, les paquets de données reçus successivement avec le même code d'identification ne seront pas considérés comme ayant été émis par le terminal **10** associé audit code d'identification et l'authentification échouera.

10 Dans un autre mode particulier de mise en œuvre de l'étape **58** de détermination, pouvant être combiné avec le précédent, les paquets de données reçus successivement avec le même code d'identification ne sont considérés comme ayant été émis par le terminal **10** associé audit code d'identification que si un critère prédéfini d'authentification est vérifié par l'ensemble desdits écarts de sauts de fréquence $\delta e_1, \delta e_2,$
15 $\dots, \delta e_M$ considérés pour l'authentification.

Par exemple, le critère d'authentification est vérifié si le cumul (somme en valeur absolue ou relative) des écarts de sauts de fréquence $\delta e_1, \delta e_2, \dots, \delta e_M$ considérés pour l'authentification est inférieur à une valeur seuil prédéfinie.

20 En plus des opérations décrites précédemment, il est également possible de mettre en œuvre, de façon indépendante, une étape **59** prenant en compte le motif de dérive fréquentielle de l'oscillateur ayant servi à générer le paquet de données considéré, de manière à renforcer le procédé d'authentification. Cette étape **59** peut notamment
25 comprendre :

- la mesure du motif de dérive fréquentielle de l'oscillateur ayant servi à générer le paquet de données considéré, puis
- la comparaison de ce motif de dérive fréquentielle mesuré avec un motif de dérive fréquentielle prédéfini associé audit code d'identification extrait dudit paquet de données
30 considéré.

De manière plus générale, il est à noter que les modes de mise en œuvre considérés ci-dessus ont été décrits à titre d'exemples non limitatifs, et que des variantes sont par conséquent envisageables.

Notamment, il est à noter que le procédé **50** d'authentification peut être considéré seul ou combiné avec d'autres procédés d'authentification, afin de renforcer la robustesse de l'authentification. Par exemple, les paquets de données peuvent comporter une partie
5 chiffrée au moyen d'une clé tournante (« rolling code » dans la littérature anglo-saxonne). Une authentification conventionnelle basée sur l'utilisation de clés tournantes peut être combinée à une authentification basée sur la vérification, conformément à l'invention, de la séquence de sauts de fréquence.

10 En outre, il a été décrit ci-avant une estimation du nombre de paquets perdus en fonction d'un compteur incorporé dans les paquets de données.

Rien n'exclut, suivant d'autres exemples, d'estimer autrement le nombre de paquets perdus. Suivant un exemple non limitatif, si une partie des paquets de données est chiffrée
15 avec une clé tournante incrémentée par le terminal à chaque nouvelle émission, la station **20** peut incrémenter la clé tournante qu'elle utilise pour essayer de déchiffrer le paquet de données considéré jusqu'à obtenir une clé tournante permettant de déchiffrer avec succès ledit paquet de données considéré. Le nombre de paquets perdus est alors estimé en fonction de la clé tournante permettant de déchiffrer le paquet de données considéré et en
20 fonction de la clé tournante qui a permis de déchiffrer le précédent paquet de données reçu incorporant le même code d'identification que ledit paquet de données considéré.

REVENDICATIONS

1. Procédé (50) d'authentification de paquets de données émis par des terminaux (10) et reçus par un système récepteur (20) comprenant au moins une station, chaque paquet de
5 données incorporant un code d'identification du terminal (10) ayant émis ledit paquet de données, 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 comprend, pour chaque paquet de données reçu par ledit
10 système récepteur (20) :

- (51) la mesure, par ladite station, de la bande fréquentielle dans laquelle le paquet de données considéré a été reçu,
- (52) l'extraction du code d'identification contenu dans ledit paquet de données considéré,
- 15 - le calcul d'un saut de fréquence, à partir de ladite bande fréquentielle mesurée du paquet considéré et d'une bande fréquentielle mesurée par le système récepteur pour un précédent paquet de données reçu incorporant ledit code d'identification extrait,
- (55) la détermination, en fonction de la séquence de sauts de fréquence prédéterminée associée audit code d'identification extrait du paquet de données considéré, d'un saut de
20 fréquence théorique appliqué depuis ledit précédent paquet de données reçu,
- (56) le calcul d'un écart de saut de fréquence en fonction dudit saut de fréquence théorique et dudit saut de fréquence calculé,

et en ce que le procédé (50) d'authentification comprend en outre une étape (58) de détermination si les paquets de données reçus successivement avec un même code
25 d'identification ont été émis par le terminal (10) associé audit code d'identification en fonction d'au moins un écart de saut de fréquence calculé pour l'un desdits paquets de données.

2. Procédé (50) selon la revendication 1, caractérisé en ce que la bande fréquentielle
30 d'un paquet de données est mesurée plusieurs fois au cours dudit paquet de données considéré, l'écart de saut de fréquence étant calculé en considérant la bande fréquentielle mesurée finale du paquet de données considéré et la bande fréquentielle mesurée finale du précédent paquet de données incorporant le même code d'identification que ledit paquet de données considéré.

3. Procédé (50) selon l'une des revendications précédentes, caractérisé en ce qu'il comporte, après l'étape (52) d'extraction du code d'identification à partir du paquet de données considéré, une étape (54) d'estimation d'un nombre de paquets de données perdus, lesdits paquets de données perdus correspondant à des paquets de données qui ont été émis par le terminal (10) associé audit code d'identification depuis que le précédent paquet de données incorporant ledit code d'identification a été reçu, mais qui n'ont pas été reçus par le système récepteur (20), le saut de fréquence théorique pour le paquet de données considéré étant déterminé en fonction du nombre de paquets de données perdus et de la séquence de sauts de fréquence associée audit code d'identification.

