



(22) Date de dépôt/Filing Date: 2003/03/26

(41) Mise à la disp. pub./Open to Public Insp.: 2003/10/02

(30) Priorité/Priority: 2002/04/02 (02 04 088) FR

(51) Cl.Int.⁷/Int.Cl.⁷ H04L 9/12, H04L 12/18

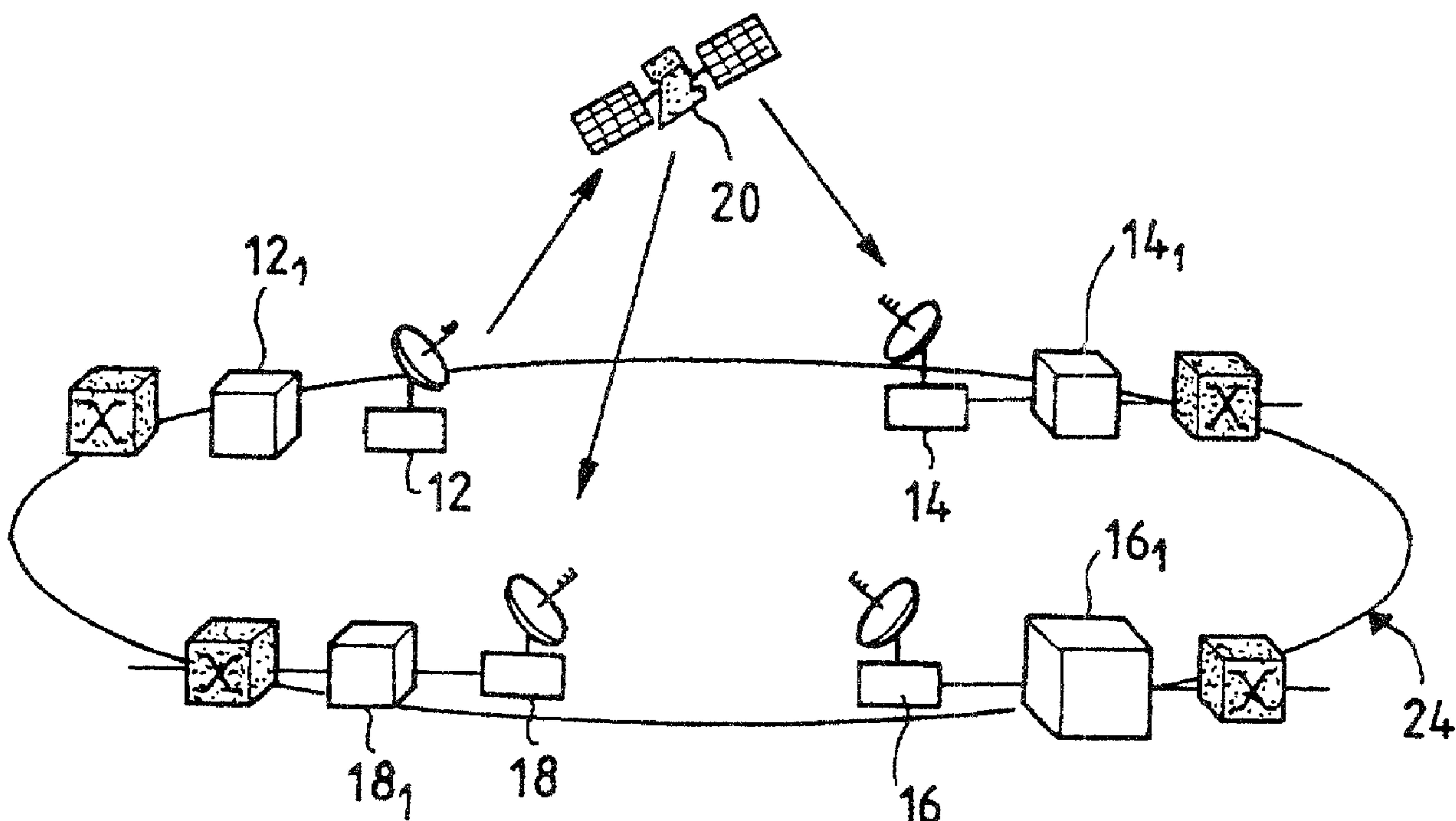
(71) Demandeur/Applicant:
ALCATEL, FR

(72) Inventeurs/Inventors:
JOSSET, SEBASTIEN, FR;
DUQUERROY, LAURENCE, FR

(74) Agent: ROBIC

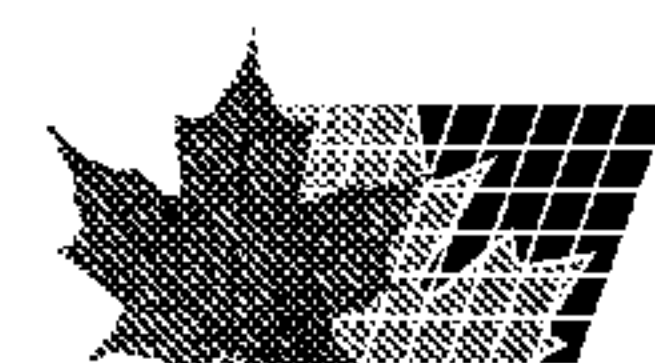
(54) Titre : SYSTEME DE TELECOMMUNICATION, NOTAMMENT DE TYPE IP, ET EQUIPEMENTS POUR UN TEL
SYSTEME

(54) Title: TELECOMMUNICATIONS SYSTEM, ESPECIALLY IP-TYPE, AND EQUIPMENT FOR SUCH A SYSTEM



(57) Abrégé/Abstract:

L'invention concerne un système de télécommunication comprenant une pluralité de terminaux (12, 14, 18) répartis selon des groupes tels qu'à l'intérieur de chaque groupe chaque terminal puisse émettre des messages multidestinations vers les autres membres du groupe. A chaque terminal d'un groupe sont associés des moyens de chiffrement et déchiffrement (12₁, 14₁, 18₁) de façon que chacun de ces terminaux puisse émettre des messages multidestinations déchiffrables uniquement par les autres terminaux du groupe. Le système comporte un serveur central (16₁) pour distribuer à chacun des moyens de chiffrement et de déchiffrement des clés pour la transmission sécurisée des communications à l'intérieur de chaque groupe.



ABREGE DESCRIPTIF

L'invention concerne un système de télécommunication comprenant une pluralité de terminaux (12, 14, 18) répartis selon des groupes tels qu'à l'intérieur de chaque groupe chaque terminal puisse émettre des messages multidestinations vers les autres membres du groupe.

A chaque terminal d'un groupe sont associés des moyens de chiffrement et déchiffrement (12₁, 14₁, 18₁) de façon que chacun de ces terminaux puisse émettre des messages multidestinations déchiffrables uniquement par les autres terminaux du groupe.

Le système comporte un serveur central (16₁) pour distribuer à chacun des moyens de chiffrement et de déchiffrement des clés pour la transmission sécurisée des communications à l'intérieur de chaque groupe.

**SYSTEME DE TELECOMMUNICATION, NOTAMMENT DE TYPE IP, ET
EQUIPEMENTS POUR UN TEL SYSTEME**

