(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 669 796**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **90 14824**

(51) Int Cl^5 : H 04 L 9/00; H 04 B 7/26; H 04 M 11/06

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 27.11.90.

(30) **Priorité** :

(43) **Date de la mise à disposition du public de la demande :** 29.05.92 Bulletin 92/22.

(56) **Liste des documents cités dans le rapport de recherche :** *Se reporter à la fin du présent fascicule.*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *ETAT FRANCAIS, représenté par le Ministre des Postes, des Télécommunications et de l'Espace (Centre National d'Etudes des Télécommunications)* — FR.

(72) **Inventeur(s) :** Baudoux Sophie, Langrand Franck et Mazziotto Gérald.

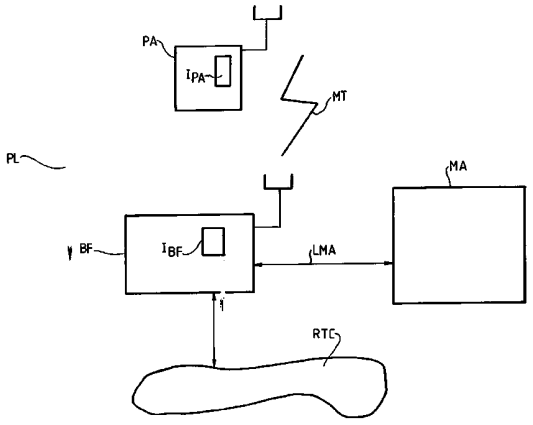
(73) **Titulaire(s) :**

(74) **Mandataire :** Cabinet Netter.

(54) Installation téléphonique à borne fixe et poste autonome pour une transmission à distance de données chiffrées.

(57) L'installation téléphonique comprend au moins une borne fixe (BF) reliée à un réseau téléphonique commuté (RTC); et au moins un poste autonome (PA) capable d'une intercommunication avec la borne fixe à travers un milieu de communication radioélectrique (MT) reliant à distance la borne fixe et le poste autonome qui possèdent l'un et l'autre une interface (I) avec ledit milieu (MT).

En réponse à une demande d'appel émanant de l'une des interfaces accompagnée d'une demande de chiffrement/déchiffrement de données, les moyens de chiffrement/déchiffrement de l'interface appelée génèrent une valeur initiale de comptage d'intervalles de temps, et transmettent ladite valeur à l'interface appelante qui applique ladite valeur à ses moyens de chiffrement/déchiffrement, ce qui permet, après acquittement de la réception de ladite valeur, de synchroniser les moyens de chiffrement/déchiffrement de la borne fixe et du poste autonome.



FR 2 669 796 - A1

Installation téléphonique à borne fixe et poste autonome pour une transmission à distance de données chiffrées.

La présente invention concerne une installation téléphonique à borne fixe et poste autonome pour une transmission à distance de données chiffrées.

Elle trouve plus particulièrement une application dans les installations téléphoniques utilisant l'interface radioélectrique CAI pour "Common Air Interface" telles que les installations françaises utilisant le système POINTEL (marque déposée).

D'une façon générale, une telle installation comprend :

- au moins une borne fixe reliée à un réseau téléphonique commuté; et

- au moins un poste autonome mobile ou fixe capable d'une intercommunication avec la borne fixe à travers un milieu de communication radioélectrique reliant à distance la borne fixe et le poste autonome.

La borne fixe et le poste autonome possèdent l'un et l'autre une interface avec le milieu de communication. Chaque interface est munie d'un protocole de communication avec duplexage par division temporelle selon lequel l'interface de la borne fixe est capable d'émettre périodiquement des données pendant un intervalle de temps d'émission/réception prédéterminé sur le milieu de communication pendant que l'interface du poste autonome est capable de recevoir périodiquement lesdites données pendant cet intervalle de temps prédéterminé et réciproquement.

Il est demandé par les exploitants de telles installations

qu'il soit permis à l'usager d'un poste autonome de transmettre des données chiffrées sur le milieu radioélectrique pour conférer à la communication un degré de confidentialité ainsi qu'éviter l'interception frauduleuse de données.

Une solution connue consiste à équiper chaque extrémité du milieu de communication radioélectrique (borne fixe et poste autonome) de moyens de chiffrement/déchiffrement symétriques, c'est-à-dire que l'une des extrémités chiffre les données à transmettre tandis que l'autre extrémité déchiffre celles ainsi transmises.

Cette solution est notamment utilisée dans les systèmes de télécommunications dits GSM pour "Groupe Spécial Mobile".

En pratique dans le système GSM, les moyens de chiffrement/déchiffrement de chaque extrémité établissent une fonction cryptographique F ayant pour opérandes une clé secrète de chiffrement/déchiffrement commune aux deux extrémités d'une part et une donnée variable représentative d'une valeur initiale de comptage d'intervalles de temps d'émission/réception commune également aux deux extrémités d'autre part.

Le transformé par la fonction cryptographique F de la clé et de la donnée variable est combiné alors avec les données numériques d'une manière prédéterminée à une des extrémités pour réaliser le chiffrement, et d'une autre manière prédéterminée à l'autre extrémité pour réaliser le déchiffrement.

L'une et l'autre des deux manières prédéterminées sont bien entendu connues des deux extrémités. Par exemple, elles peuvent être une addition bit à bit des données numériques et du transformé des moyens de chiffrement/déchiffrement.

Les algorithmes de chiffrement/déchiffrement sont synchroni-

sés lorsque les moyens de chiffrement/déchiffrement situés à chaque extrémité du milieu de transmission radioélectrique (borne fixe et poste autonome) produisent le même transformé au même intervalle de temps d'émission/réception.

Il est clair que cette synchronisation nécessite que les moyens de chiffrement/déchiffrement de chaque extrémité aient démarré de façon concertée avec des valeurs initiales de comptage d'intervalles de temps cohérentes et des instants initiaux de démarrage cohérents.

Dans le système GSM, la concertation des deux extrémités est automatiquement réalisée car la valeur commune de comptage d'intervalles de temps est connue à tout instant des deux extrémités, par une acquisition externe et indépendante du processus d'émission/réception des données chiffrées.

Plus précisément, cette acquisition externe s'effectue pendant les intervalles de temps alloués à la voie de gestion de l'installation appelée encore voie balise par l'homme du métier.

Par exemple dans le système GSM, la trame de communication de chaque poste autonome se décompose en un intervalle de temps alloué à l'émission, un intervalle de temps alloué à la réception et six intervalles de temps qui restent disponibles et qui peuvent être ainsi alloués à la voie balise.

C'est donc par la voie balise que les deux extrémités de l'installation (poste autonome et borne fixe) ont connaissance en permanence de la valeur commune du compteur d'intervalles de temps intervenant dans le processus de chiffrement/déchiffrement.

Dans le système POINTEL, les interfaces de communication

sont munies d'un protocole de communication dépourvu de voie balise, c'est à dire que la trame de communication de chaque poste autonome se décompose seulement en un intervalle de temps alloué à l'émission et un intervalle de temps alloué à la réception des données, protocole appelé encore TDD pour duplexage par division temporelle (time division duplex) par l'homme de métier.

Il en résulte que la solution utilisée dans le système GSM n'est pas réalisable dans le système POINTEL.

Une autre méthode connue de synchronisation consiste à utiliser des algorithmes de chiffrement/déchiffrement susceptibles de se synchroniser eux mêmes, les uns par rapport aux autres sans l'utilisation d'une valeur commune de comptage d'intervalles de temps.

Néanmoins, de tels moyens autosynchronisables ont pour inconvénient de perdre les premières données échangées avant que les algorithmes de chiffrement/déchiffrement se synchronisent par eux mêmes. En outre, ils sont inadaptés aux transmissions de données présentant un taux d'erreur élevé telle que la transmission via un milieu de communication radioélectrique car ils ont tendance à accroître ce taux d'erreur de transmission.

La présente invention vient rémédier au problème ainsi posé.