4. Procédé (50) selon la revendication 3, caractérisé en ce que les paquets de données incorporant un compteur incrémenté par le terminal (10) à chaque nouvelle émission, le nombre de paquets perdus est estimé en fonction du compteur du paquet de données considéré et du compteur du précédent paquet de données reçu incorporant le même code d'identification que ledit paquet de données considéré.

5. Procédé (50) selon la revendication 3, caractérisé en ce que les paquets de données comportant une partie chiffrée au moyen d'une clé tournante incrémentée par le terminal (10) à chaque nouvelle émission, le nombre de paquets perdus est estimé en fonction de la clé tournante utilisée pour le paquet de données considéré et de la clé tournante utilisée pour le précédent paquet de données reçu incorporant le même code d'identification que ledit paquet de données considéré.

6. Procédé (50) selon la revendication 3, caractérisé en ce que les paquets de données étant émis par un terminal (10) avec une période prédéfinie, le nombre de paquets perdus est estimé en fonction de ladite période et d'un écart temporel entre la réception du paquet de données considéré et la réception du précédent paquet de données incorporant le même code d'identification que ledit paquet de données considéré.

7. Procédé (50) selon l'une des revendications précédentes, caractérisé en ce que les paquets de données reçus successivement avec un même code d'identification ne sont considérés comme ayant été émis par le terminal (10) associé audit code d'identification

que si chaque écart de saut de fréquence considéré pour l'authentification est de valeur absolue inférieure à une valeur seuil.

8. Procédé (50) selon la revendication 7, caractérisé en ce que la valeur seuil à utiliser
5 pour le paquet de données considéré est déterminée en fonction d'un écart temporel entre la réception dudit paquet de données considéré et la réception du précédent paquet de données incorporant le même code d'identification que ledit paquet de données considéré.
9. Procédé (50) selon l'une des revendications précédentes, caractérisé en ce que
10 plusieurs écarts de saut de fréquence étant considérés pour l'authentification, les paquets de données reçus successivement avec un même code d'identification ne sont considérés comme ayant été émis par le terminal (10) associé audit code d'identification que si un critère prédéfini d'authentification est vérifié par l'ensemble desdits écarts de sauts de fréquence considérés pour l'authentification.
- 15
10. Procédé (50) selon la revendication 9, caractérisé en ce que le critère d'authentification est vérifié si le cumul des écarts de sauts de fréquence considérés pour l'authentification est inférieur à une valeur seuil prédéfinie.
- 20 11. Procédé (50) selon l'une des revendications précédentes, caractérisé en ce qu'il comprend en outre, pour chaque paquet de données reçu par ledit système récepteur :
- la mesure, par ce système récepteur, d'un motif de dérive fréquentielle d'un oscillateur ayant servi à générer le paquet de données considéré, et
 - la comparaison du motif de dérive fréquentielle mesuré avec un motif de dérive
- 25 fréquentielle prédéfini associé audit code d'identification extrait dudit paquet de données considéré.
12. Procédé (50) selon l'une des revendications précédentes,
caractérisé en ce que le système récepteur comprend un serveur fédérateur
30 coopérant avec au moins une station,
et en ce que les opérations du procédé d'authentification sont réparties entre ladite station et ledit serveur.

-26-

13. Procédé (50) selon la revendication 12, caractérisé en ce que :

- la station réalise les mesures de bande fréquentielle des paquets de données qu'il reçoit ;
et
- le serveur collecte l'ensemble des paquets de données reçus par chaque station et les
5 bandes fréquentielles mesurées par chaque stations, et réalise au moins les opérations
restantes du procédé d'authentification.

14. Produit programme d'ordinateur, caractérisé en ce qu'il comporte un ensemble
d'instructions de code de programme qui, lorsqu'elles sont exécutées par un processeur,
10 mettent en œuvre un procédé (50) d'authentification selon l'une des revendications
précédentes.

15. Système récepteur d'un système de télécommunications numérique, adapté à
recevoir des paquets de données émis par des terminaux (10), ledit système récepteur
15 comprenant au moins une station, chaque paquet de données incorporant un code
d'identification du terminal (10) ayant émis ledit paquet de données, 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, caractérisée en ce qu'il comprend des moyens configurés pour authentifier
20 les paquets de données reçus conformément à un procédé selon l'une des revendications 1
à 13.

16. Système de télécommunication comprenant :

- des terminaux, chaque terminal étant apte à émettre successivement des paquets de
25 données dans une pluralité de bandes fréquentielles différentes selon une séquence de
sauts de fréquence prédéfinie spécifique dudit terminal, chaque paquet de données
incorporant un code d'identification du terminal (10) ayant émis ledit paquet de données,
 - des stations coopérant avec un serveur fédérateur pour réaliser le procédé
d'authentification selon l'une des revendications 1 à 13,
- 30 - chaque station étant apte à réaliser les mesures de bande fréquentielle des paquets
de données qu'il reçoit ; et
- le serveur étant apte à collecter l'ensemble des paquets de données reçus par
chaque station et les bandes fréquentielles mesurées par chaque stations, et étant
apte à réaliser au moins les opérations restantes dudit procédé d'authentification.