L'invention est relative à un système de
5 télécommunications, notamment de type IP ("Internet Protocol"),
et à des équipements pour un tel système.

Elle concerne plus particulièrement un système de
télécommunication dans lequel certains terminaux forment des
groupes et dans chaque groupe un terminal est susceptible
10 d'émettre, vers tous les autres terminaux, des messages, tels
que des paquets IP, qui ne doivent pas être compréhensibles par
les terminaux des autres groupes.

Pour résoudre ce type de problème de façon sûre on
fait en général appel à un chiffrement des messages. A cet effet
15 des algorithmes et des clés sont négociés entre les terminaux
deux à deux. Autrement dit un message sécurisé ne peut être
adressé qu'à un seul destinataire et non simultanément à une
pluralité de destinataires. Dans ces conditions si un groupe
comporte n terminaux, chaque message doit être envoyé $n-1$ fois.

20 Cette multiplication des messages sécurisés à envoyer
entraîne une augmentation du trafic qui peut conduire à une
saturation du réseau. En outre, les sessions d'établissements de
liens sécurisés deux à deux entre terminaux peuvent aussi
contribuer à l'augmentation du trafic.

25 L'invention remédie à ces inconvénients.

Le système selon l'invention est caractérisé en ce
qu'il comprend un serveur central destiné à fournir à tous les
terminaux d'un groupe des clés de chiffrement et de déchif-
frement pour permettre que chaque terminal du groupe puisse
30 émettre vers les autres terminaux du groupe un seul message
chiffré et que les terminaux destinataires puissent déchiffrer
le message ainsi émis.

Ainsi, avec l'invention, l'envoi de messages
multidestination de type sécurisé n'entraîne pas la nécessité de

transmettre autant de messages cryptés que de destinataires et le trafic est donc limité au minimum.

L'invention est particulièrement utile pour les transmissions sans fil à l'aide d'antennes terrestres ou à
5 l'aide d'équipements à bord d'un ou plusieurs satellites. En effet, ce type de diffusion d'informations présente l'avantage de permettre de servir une multiplicité de terminaux, en particulier des terminaux éloignés les uns des autres dans le cas d'une diffusion par satellite.