Un premier but de l'invention est de fournir une installation téléphonique à borne fixe et poste autonome pour une transmission de données chiffrées dans laquelle la borne fixe et le poste autonome sont équipés de moyens de chiffrement/déchiffrement synchronisés les uns par rapport aux autres.

Un autre but de l'invention vise une synchronisation des moyens de chiffrement/déchiffrement de chaque extrémité qui ne nécessite pas une connaissance permanente par lesdits moyens de chiffrement/déchiffrement de la valeur de comptage d'intervalles de temps délivrée par un compteur externe aux deux extrémités.

Encore un autre but de l'invention, est de fournir une synchronisation des moyens de chiffrement/déchiffrement de chaque extrémité qui n'augmente pas le taux d'erreur de transmission de données.

Enfin, l'invention vise à fournir une installation permettant d'assurer la cohérence des démarrages des moyens de chiffrement/déchiffrement de chaque extrémité malgré l'absence d'une voie balise.

L'invention porte sur une installation comprenant :

- au moins une borne fixe reliée à un réseau téléphonique commuté; et

- au moins un poste autonome capable d'une intercommunication avec la borne fixe à travers un milieu de communication radioélectrique reliant à distance la borne fixe et le poste autonome qui possèdent l'un et l'autre une interface avec le milieu de communication, interface munie d'un protocole de communication avec duplexage par division temporelle selon lequel l'interface de la borne fixe est capable d'émettre périodiquement des données pendant un intervalle de temps d'émission/réception prédéterminé sur le milieu de communication pendant que l'interface du poste autonome est capable de recevoir périodiquement lesdites données pendant cet intervalle de temps prédéterminé et réciproquement.

Selon une définition générale de l'invention, le poste autonome et la borne fixe comprennent chacun des moyens de chiffrement/déchiffrement de données propres à établir une fonction cryptographique F ayant pour opérandes une clé secrète de chiffrement/déchiffrement d'une part et une donnée variable représentative d'une valeur initiale de comptage d'intervalles de temps d'émission/réception d'autre part, et propres à utiliser le transformé par la fonction cryptographique F de la clé et de la donnée variable pour effectuer une opération de chiffrement/déchiffrement sur les données à chiffrer/déchiffrer, et

en réponse à une demande d'appel émanant de l'une des interfaces accompagnée d'une demande de chiffrement/déchiffrement de données, les moyens de chiffrement/déchiffrement de l'interface appelée génèrent la valeur initiale de comptage d'intervalles de temps, et transmettent ladite valeur à l'interface appelante qui applique ladite valeur à ses moyens de chiffrement/déchiffrement, ce qui permet, après acquittement de la réception de ladite valeur, de synchroniser les moyens de chiffrement/déchiffrement de la borne fixe et du poste autonome.

Selon un mode de réalisation de l'invention, les moyens de chiffrement/déchiffrement du poste autonome et de la borne fixe comprennent chacun :

- un compteur d'intervalles de temps possédant une entrée reliée à l'interface et une sortie propre à délivrer une valeur initiale de comptage d'intervalles de temps;

- un organe de chiffrement/déchiffrement propre à établir la fonction cryptographique F et possédant :
. une première entrée connectée à la sortie du compteur pour recevoir la valeur initiale de comptage d'intervalles de temps,

. une seconde entrée propre à recevoir la clé secrète de chiffrement/déchiffrement, et

. une sortie propre à délivrer le transformé par la fonction cryptographique F de la clé et de la valeur initiale de comptage d'intervalles de temps, et

- un opérateur propre à effectuer l'opération de chiffrement/déchiffrement et possédant :

. une première entrée propre à recevoir les données à chiffrer/déchiffrer,

. une seconde entrée propre à recevoir le transformé de la fonction cryptographique F, et

. une sortie propre à délivrer le résultat de l'opération de chiffrement/déchiffrement en synchronisme avec la sortie du compteur d'intervalles de temps; et

en réponse à la demande d'appel émanant de l'une des interfaces accompagnée de la demande de chiffrement/déchiffrement de données, le compteur de l'interface appelée génère la valeur initiale de comptage d'intervalles de temps, et transmet ladite valeur à l'interface appelante qui applique ladite valeur à l'entrée de son compteur.

De préférence, après la transmission à l'interface appelante de la valeur initiale de comptage d'intervalles de temps, le compteur de l'interface appelée délivre une valeur complémentaire de comptage d'intervalles de temps initialisée en fonction de la valeur initiale d'intervalles de temps, et transmet ladite valeur complémentaire à l'interface appelante qui applique ladite valeur complémentaire à l'entrée de son compteur pour comparaison avec la valeur de comptage dudit compteur qui a été initialisée également en fonction de la valeur initiale d'intervalles de temps, l'interface appelante transmettant à l'interface appelée un acquittement de la réception de la valeur initiale de comptage d'intervalles de temps en fonction de la comparaison.

Selon un autre mode de réalisation de l'invention, le compteur d'intervalles de temps délivre à sa sortie une série périodique de valeurs auxiliaires de comptage d'intervalles de temps dont la valeur extrême représente la valeur initiale de comptage d'intervalles de temps et les moyens de chiffrement/déchiffrement de chaque interface comprennent en outre :

- un commutateur possédant :
. une première entrée reliée à la sortie du compteur,
. une seconde entrée reliée à l'interface, et
. une sortie connectée à la première entrée de l'organe de chiffrement/déchiffrement ; le commutateur étant propre à délivrer à sa sortie soit les données appliquées à sa seconde entrée lorsque la valeur auxiliaire ainsi appliquée est égale à la valeur auxiliaire extrême soit la série de valeurs auxiliaires de comptage lorsque la valeur auxiliaire ainsi appliquée est différente de la valeur auxiliaire extrême, l'application de la valeur auxiliaire extrême à la première entrée du commutateur faisant office d'acquittement de la réception de la valeur initiale de comptage.

De préférence, l'interface du poste autonome comprend un convertisseur analogique/numérique propre à convertir les données de parole en données numériques et la sortie dudit convertisseur est appliquée à la seconde entrée du commutateur.

En pratique, le milieu de communication comprend une voie de signalisations numériques et une voie de parole et la valeur initiale de comptage d'intervalles de temps est transmise sur la voie de signalisations numériques.

En variante, le milieu de communication comprend une voie de signalisations numériques et une voie de parole et la valeur initiale de comptage d'intervalles de temps est transmise sur la voie de parole.

D'autres caractéristiques et avantages de l'invention apparaîtont à la lumière de la description détaillée ci-après et des dessins annexés dans lesquels :

- la figure 1 est une vue schématique d'une installation téléphonique de type POINTEL (marque déposée);

- la figure 2 est un chronogramme illustrant le protocole de communication de l'installation de la figure 1 ;

- la figure 3 est une vue schématique d'un mode de réalisation des moyens de chiffrement/déchiffrement équipant une borne fixe et un poste autonome selon l'invention ;

- la figure 4 illustre le fonctionnement des moyens de chiffrement décrit en référence à la figure 3 ;

- la figure 5 est une vue schématique d'un autre mode de réalisation des moyens de chiffrement/déchiffrement équipant une borne fixe et un poste autonome selon l'invention ;et

- la figure 6 illustre le fonctionnement des moyens de chiffrement décrit en référence à la figure 5.

Sur la figure 1, la référence PL désigne une installation téléphonique utilisant le système POINTEL (Marque déposée).

D'une façon générale, une installation téléphonique du type POINTEL comprend :

- au moins une borne fixe BF reliée à un réseau téléphonique commuté RTC, et

- au moins un poste autonome PA mobile ou fixe, capable d'une intercommunication avec la borne fixe BF à travers

un milieu de communication radioélectrique MT reliant à distance la borne fixe BF et le poste autonome PA.

La borne fixe BF et le poste autonome PA possèdent respectivement une interface IBF et IPA avec le milieu de communication MT.

Des moyens d'autorisation MA sont reliés à la borne fixe BF via une ligne de communication LMA en vue de contrôler l'établissement d'une liaison téléphonique entre le poste autonome PA et le réseau téléphonique commuté RTC.