10 Mais de tels moyens de transmission de données sont plus difficiles à protéger contre les indiscretions que les réseaux filaires terrestres car, dans un réseau filaire, pour pouvoir intercepter des informations il faut accéder au câblage alors qu'avec une transmission sans fil, tout terminal se
15 trouvant dans le champ de l'antenne correspondante est capable d'intercepter les informations transmises. De même un terminal émetteur non autorisé peut s'insérer dans le réseau.

Il est donc préférable de transporter les informations, tels que les paquets IP, en mode sécurisé comme
20 c'est le cas avec l'invention.

Bien que l'invention ne soit pas limitée à ces applications, dans ce qui suit on décrira surtout l'invention pour les réseaux faisant intervenir une transmission de paquets IP par l'intermédiaire d'équipements à bord de satellites. Il
25 existe divers protocoles permettant de sécuriser le transport des paquets IP. Cette sécurité s'effectue soit au niveau physique (par exemple par agilité en fréquence), soit au niveau accès (par exemple par brouillage), soit au niveau IP (en utilisant le protocole IPsec), soit au niveau transport (en
30 faisant appel au protocole TLS "Transport Layer Security"), soit, enfin, au niveau de l'application (protocole SSL "Secure Socket Layer"). Mais aucun de ces protocoles de sécurité n'est adapté à l'obtention d'une sécurité élevée pour la transmission de type multidestination, c'est-à-dire pour la transmission
35 simultanée de paquets IP à une multiplicité de destinataires.

Ainsi, le brouillage par le protocole DVB-RCS n'offre pas une sécurité d'un degré élevé ; les protocoles IPsec au niveau IP et les protocoles TLS au niveau transport ainsi que SSL au niveau application ne sont adaptés qu'à une sécurité point à point, c'est-à-dire entre deux destinataires mais non dans un groupe, c'est-à-dire vers une multiplicité de destinataires.

Dans cette application, les terminaux sont en communication les uns avec les autres par transmission sans fil, notamment par satellite, et à chaque terminal d'émission/réception est associé un organe de chiffrement et de déchiffrement destiné à chiffrer les informations émises par voie hertzienne et à déchiffrer les informations reçues par cette voie.

Dans une réalisation préférée (qui s'applique quel que soit le type de réseau) le serveur, outre sa fonction de distribution des clés de chiffrement et déchiffrement permet d'authentifier les organes de chiffrement et de déchiffrement associés à chaque terminal.

Dans une réalisation, les paquets IP émis par un terminal sont transmis en mode tunnel, c'est-à-dire que chaque paquet IP chiffré est encapsulé dans un autre paquet de façon à non seulement protéger les données elles-mêmes, mais aussi les en-têtes, dont par exemple les adresses source et destinataires.

L'organe de chiffrement et déchiffrement associé à chaque terminal constitue, dans une réalisation, un boîtier distinct de celui du terminal. En variante, cet organe est réalisé par logiciel au sein de la pile IP du terminal.

Dans un mode de réalisation, chaque organe associé à un terminal du réseau comporte un premier sélecteur pour déterminer si les données à émettre doivent être chiffrées ou non, et un second sélecteur pour déterminer si les données reçues doivent subir un déchiffrement ou non.

La commande des sélecteurs ainsi que du chiffrement et du déchiffrement est de préférence effectuée dans un plan de contrôle séparé du plan des données.

En variante, à la place de paquets IP, on fait appel à
5 d'autres formats ou normes tels que ATM, Ethernet, MPLS ("Multi-protocol Label Switching" de la norme IETF), PPP ("Point to Point Protocol") ou PPPoE ("Point to Point Protocol Over Ethernet").

L'invention concerne de façon générale un système de
10 télécommunication comprenant une pluralité de terminaux répartis selon des groupes tels qu'à l'intérieur de chaque groupe chaque terminal puisse émettre des messages multide destinations vers les autres membres du groupe qui est caractérisé en ce qu'à chaque terminal d'un groupe sont associés des moyens de chiffrement et
15 déchiffrement de façon que chacun de ces terminaux puisse émettre des messages multide destinations déchiffrables uniquement par les autres terminaux du groupe, et en ce que le système comporte un serveur central pour distribuer à chacun des moyens de chiffrement et de déchiffrement des clés pour la transmission
20 sécurisée des communications à l'intérieur de chaque groupe.

Les messages transmis sont, par exemple, selon un protocole réseau. Dans une réalisation, le protocole réseau est choisi dans le groupe comprenant les protocoles IP, ATM, MPLS, Ethernet, PEP, PPPoE.

25 Selon une réalisation, les terminaux sont reliés à un réseau terrestre filaire et fournissent les messages déchiffrés à ce réseau filaire.

Les terminaux sont, dans un exemple, reliés les uns aux autres par un réseau à diffusion, par exemple de type
30 hertzien, notamment par satellite, ou local, par exemple du type ethernet. De préférence, les terminaux sont aptes à fournir des messages chiffrés au réseau à diffusion ou au réseau local. Le serveur central est, par exemple, relié aux terminaux par l'intermédiaire du réseau à diffusion.

L'invention concerne aussi un dispositif de chiffrement et de déchiffrement qui est caractérisé en ce qu'il comporte une interface pour recevoir et émettre, à travers un premier réseau de télécommunication, des messages chiffrés, une
5 interface connectée à un second réseau pour recevoir de ce second réseau des messages à chiffrer à transmettre par le premier réseau et pour délivrer sur ce second réseau des messages déchiffrés et provenant du premier réseau, et une interface pour recevoir d'un serveur des clés de chiffrement et
10 déchiffrement, les clés de chiffrement permettant de chiffrer un message multidestinations vers des destinataires sélectionnés faisant partie d'un même groupe qu'un terminal auquel le dispositif est associé.

De préférence, le dispositif est tel que le premier
15 réseau est du type hertzien ou filaire, notamment par satellite, et le second réseau est de type filaire.

Dans une réalisation, le plan de contrôle et le plan de données du dispositif sont séparés.

Selon un mode de réalisation, le dispositif est tel
20 que les messages sont des paquets d'un protocole réseau. Dans ce cas, le dispositif comporte de préférence des moyens pour émettre des paquets IP sécurisés en mode tunnel. Le dispositif comporte, selon une réalisation, un moyen pour transmettre les paquets IP chiffrés avec un premier en-tête de routage et
25 d'adresse et un second en-tête concernant les données de sécurité de ce paquet.

Toujours dans le cas où le dispositif comporte des moyens pour émettre des paquets IP sécurisés en mode tunnel, selon une réalisation, ce dispositif comporte un moyen pour
30 émettre et recevoir des seconds en-têtes avec des données de sécurité comprises dans le groupe comportant : des données d'identi-fication permettant au(x) récepteur(s) de déterminer les fonctions et clés à utiliser pour rendre sa forme initiale à chaque paquet et vérifier son intégrité et son origine, des

données relatives à la segmentation des paquets, des données de durée de vie de clés de session, et un numéro de paquet.

Dans une réalisation, l'interface pour la connexion du dispositif au premier réseau est connectée directement à une interface d'un terminal de ce réseau.

En variante, le dispositif est réalisé sous la forme d'un logiciel intégré à la pile de logiciels réseau d'un terminal du premier réseau.

L'invention concerne, enfin, un serveur pour système de télécommunication permettant la transmission et la réception de messages multi-destinations, qui est caractérisé en ce qu'il comprend des moyens pour transmettre à chacun des émetteurs et récepteurs de messages multi-destinations des éléments de sécurité pour permettre que chacun des émetteurs puisse chiffrer les messages multi-destinations et chacun des récepteurs puisse déchiffrer les messages reçus afin que tous les destinataires faisant partie d'un groupe puissent recevoir simultanément les messages chiffrés reçus.

De préférence, le serveur est tel que les messages sont des paquets selon un protocole réseau.

Dans une réalisation, le serveur comporte des moyens de connexion à un réseau pour transmettre de façon confidentielle et sécurisée les éléments de sécurité à chacun des émetteurs et récepteurs de messages selon un mode mono et/ou multidestinations. Les éléments de sécurité à transmettre sont, par exemple, compris dans le groupe comportant : des fonctions et clés à utiliser pour protéger des paquets, c'est-à-dire pour chiffrer, déchiffrer et authentifier les paquets, ou pour modifier les paquets, des formats d'encapsulation des paquets, notamment IP, des données de filtrage définissant le groupe destinataire des paquets, et des données de durées de vie des éléments de sécurité.

De préférence, les fonctions de sécurité et les modifications apportées aux paquets réseau sont séparées et forment des blocs chaînés. Dans ce cas, selon une réalisation,

le serveur comporte des moyens pour supprimer, ajouter ou remplacer au moins un bloc. Les blocs chaînés sont, par exemple, compris dans le groupe incluant : le protocole IPSec ESP, le protocole IPSec AH, le chiffrement, l'authentification, le mode
5 tunnel, un protocole TCP spoofer, un protocole IGMP proxy et un protocole Drop.