Chaque interface est munie d'un protocole de communication utilisant l'interface radioélectrique CAI pour "Common Air Interface" portant la référence MPT 1375.

Nous faisons maintenant référence à la figure 2 qui est un chronogramme illustrant le protocole de communication de l'installation décrite en référence à la figure 1.

Les interfaces de communication dans le système POINTEL sont munies d'un protocole de communication dépourvu de voie balise, c'est-à-dire que la trame de communication de chaque poste autonome se décompose seulement en un intervalle de temps IT1 alloué à l'émission de données binaires b et en un intervalle de temps IT2 alloué à la réception desdites données binaires b.

Ce protocole de communication est appelé "TDD" pour "Duplexage par Division Temporelle ("Time Division Duplex) par l'homme du métier.

Plus précisément, pendant l'intervalle de temps IT1, l'interface du poste autonome PA est capable d'émettre des données b individualisées en b1 à b72 vers la borne fixe BF

qui les reçoit via le milieu de transmission radioélectrique MT.

Pendant l'intervalle IT2, c'est la borne fixe BF qui est capable d'émettre des données binaires b individualisées en b74 à b144 vers le poste autonome PA via le milieu de transmission radioélectrique MT.

Bien entendu, cette émission/réception est répétée périodiquement tous les 144 bits dans la mesure où le poste autonome est capable d'émettre 72 bits pendant l'intervalle IT1 et recevoir 72 bits pendant l'intervalle IT2.

Le protocole de communication avec duplexage par division temporelle a un débit de 72 kilobits par seconde et chaque intervalle de temps IT est de l'ordre de la milliseconde.

Le milieu de transmission est subdivisé en un canal de transmission de signalisation (voie D) et en un canal de transmission des données de parole (voie B).

Selon la norme CAI, le protocole de communication est du type maître-esclave selon lequel la borne fixe joue le rôle de maître tandis que le poste autonome joue le rôle d'esclave.

Nous faisons maintenant référence à la figure 3.

Nous avons représenté une installation PL à borne fixe BF et poste autonome PA pour une transmission à distance de données chiffrées selon l'invention.

L'interface IBF de la borne fixe BF est reliée via le milieu de transmission MT à l'interface IPA du poste autonome PA.

Il est à remarquer que les éléments essentiels et constitu-

tifs de l'interface IBF et IPA sont identiques et fonctionnent de façon symétrique. Par conséquent, pour faciliter la compréhension de l'invention, ces éléments essentiels et constitutifs portent les mêmes références accompagnées d'indices PA ou BF indiquant l'extrémité de l'installation concernée.

Chaque extrémité comprend des moyens de chiffrement/déchiffrement de données CD propres à établir une fonction cryptographique F ayant pour opérande une clé secrète de chiffrement/déchiffrement K d'une part et une donnée variable représentative d'une valeur initiale de comptage d'intervalles de temps d'émission/réception Ti d'autre part.

En outre, les moyens de chiffrement/déchiffrement CD utilisent le transformé par la fonction cryptographique F de la clé K et de la donnée variable Ti pour effectuer une opération de chiffrement/déchiffrement sur les données à chiffrer/déchiffrer provenant de l'interface I.

Par exemple, l'opération de chiffrement/déchiffrement est une addition bit à bit des données binaires b et du transformé des moyens de chiffrement/déchiffrement.

En pratique, les moyens de chiffrement/déchiffrement CD comprennent un compteur d'intervalles de temps CT possédant une entrée 10 reliée à l'interface I et une sortie 12 délivrant une valeur initiale de comptage d'intervalles de temps Ti.

Un organe de chiffrement/déchiffrement 20 établit la fonction cryptographique F et possède une première entrée 22 connectée à la sortie 12 du compteur CT pour recevoir la valeur initiale de comptage d'intervalles de temps Ti, une seconde entrée 24 pour recevoir la clé secrète K, et une

sortie 26 pour délivrer le transformé par la fonction cryptographique F de la clé K et de la valeur initiale de comptage Ti.

Il est prévu en outre un opérateur OP capable d'effectuer l'opération de chiffrement/déchiffrement sur les données à chiffrer/déchiffrer à l'aide du transformé de la fonction cryptographique F.

L'opérateur OP possède une première entrée 32 recevant les données à chiffrer provenant de l'interface I, une seconde entrée 34 recevant le transformé de la fonction cryptographique F, et une sortie 36 délivrant le résultat de l'opération de chiffrement/déchiffrement en synchronisme avec la sortie du compteur d'intervalles de temps CT.

Par exemple, la fréquence de comptage du compteur d'intervalles de temps CT est de l'ordre de 500 Hertz.

Nous faisons maintenant référence à la figure 4 qui illustre le fonctionnement des moyens de chiffrement décrits en référence à la figure 3.

Selon un mode de réalisation préféré de l'invention, la transmission des données chiffrées s'effectue uniquement sur le canal B du milieu de transmission, c'est-à-dire sur le canal réservé aux données de parole.

Nous avons vu que le chiffrement/déchiffrement était basé sur une clé de chiffrement/déchiffrement secrète commune aux deux extrémités (borne fixe et poste autonome).

Par exemple, selon l'étape E0, la clé de chiffrement KBF est transmise de la borne fixe BF vers le poste autonome PA via le milieu MT.

En pratique, la clé secrète KBF est transmise chiffrée selon une méthode d'authentification comme celle décrite dans la Demande de Brevet français 90 06662 déposée par la Demanderesse le 29 mai 1990.

Selon l'étape E1, le poste autonome transmet un message acK montrant qu'il a bien reçu la clé secrète commune K.

La synchronisation selon l'invention des moyens de chiffrement/déchiffrement équipant la borne fixe et le poste autonome peut alors commencer (étape E2).

Selon l'invention, en réponse à une demande d'appel émanant du poste autonome PA, accompagnée d'une demande de chiffrement/déchiffrement de données, le compteur CTBF génère une valeur initiale de comptage d'intervalles de temps Ti représentative de la valeur initiale commune de comptage d'intervalles de temps.

Par exemple, cette valeur Ti est envoyée par la borne fixe dans un message "COMP_INIT" comprenant un champ unique dont la longueur dépend du nombre de bits de la sortie du compteur CT.

Par exemple, la longueur du message COMP_INIT est de 96 bits.

Dans l'étape E2, la borne fixe BF envoie donc un message appelé SYNCHRO en vue d'imposer une synchronisation de chiffrement au poste autonome PA. Ce message SYNCHRO est représentatif par conséquent d'un ordre de chiffrement/déchiffrement de données. Il comprend en outre le message COMP_INIT contenant la valeur commune de comptage d'intervalles de temps Ti.

Par exemple, le message SYNCHRO a une longueur totale de 4 octets.

De son côté, le poste autonome applique la valeur commune Ti à l'entrée de son compteur CTPA.

Selon l'étape E3, après la transmission de la valeur commune initiale de comptage d'intervalles de temps TI, le compteur CTBF de la borne fixe génère une valeur complémentaire de comptage d'intervalles de temps Ti+n où n est un nombre entier d'intervalles de temps s'étant écoulés entre la génération de la valeur commune Ti et la valeur commune complémentaire Ti+n. Il en résulte que la valeur Ti+n est initialisée en fonction de la valeur initiale d'intervalles de temps Ti.

Cette valeur commune complémentaire Ti+n est transmise dans le message COMP_INIT vers le poste autonome via le message SYNCHRO.

Cette valeur commune complémentaire est appliquée à l'entrée du compteur de l'interface appelante pour comparaison avec la valeur de comptage dudit compteur qui a été également initialisée en fonction de la valeur initiale d'intervalles de temps.

En fonction de la comparaison, l'interface appelante PA transmet alors à l'interface de la borne fixe BF un acquittement de la réception de la valeur initiale de comptage d'intervalles de temps (étape E4).

Par exemple, l'acquittement de la réception de la valeur initiale est transmise dans un message READY qui est envoyé par le poste autonome une fois qu'il est certain d'avoir acquis la synchronisation de chiffrement, c'est-à-dire quand

il a reçu une valeur de champ COMP_INIT coïncidant avec sa propre valeur de compteur d'intervalles de temps.