Les moyens de transmission du serveur vers les émetteurs et récepteurs comportent, dans une réalisation, des moyens pour, qu'au cours d'une première phase, le serveur
10 communique par des messages mono-destination avec les émetteurs et récepteurs afin de réaliser une authentification mutuelle et mettre en place un tunnel chiffré. De préférence, le serveur comporte, dans ce cas, des moyens pour, qu'au cours d'une seconde phase, il puisse envoyer à chaque émetteur et récepteur
15 des messages de configuration en mode mono-destination. Le serveur peut aussi comporter des moyens pour, qu'au cours d'une autre phase, il puisse envoyer des messages de configuration de type multidestinations à plusieurs émetteurs et récepteurs.

De préférence, le serveur comprend des moyens pour
20 fiabiliser l'envoi des éléments de sécurité vers chacun des émetteurs et récepteurs de messages multi-destinations ou monodestinations.

Ces moyens de fiabilisation comprennent, par exemple, un moyen pour retransmettre un message non acquitté par son
25 destinataire après un temps prédéterminé.

Selon une réalisation, le serveur est tel que les éléments de sécurité sont envoyés vers chacun des émetteurs/récepteurs par un message multidestinations, et à chaque émetteur/récepteur destinataire est associé une durée
30 prédéterminée d'acquiescement qui diffère d'un destinataire à un autre afin que le serveur ne reçoive pas simultanément plusieurs signaux de non acquiescement.

Les moyens de fiabilisation comportent, dans un exemple, un moyen pour associer à chaque message un numéro de
35 séquence. Dans ce cas, selon une réalisation, les moyens de

fiabilisation comprennent un moyen pour recevoir des messages d'acquittement comportant les numéros de séquence des messages émis correspondants et pour renvoyer les messages correspondant aux numéros de séquence non acquittés.

5 En variante, les moyens de fiabilisation comportent, pour les messages multidestinataires, un moyen pour détecter des acquittements négatifs provenant d'émetteurs/récepteurs indiquant que ces derniers n'ont pas reçu de messages pour un numéro de séquence donné et des moyens pour retransmettre les
10 messages correspondant aux acquittements négatifs.

D'autres caractéristiques et avantages de l'invention apparaîtront avec la description de certains de ses modes de réalisation, celle-ci étant effectuée en se référant aux dessins ci-annexés sur lesquels:

15 la figure 1 est un schéma d'un système de télécommunication conforme à l'invention,

 la figure 2 est un schéma d'un dispositif de chiffrement et déchiffrement conforme à l'invention,

 la figure 3 montre une application du dispositif
20 montré sur la figure 2,

 la figure 4 représente une variante de l'utilisation du dispositif montré sur la figure 2,

 la figure 5 est un schéma montrant un paquet chiffré par le dispositif de la figure 2,

25 la figure 6 représente un exemple d'échanges de messages de sécurité,

 la figure 7 est un schéma analogue à celui de la figure 6 pour une autre phase d'échanges de messages, et

 la figure 8 est aussi un schéma analogue à celui de la
30 figure 6, mais pour encore une autre phase d'échanges de messages.

L'exemple de réalisation de l'invention que l'on va maintenant décrire en relation avec les figures concerne un réseau de télécommunication par satellite, relié à un réseau

terrestre. Ces réseaux sont destinés à transporter des paquets selon le protocole IP.

Le réseau de télécommunication par satellite comporte un ensemble de terminaux terrestres 12, 14, 16, 18 etc. destinés à émettre, et recevoir, selon le protocole IP. Les paquets émis et reçus transitent par des équipements de réémission et de réception à bord d'un satellite 20. Le satellite 20 est d'un type quelconque, géostationnaire ou défilant.

Les paquets émis par chaque terminal 12 sont de type mono ou multideestination. Par monodeestination on entend qu'un terminal envoie un message vers un seul autre terminal. Par "multideestination", on entend qu'un terminal envoie ses messages vers une pluralité d'autres terminaux. Certaines communications multide destinations ne sont pas destinées à l'ensemble des terminaux se trouvant dans le champ du satellite mais seulement à des terminaux faisant partie d'un même groupe. Les données destinées à des terminaux sélectionnés sont donc chiffrées.

A cet effet, on affecte à chaque terminal 12, 14, etc. un organe de chiffrement et de déchiffrement 12₁, 14₁ etc. qui, comme représenté, peut être sous forme d'un boîtier séparé du terminal 12.

En variante (non montrée sur la figure 1) les organes de chiffrement et de déchiffrement sont intégrés dans les logiciels des terminaux satellites. Ces mécanismes de chiffrement et déchiffrement ainsi que les autres fonctions des organes 12₁, 14₁ etc. peuvent être, dans ce cas, intégrés dans la pile IP des terminaux 12, 14.

Dans ce qui suit, on décrira principalement le cas représenté, c'est-à-dire le cas où l'on prévoit des boîtiers 12₁, 14₁ etc. de chiffrement et de déchiffrement qui sont séparés des terminaux 12, 14, etc.

Les boîtiers 12₁, 14₁ sont gérés par un boîtier maître 16₁, ou serveur, dont le rôle est d'authentifier les boîtiers 12₁, 14₁, 16₁, 18₁ etc., appelés boîtiers clients, et de leur distribuer toutes les informations dont ils ont besoin qui se

rapportent au niveau de sécurité retenu pour la transmission des données du groupe formé par les terminaux et boîtiers associés, c'est-à-dire toutes les informations permettant que les données fournies par un membre du groupe soient compréhensibles
5 seulement par les autres membres de ce groupe.

L'ensemble des paramètres à fournir à chaque boîtier est appelé une "association de sécurité" et ces paramètres sont distribués à chaque nouveau boîtier après vérification de son identité.

10 Les paquets IP émis par un des membres du groupe sont chiffrés, par le boîtier 12₁, 14₁, ... à leur entrée dans le réseau de communication par satellite 20. Ces paquets peuvent être reçus par l'ensemble des terminaux dans le champ du satellite mais ne pourront être déchiffrés que par les
15 différents autres membres du groupe, grâce à leurs boîtiers correspondants.

La transmission dans le réseau satellite peut s'effectuer en mode tunnel, c'est-à-dire qu'un paquet IP, qui comprend des données et un en-tête, est chiffré dans son entier
20 et ce paquet chiffré forme la partie de données d'un nouveau paquet auquel on ajoute un autre en-tête. Le type de traitement exact qui est effectué sur le paquet est décrit dans l'association de sécurité. Il est non seulement possible de chiffrer le paquet en entier mais aussi de modifier des champs
25 IP.

On comprend que l'invention permet d'utiliser une architecture de réseau de transmission par satellite sans le modifier.

La figure 2 représente sous forme de bloc fonctionnel
30 la structure d'un boîtier, tel que le boîtier 12₁.

Ce boîtier comporte un premier sélecteur 30 recevant des données du réseau terrestre 24 et qui fournit au réseau 20₁ satellite 20 soit directement les données (liaison 32), dans le cas où aucun chiffrement n'est prévu, soit des données chiffrées
35 par l'intermédiaire d'un organe 34 de chiffrement.

Le boîtier 12₁ comporte un second sélecteur 36 recevant des données du réseau 20₁ et fournissant des données au réseau terrestre 24 soit directement par la liaison 38, soit par l'intermédiaire d'un organe 40 de déchiffrement.

5 Chacun des sélecteurs 30 et 36 ainsi que l'organe de chiffrement 34 et l'organe de déchiffrement 40 reçoit des données de commandes d'un plan de commande ou contrôle 42.

10 La figure 3 illustre une réalisation dans laquelle les protocoles utilisés par les boîtiers 12₁, 14₁ ... sont du type Ethernet (eth0, eth1), la transmission s'effectuant au niveau de la couche physique des données, c'est-à-dire au niveau d'une trame Ethernet sans remonter à la couche IP.

15 Ainsi toutes les trames Ethernet sont capturées par les boîtiers clients et les paquets en sont extraits, éventuellement chiffrés comme expliqué ci-dessus, puis réintroduits dans la trame avant d'être transmis vers le réseau satellite 20₁.

Les trames provenant du réseau 20₁ subissent le traitement inverse après vérification de leur intégrité.

20 Chacun des boîtiers clients, est muni d'une adresse IP qui lui est spécifique. Cette adresse IP permet de communiquer avec le boîtier maître et de s'authentifier auprès de ce boîtier pour recevoir les paramètres de l'association de sécurité. L'adresse IP est également utile pour le renouvellement des
25 clés.

La figure 4 illustre l'organe de chiffrement et de déchiffrement dans le cas où il constitue un logiciel du terminal satellite.

30 Les données provenant du réseau satellite sont fournies à un module d'interface 50 qui transmet ces données à un module 52 de désencapsulage des paquets IP. Les paquets IP désencapsulés sont fournis à un bloc 54 contenant des modules sélecteurs et de déchiffrement ayant la même fonction que les organes décrits en relation avec la figure 2. Les données du

bloc 54 sont fournies à la couche IP 56 par l'intermédiaire d'une interface 58 avec la couche IP.

Les données de la couche IP sont transmises sur le réseau terrestre et routées à l'aide d' interfaces 60₁, 60₂ et
5 transmises vers des interfaces respectifs 62₁, 62₂.

Bien entendu, les interfaces fonctionnent dans les deux sens.