Par exemple, le message READY a une longueur totale de 2 octets.

Ensuite, selon l'étape E5, la borne fixe transmet un message CC autorisant l'établissement de la transmission de données.

Enfin, selon les étapes E6 et E7, la liaison téléphonique est établie entre la borne fixe et le poste autonome, ce qui permet de transmettre les données chiffrées via le milieu de transmission MT.

Nous faisons maintenant référence à la figure 5 qui illustre schématiquement un autre exemple de réalisation des moyens de chiffrement/déchiffrement selon l'invention.

Nous avons vu ci-avant que l'acquittement de la réception de la valeur commune de comptage d'intervalles de temps est effectuée par comparaison de deux valeurs communes transmises l'une après l'autre et espacées d'un nombre d'intervalles de temps choisi n.

Selon l'invention, il est possible de réaliser cet acquittement sans la génération d'une valeur commune complémentaire de comptage d'intervalles de temps.

Selon la variante de l'invention, le rôle joué par la valeur complémentaire commune de comptage d'intervalles de temps Ti+n est maintenant joué par le compteur d'intervalles de temps qui délivre une série périodique de valeurs auxiliaires de comptage d'intervalles de temps dont la valeur extrême représente la valeur initiale d'intervalles de temps Ti.

Plus précisément, il est prévu d'équiper les moyens de chiffrement/déchiffrement du poste autonome d'un compteur d'intervalles de temps CT possédant une entrée 100 reliée à l'interface IPA.

Le compteur d'intervalles de temps CT délivre à sa sortie 102 une série périodique de valeurs auxiliaires de comptage d'intervalles de temps Ta.

En pratique, la série périodique de valeurs auxiliaires de comptage d'intervalles de temps comprend 30 valeurs Ta individualisées en Ta30 à Ta0.

Il est prévu en outre un commutateur COM possédant :

- une première entrée 104 reliée à la sortie 102 du compteur CT,

- une seconde entrée 106 reliée à l'interface IPA ou bien à la sortie d'un convertisseur analogique/numérique CAN propre à convertir la voie du locuteur en un train de données binaires.

La sortie 108 du commutateur COM est reliée à l'entrée 22 de l'organe de chiffrement/déchiffrement 20 capable d'établir la fonction cryptographique F.

Lorsque la valeur auxiliaire de comptage a atteint sa valeur extrême Ta0, le commutateur COM délivre à sa sortie 108 les données appliquées à l'interface IPA ou au convertisseur CAN. Si la valeur auxiliaire de comptage est différente de la valeur Ta0, la sortie du commutateur COM délivre alors à sa sortie 108 les valeurs auxiliaires de comptage Ta jusqu'à la valeur extrême Ta0.

L'obtention de la valeur auxiliaire de comptage extrême Ta0 représente ici l'acquittement de la réception de la valeur initiale de comptage d'intervalles de temps Ti.

Il est à remarquer que l'organe de chiffrement/déchiffrement 20 ainsi que l'opérateur de chiffrement/déchiffrement OP sont identiques à ceux décrits en référence à la figure 3.

Nous faisons maintenant référence à la figure 6 qui illustre le fonctionnement des moyens de chiffrement/déchiffrement décrits en référence à la figure 5.

Lors de l'étape A0, la borne fixe BF transmet tout d'abord la clé secrète de chiffrement/déchiffrement KBF vers le poste autonome via le milieu de transmission MT comme décrit en référence à la figure 4.

Une fois que la clé secrète KBF est stockée dans le poste autonome, ce dernier émet un message d'acquittement acK (étape A1).

Le processus de synchronisation de chiffrement/déchiffrement selon l'invention commence alors.

Lors de l'étape A2, la borne fixe transmet le message COMP_INIT. Ce message, envoyé par la borne fixe au cours de la procédure de passage en chiffrement, permet de transmettre la série périodique de valeurs auxiliaires de comptage d'intervalles de temps Ta30 à Ta0.

Le message COMP_INIT est par exemple celui décrit en référence à la figure 4.

Une fois que le message COMP_INIT est stocké dans le poste autonome, celui-ci émet un signal d'acquittement acK lors de l'étape A3.

Ensuite, lors de l'étape A4, la borne fixe envoie un message SYNCHRO en vue d'imposer une synchronisation de chiffrement au poste autonome. Il s'agit en fait d'un ordre de chiffrement/déchiffrement de données accompagné d'un ordre de synchronisation.

Ce message a une longueur totale de l'ordre de 4 octets.

C'est dans ce message SYNCHRO qu'il est établi le nombre de valeurs auxiliaires de comptage Ta.

Par exemple, ce nombre de valeurs auxiliaires de comptage Ta est égal à 30.

Il s'ensuit que lors des étapes A4, A5 et A6, le compteur de la borne fixe BF génère une pluralité de valeurs auxiliaires de comptage de Ta30 jusqu'à une valeur auxiliaire extrême Ta0 (étape A6).

Cette valeur auxiliaire de comptage extrême Ta0 sert de signal de commande pour actionner le commutateur COM pour que celui-ci permette le passage des données à chiffrer ou à déchiffrer vers l'organe de chiffrement/déchiffrement 20.

Simultanément au forçage du compteur auxiliaire à la valeur auxiliaire extrême Ta0, la borne fixe émet un message CC indiquant l'autorisation de la liaison entre la borne fixe et le poste autonome sur le canal B. A partir de cette étape A7, le poste autonome peut passer des données chiffrées vers la borne fixe tandis que celle-ci peut recevoir des données chiffrées émanant du poste autonome.

Lors de l'étape A8, le poste autonome libère un message d'acquittement acK.

Le trafic de communication peut alors s'effectuer entre le poste autonome et la borne fixe lors de l'étape A9.

Il est à noter que la transmission de la valeur initiale Ti ainsi que les valeurs auxiliaires Ta peut se dérouler sur un certain laps de temps en fonction de la distance entre la borne fixe et le poste autonome. Il s'ensuit que la valeur initiale de comptage commune Ti ainsi que les valeurs auxiliaires Ta transmises par la borne fixe vers le poste autonome peuvent comprendre en outre une valeur supplémentaire représentative de ce laps de temps.

Plusieurs solutions se présentent pour tenir compte de ce laps de temps de transmission. Par exemple, il peut être inséré dans la valeur initiale de comptage Ti, c'est-à-dire que la valeur initiale de comptage Ti comprend en plus un surcroît d'intervalles de temps.

Une autre solution consiste à inclure ce laps de temps dans le compteur logé dans le poste autonome et dans la borne fixe.

Dans le système POINTEL, nous avons vu que le milieu de communication MT comprend une voie de signalisations numériques B et une voie de parole D.

Jusqu'à présent nous avons considéré que la valeur initiale de comptage d'intervalles de temps est transmise sur la voie de signalisations numériques B.

Selon l'invention, il est également possible de transmettre la valeur initiale de comptage d'intervalles de temps sur la voie de parole D.

Nous venons de décrire l'application de l'invention à la

synchronisation d'algorithmes de chiffrement et de déchiffrement pour le système de communication avec les personnes en déplacement dans le système POINTEL, c'est-à-dire dans le cadre de l'interface radioélectrique CAI (norme britannique MPT1375). La terminologie employée ci-avant, notamment les noms des canaux et des messages, fait référence à cette spécification. Les nouveaux messages proposés sont destinés à s'insérer dans cette spécification. En revanche, l'algorithme de chiffrement/déchiffrement lui-même ne fait pas partie de l'invention.

Il est à noter que l'invention peut trouver une application dans le système DECT pour Digital European Cordless Telephon.