Quel que soit le mode de réalisation des boîtiers clients et maître leur fonction la plus importante est d'assurer
10 des services de sécurité.

Ainsi, les boîtiers clients ainsi que le boîtier maître permettent tout d'abord de protéger et sécuriser les communications IP. La confidentialité du trafic est assurée grâce au chiffrement des données et des en-têtes des paquets IP
15 et par la transmission en mode tunnel dans le réseau 20₁ à satellite.

Chacun des boîtiers clients comporte des moyens pour vérifier l'intégrité des données, c'est-à-dire pour vérifier si chaque paquet IP reçu a subi des modifications, accidentelles ou
20 intentionnelles.

Chaque boîtier client peut permettre aussi d'authentifier l'origine des données, c'est-à-dire de vérifier que chaque paquet IP provient d'un des membres du groupe.

Les boîtiers peuvent permettre enfin d'empêcher les
25 attaques par rejeu. A cet effet on assigne à chaque paquet un nombre entier unique constituant un numéro d'ordre. Dans ces conditions, si un paquet est renvoyé par un tiers étranger au groupe, ce paquet "rejoué" aura un numéro qui ne correspondra pas à la succession des autres paquets.

30 Le boîtier maître 16₁ comporte des moyens d'authentification des boîtiers.

De façon générale ce boîtier maître assure une gestion centralisée des clés à utiliser par chaque boîtier client pour sécuriser le trafic IP. Ainsi le boîtier maître génère les clés,
35 les distribue et les renouvelle.

Le boîtier maître et les boîtiers clients peuvent être organisés de façon telle que, dans un même groupe, on puisse définir plusieurs niveaux de sécurité. Par exemple si un groupe d'utilisateurs est constitué de tous les membres d'une
5 entreprise, on pourra distinguer entre les membres du siège et les membres de chaque filiale, caractérisés par leurs adresses réseau.

On notera que les services de protection des données, à savoir le service de confidentialité du trafic, le service
10 d'authentification de l'origine des données, et le service de vérification de l'intégrité des données peuvent être utilisés séparément ou en combinaison.

Ainsi il est possible d'assurer la confidentialité du trafic sans vérification de l'authenticité de l'origine des
15 données ou de l'intégrité de ces données. Pour une sécurité plus importante on assurera à la fois la confidentialité du trafic et l'authentification des données et/ou la vérification de leur intégrité. Il est également possible de vérifier l'authenticité de leur origine des données et/ou leur intégrité, sans assurer
20 la confidentialité du trafic.

Pour le contrôle des données, on définit un plan de contrôle qui comporte des moyens dans chaque boîtier maître et dans chaque boîtier client.

Le boîtier maître constitue un serveur central pour la
25 gestion des boîtiers clients. Ce boîtier maître comporte une base de données des boîtiers clients autorisés à accéder aux données qui doivent être échangées à l'intérieur du groupe.

Dans cette base de données chaque boîtier client est répertorié par un identifiant logique unique et par une donnée
30 secrète connue uniquement du boîtier maître et du boîtier client concerné et servant à l'authentification. Dans la base de données on prévoit aussi, pour chaque boîtier client, une liste d'identifiants d'associations de sécurité auxquelles ce boîtier client est autorisé à accéder.

Les paramètres principaux de la base de données des associations de sécurité sont:

- des paramètres de filtrage, définissant le groupe destinataire;
- 5 - les paramètres des fonctions réalisées par l'association de sécurité, à savoir:
 - Le type de l'association de sécurité qui définit le format d'encapsulation des paquets IP,
 - la transmission en mode tunnel pur ou en mode tunnel
 - 10 transport avec l'adresse IP du (ou des) destinataire(s) (selon qu'il s'agisse d'une transmission mono ou multidestinataires),
 - une fonction d'authentification qui comprend les possibilités suivantes: aucune authentification, une fonction HMAC-SHA1, HMAC-RD5 etc. ; les paramètres de cette fonction
 - 15 d'authentification sont d'une part, la clé à utiliser, et, d'autre part, la longueur de cette clé et sa durée de vie,
 - la fonction de chiffrement qui peut comprendre les possibilités suivantes: aucun chiffrement, 3DESECB, 3DESCBC, etc.; le chiffrement comporte aussi comme paramètres la clé à
 - 20 utiliser, sa longueur et sa durée de vie.
- la durée de validité de l'association de sécurité ; cette durée de validité est, bien entendu, liée à la durée de vie des clés utilisées.

Pour le plan de contrôle, chaque boîtier client

25 comporte, dans l'exemple, une carte à mémoire, par exemple à microprocesseur, dont la mémoire contient l'identifiant logique du boîtier ainsi que la clé (secrète) partagée uniquement avec le boîtier maître. Dans la mémoire de la carte, on prévoit aussi une adresse IP et un paramètre définissant ce boîtier comme

30 constituant un élément du réseau.