Revendications

1. Installation téléphonique comprenant :

- au moins une borne fixe (BF) reliée à un réseau téléphonique commuté (RTC);

- au moins un poste autonome (PA) capable d'une intercommunication avec la borne fixe à travers un milieu de communication radioélectrique (MT) reliant à distance la borne fixe et le poste autonome qui possèdent l'un et l'autre une interface (I) avec ledit milieu (MT), interface munie d'un protocole de communication avec duplexage par division temporelle selon lequel l'interface de la borne fixe est capable d'émettre périodiquement des données pendant un intervalle de temps d'émission/réception prédéterminé sur le milieu de communication pendant que l'interface du poste autonome est capable de recevoir périodiquement lesdites données pendant cet intervalle de temps prédéterminé et réciproquement, caractérisée en ce que le poste autonome et la borne fixe comprennent chacun des moyens de chiffrement/déchiffrement (CD) de données propres à établir une fonction cryptographique F ayant pour opérandes une clé secrète de chiffrement/déchiffrement (K) d'une part et une donnée variable représentative d'une valeur initiale de comptage d'intervalles de temps (Ti) d'autre part, et propres à utiliser le transformé par la fonction cryptographi-que F de la clé et de la donnée variable pour effectuer une opération de chiffrement/déchiffrement sur les données à chiffrer/déchiffrer,

et en ce qu'en réponse à une demande d'appel émanant de l'une des interfaces accompagnée d'une demande de chiffrement/déchiffrement de données, les moyens de chiffrement/déchiffrement l'interface appelée génèrent la valeur initiale

de comptage d'intervalles de temps (Ti), et transmettent ladite valeur à l'interface appelante qui applique ladite valeur à ses moyens de chiffrement/déchiffrement, ce qui permet, après acquittement de la réception de ladite valeur, de synchroniser les moyens de chiffrement/déchiffrement de la borne fixe et du poste autonome.

2. Installation selon la revendication 1, caractérisée en ce que les moyens de chiffrement/déchiffrement du poste autonome et de la borne fixe comprennent chacun :

- un compteur d'intervalles de temps (CT) possédant une entrée (10) reliée à l'interface (I) et une sortie (12) propre à délivrer une valeur initiale de comptage d'intervalles de temps (Ti);

- un organe de chiffrement/déchiffrement (20) propre à établir la fonction cryptographique F et possédant :
. une première entrée (22) connectée à la sortie (12) du compteur (CT) pour recevoir la valeur initiale de comptage d'intervalles de temps (Ti),
. une seconde entrée (24) propre à recevoir la clé secrète de chiffrement/déchiffrement (K), et
. une sortie (26) propre à délivrer le transformé par la fonction cryptographique F de la clé et de la valeur initiale de comptage,

- un opérateur (OP) propre à effectuer l'opération de chiffrement/déchiffrement et possédant :
. une première entrée (32) propre à recevoir les données à chiffrer/déchiffrer,
. une seconde entrée (34) propre à recevoir le transformé de la fonction cryptographique F, et
. une sortie (36) propre à délivrer le résultat de l'opération de chiffrement/déchiffrement en synchronisme avec la

sortie (12) du compteur d'intervalles de temps(CT); et

en ce qu'en réponse à la demande d'appel émanant de l'une des interfaces (IPA) accompagnée de la demande de chiffrement/déchiffrement de données, le compteur (CT) de l'interface appelée (IBF) génère la valeur initiale de comptage d'intervalles de temps (Ti), et transmet ladite valeur initiale de comptage à l'interface appelante (IPA) qui applique ladite valeur initiale de comptage à l'entrée (10) de son compteur (CT).

3. Installation selon la revendication 2, caractérisée en ce qu'après la transmission à l'interface appelante de la valeur initiale de comptage d'intervalles de temps (Ti), le compteur de l'interface appelée (IBF) délivre une valeur complémentaire de comptage d'intervalles de temps (Ti+n) initialisée en fonction de la valeur initiale d'intervalles de temps, et transmet ladite valeur complémentaire (Ti+n) à l'interface appelante (IPA) qui applique ladite valeur complémentaire (Ti+n) à l'entrée (10) de son compteur pour comparaison avec la valeur de comptage dudit compteur qui a été également initialisée en fonction de la valeur initiale d'intervalles de temps, l'interface appelante (IPA) transmettant à l'interface appelée (IBF) un acquittement (READY) de la réception de la valeur initiale de comptage d'intervalles de temps (Ti) en fonction de la comparaison.

4. Installation selon la revendication 2, caractérisée en ce que :

- le compteur d'intervalles de temps (CT) possédant une entrée (100) reliée à l'interface et une sortie (102) propre à délivrer une série périodique de valeurs auxiliaires de comptage d'intervalles de temps (Ta30 à Ta0) dont la valeur extrême (Ta0) représente la valeur initiale de comptage

d'intervalles de temps (Ti) ; et en ce que les moyens de chiffrement/déchiffrement comprennent en outre :

- un commutateur (COM) possédant :
. une première entrée (104) reliée à la sortie (102) du compteur (CT),
. une seconde entrée (106) reliée à l'interface, et
. une sortie (108) connectée à la première entrée (22) de l'organe de chiffrement/déchiffrement (20); le commutateur (COM) étant propre à délivrer à sa sortie (108) soit les données appliquées à la seconde entrée (106) lorsque la valeur auxiliaire de comptage (Ta) ainsi appliquée est égale à la valeur auxiliaire extrême (Ta0) soit la série de valeurs auxiliaires de comptage (Ta30 à Ta0), lorsque la valeur auxiliaire de comptage (Ta) ainsi appliquée est différente de la valeur auxiliaire extrême (Ta0), l'application de la valeur auxiliaire extrême (Ta0) à la première entrée du commutateur (COM) faisant office d'acquittement de la réception de la valeur initiale de comptage.

5. Installation selon la revendication 4, caractérisée en ce que l'interface du poste autonome comprend un convertisseur analogique/numérique (CAN) propre à convertir les données de parole en données numériques et en ce que la sortie dudit convertisseur est appliquée à la seconde entrée (106) du commutateur (COM).

6. Installation selon l'une quelconque des précédentes revendications, caractérisée en ce que le milieu de communication (MT) comprend une voie de signalisations numériques et une voie de parole et en ce que la valeur initiale de comptage d'intervalles de temps est transmise sur la voie de signalisations numériques.

7. Installation selon l'une quelconque des précédentes re-

vendications 1 à 5, caractérisée en ce que le milieu de communication comprend une voie de signalisations numériques et une voie de parole et en ce que la valeur initiale de comptage d'intervalles de temps est transmise sur la voie de parole.

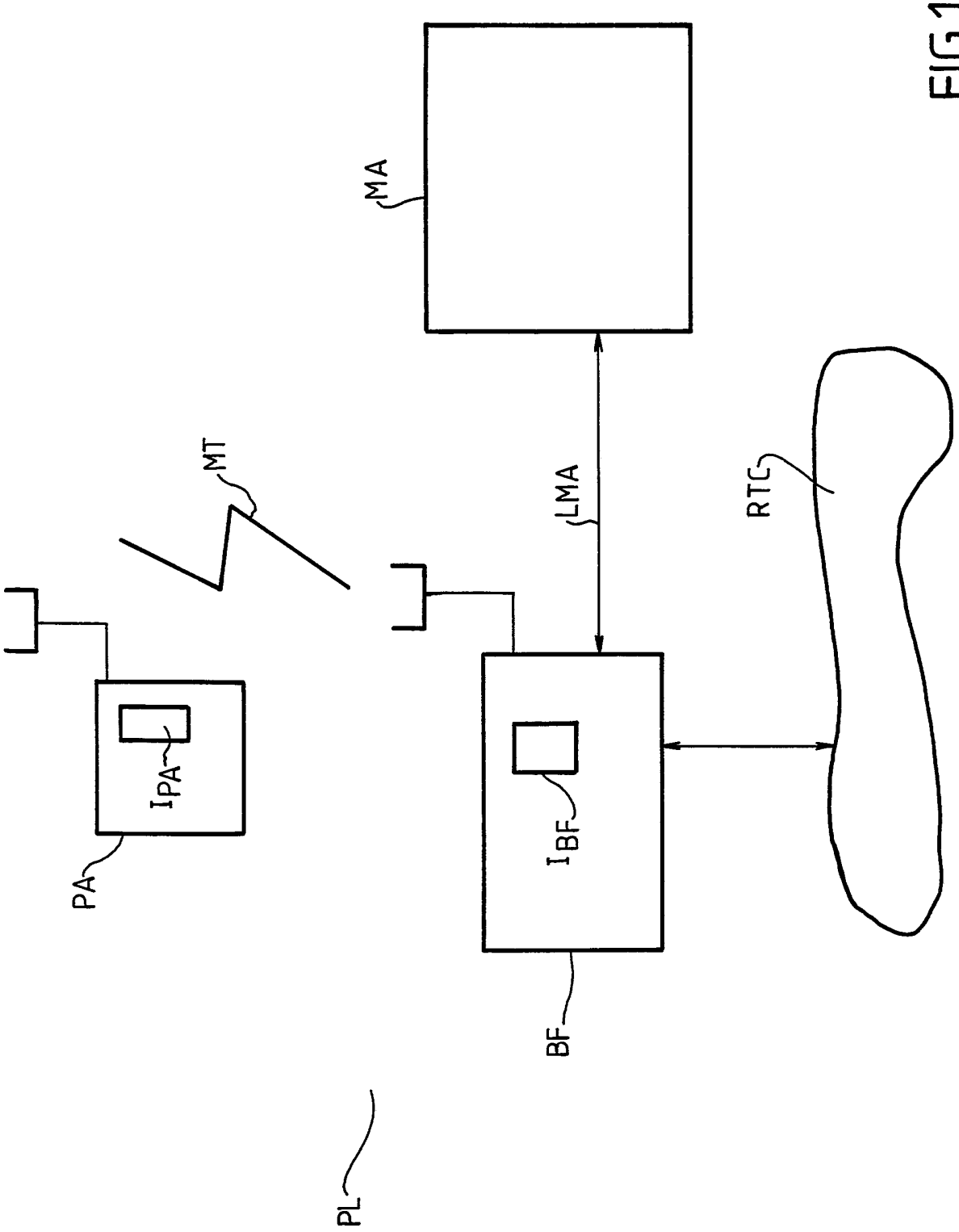


FIG.1

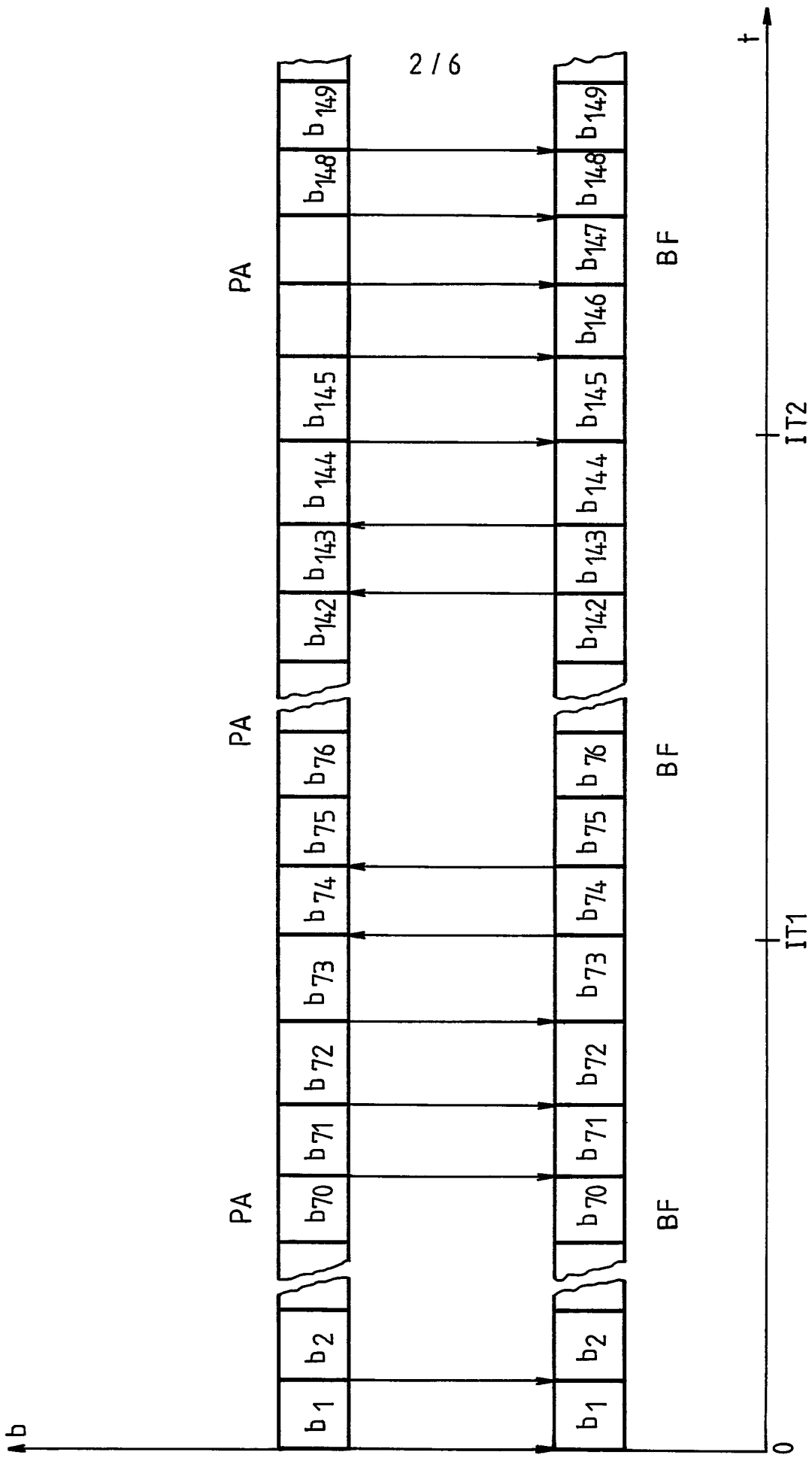

b
t
0
IT1
IT2
PA
PA
PA
BF
BF
BF
b1
b2
b70
b71
b72
b73
b74
b75
b76
b142
b143
b144
b145
b146
b147
b148
b149

FIG.2

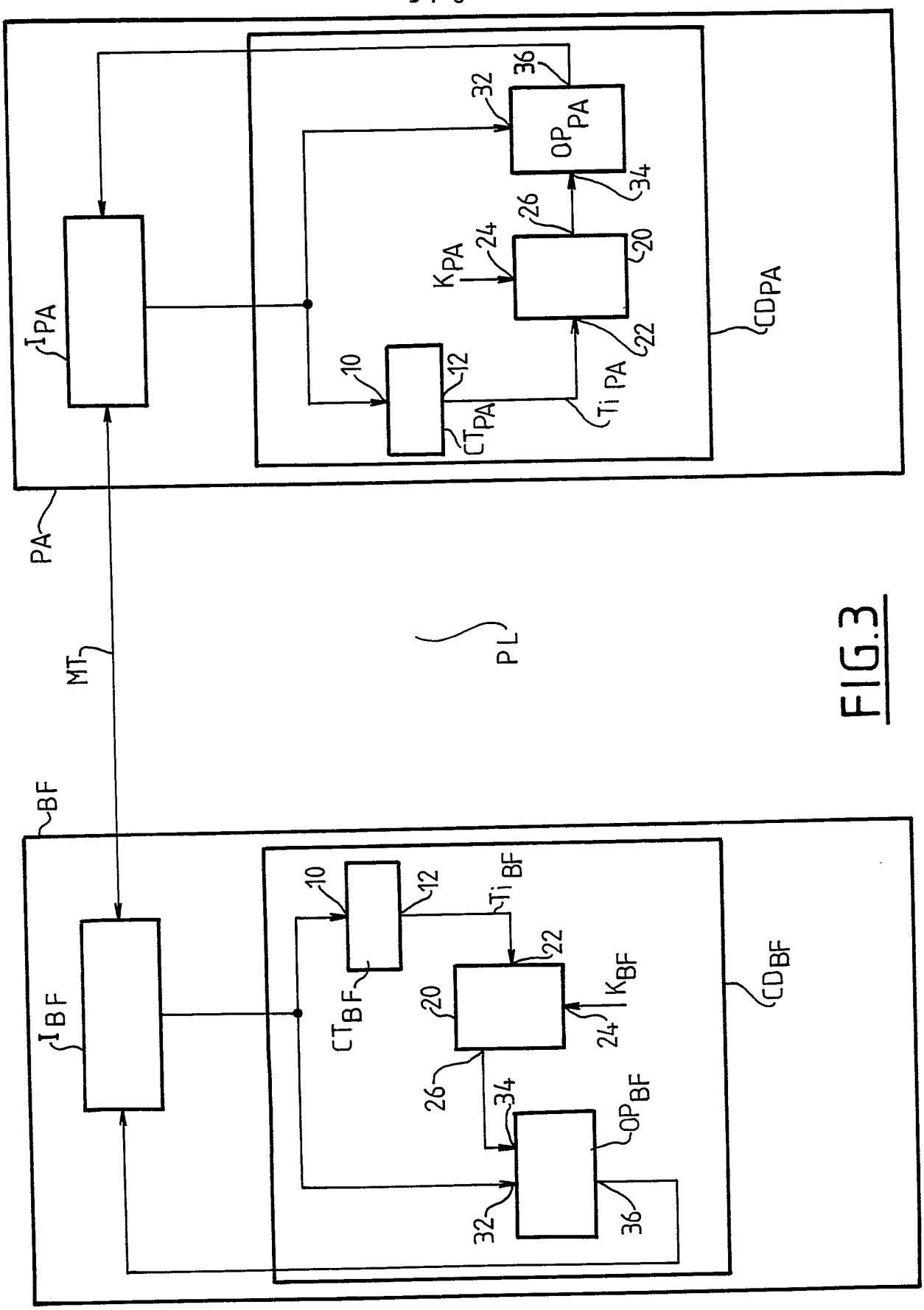

PA
IPA
10
12
CTPA
Ti PA
22
KPA
24
26
20
32
OPPA
34
36
CDPA
MT
PL
BF
IBF
10
12
CTBF
Ti BF
22
20
KBF
24
26
34
OPBF
32
36
CDBF

FIG.3

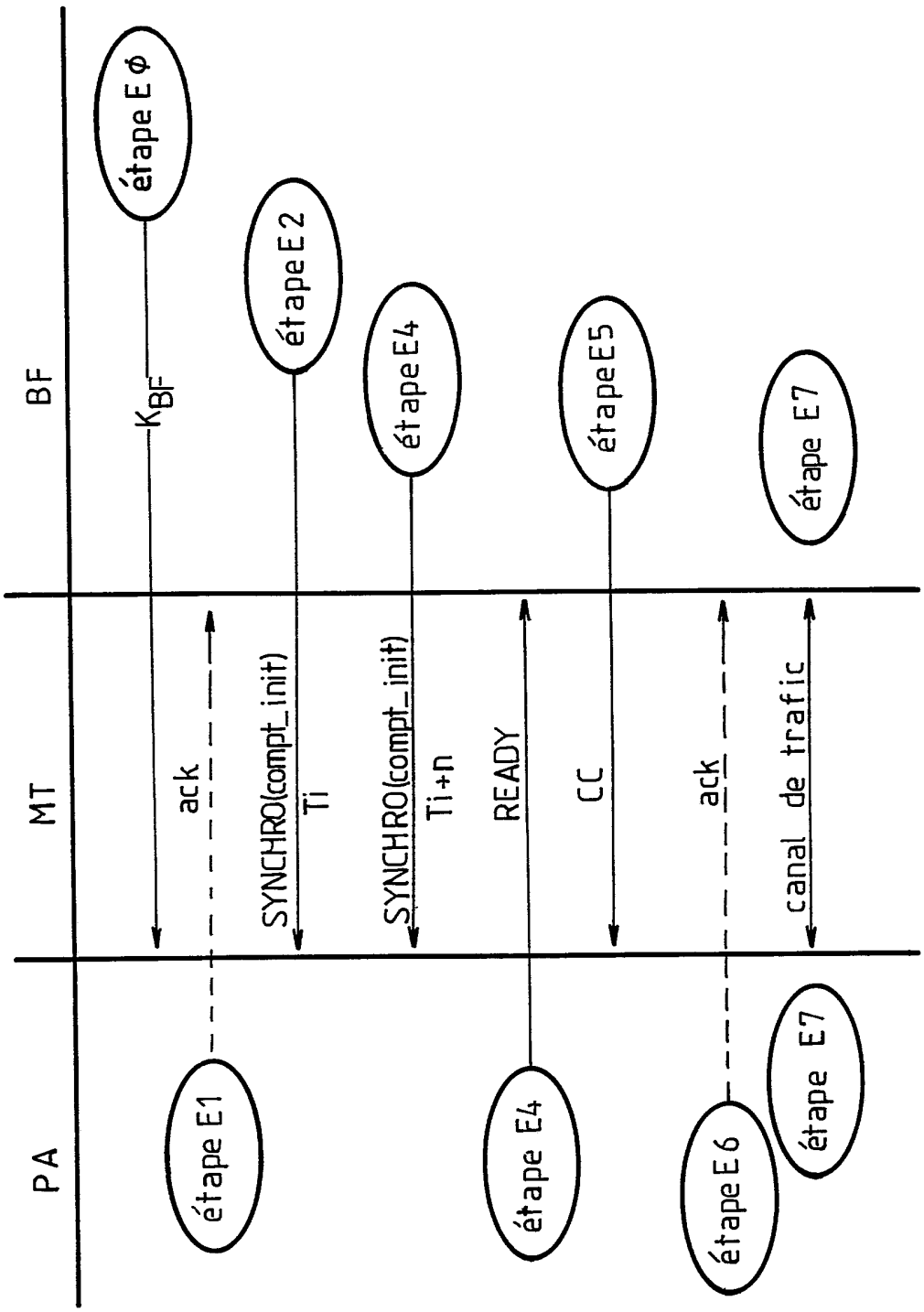

PA
MT
BF
étape E1
étape E4
étape E6
étape E7
étape E Φ
étape E 2
étape E4
étape E5
étape E7
K_{BF}
ack
SYNCHRO(compt_init)
Ti
SYNCHRO(compt_init)
Ti+n
READY
CC
ack
canal de trafic

FIG.4

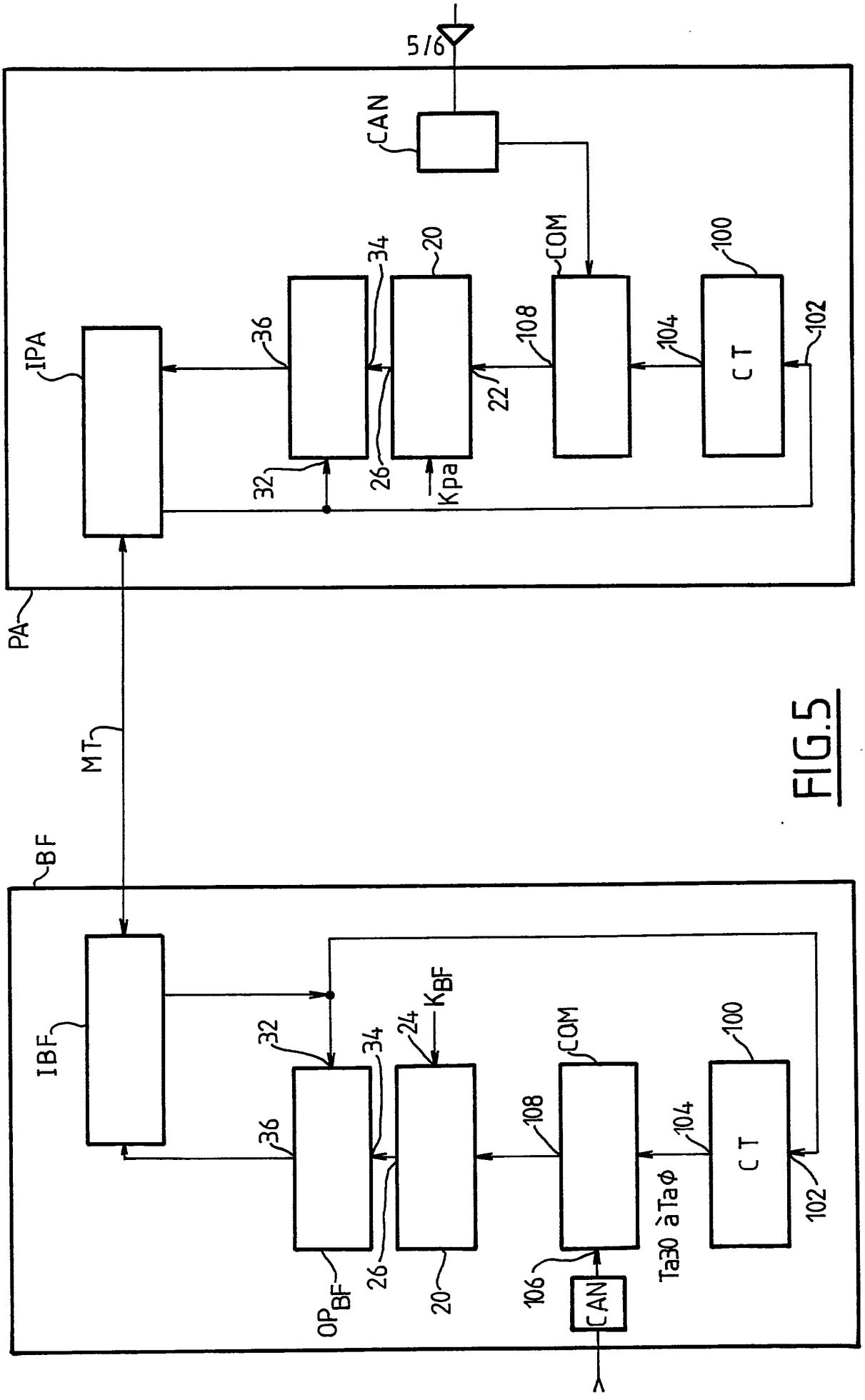

5/6
CAN
COM
100
20
34
36
IPA
108
104
C T
102
22
32
26
Kpa
PA
MT
BF
IBF
32
34
24
K_{BF}
COM
100
36
108
104
C T
102
Ta30 à Taφ
OP_{BF}
26
20
106
CAN

FIG.5

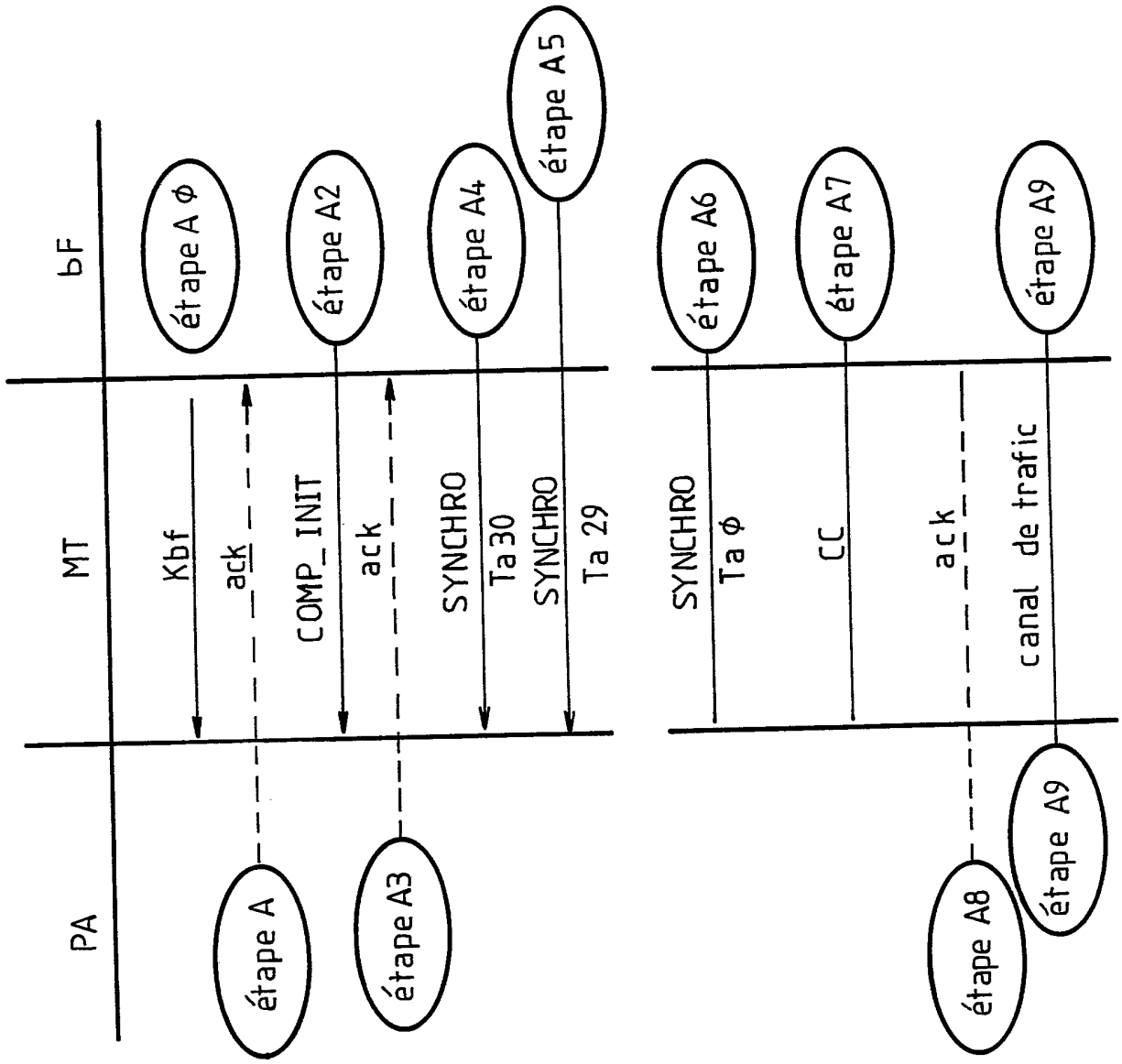

PA
MT
bF
étape A
étape A3
étape A Φ
étape A2
étape A4
étape A5
étape A6
étape A7
étape A8
étape A9
étape A9
Kbf
ack
COMP_INIT
ack
SYNCHRO
Ta 30
SYNCHRO
Ta 29
SYNCHRO
Ta Φ
CC
ack
canal de trafic

FIG.6

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

2669796

N° d'enregistrement national

FR 9014824
FA 453008

RAPPORT DE RECHERCHE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
A	BRITISH TELECOMMUNICATIONS ENGINEERING, vol. 9, partie 2, juillet 1990, pages 98-102, Londres, GB; R.S. SWAIN: "Digital cordless telecommunications-CT2" * Page 100, colonne de gauche, lignes 25-57; page 102, colonne de gauche, ligne 35 - colonne de droite, ligne 11 *	1
A	ELECTRICAL COMMUNICATION, vol. 63, no. 4, 1989, pages 389-399, Romford, Essex, GB; M. BALLARD et al.: "Cellular mobile radio as an intelligent network application" * Page 392, colonne de droite, ligne 22 - page 393, colonne de droite, ligne 12 *	1
A	DE-A-3 439 249 (PHILIPS KOMMUNIKATIONS INDUSTRIE) * Page 3, ligne 12 - page 4, ligne 12 *	1

DOMAINES TECHNIQUES RECHERCHES (Int. Cl.5)

H 04 Q
H 04 M
H 04 L

Date d'achèvement de la recherche: 09-08-1991

Examinateur: BEHRINGER L.V.

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P0413)