Avant qu'un boîtier client soit autorisé à recevoir et émettre des paquets IP de façon sécurisée, une connexion est établie entre ce boîtier client et le boîtier maître afin de démarrer une session préalable d'autorisation appelée phase 1

35 (figure 6), suivie de l'envoi par le boîtier maître des

informations de configuration en mode monodestination (phase 2 - figure 7) et/ou en mode multide destinations (phase 2 bis - figure 8). Ces informations sont échangées par l'intermédiaire du réseau à satellite.

5 Lors de la phase 1 (figure 6) une authentification mutuelle est effectuée entre le boîtier client et le boîtier maître (par exemple, à l'aide d'une clé partagée). Le boîtier maître peut alors vérifier l'identité du boîtier client et déterminer s'il est autorisé à accéder aux associations de
10 sécurité du groupe auquel il appartient. Le boîtier client, de son côté, vérifie qu'il a bien affaire au boîtier maître.

 Lors de la phase 1 (figure 6), une clé commune secrète est engendrée, par exemple à l'aide du schéma Diffie-Hellman, et cette clé est utilisée ensuite pour transmettre de façon
15 sécurisée les tables ou paramètres de l'association de sécurité du groupe.

 Pour la phase 1, on peut utiliser la première phase du protocole IKE (Internet Key Exchange : Norme IETF), soit en mode principal (comme montré sur la figure 6), soit en mode
20 agressif.

- Le mode principal permet de réaliser une authentification mutuelle par clés partagées et de générer une clé commune secrète.

- Le mode agressif permet également de réaliser
25 une authentification mutuelle par clés partagées et de générer une clé commune secrète. Lorsqu'on fait appel à ce mode, la phase 1 s'effectue de façon plus rapide que dans le cas du mode principal. Ce mode agressif ne protège pas l'identité des boîtiers maître et client.

30 On établit ainsi un tunnel sécurisé entre chaque boîtier client et le boîtier maître. Ce n'est qu'à la suite de ces échanges que l'ensemble des paramètres des associations de sécurité à utiliser pour sécuriser les paquets IP à destination du groupe d'utilisateurs (clés incluses) peut être envoyé
35 secrètement au boîtier client par le boîtier maître.

Cette transmission des paramètres peut non seulement être effectuée par des messages monodestination (phase 2 - figure 7), mais elle peut être également réalisée par des messages multide destinations (phase 2 bis - figure 8). Dans ce dernier cas, le boîtier maître s'adresse à plusieurs boîtiers clients appartenant à un même groupe. Cette phase est protégée par l'association de sécurité de contrôle. Elle peut servir à la configuration des boîtiers clients ou à la mise à jour de leurs associations de sécurité. Cette phase peut être utilisée lorsque de nombreux boîtiers clients d'un même groupe établissent en même temps une connexion avec le boîtier maître. Dans ce cas, le boîtier maître peut envoyer en monodestination seulement l'association de sécurité de contrôle pour chaque boîtier client, et ensuite se peut transmettre simultanément à l'ensemble des boîtiers clients les tables des associations de sécurité auxquelles ils ont le droit d'accéder.

Cette transmission multide destinations optimise la bande passante. Elle peut également intervenir après la transmission monodestination pour mettre à niveau les associations de sécurité des boîtiers clients afin que ceux-ci soient mis à jour en même temps.

A la suite de la phase 1, en mode principal ou agressif, les clés de session -utilisées pour le chiffrement et le déchiffrement, l'authentification et la vérification de l'intégrité des paquets IP par les boîtiers clients- sont donc distribuées par le boîtier maître et renouvelées ensuite de façon régulière. Pour cette distribution et ce renouvellement de clés, on utilise soit un mode nominal soit un mode dégradé.

- Pour le renouvellement des clés en mode nominal, on fait appel à l'association de sécurité de contrôle, qui est commune à tous les boîtiers clients et reçue lors de la phase 2 (figure 7). Cette association de sécurité de contrôle sert à protéger les clés de session. Lors du renouvellement des clés de session, le boîtier maître peut envoyer simultanément à tous

les boîtiers clients autorisés les nouvelles clés chiffrées avec la clé de chiffrement de l'association de sécurité de contrôle.

Ce mode nominal convient particulièrement bien lorsque le nombre de boîtiers est élevé puisque les clés sont envoyées
5 simultanément à tous les boîtiers.

- En mode dégradé, les clés de session sont envoyées à chaque boîtier client. Pour chaque boîtier client, elles sont protégées par le tunnel sécurisé établi en phase 1 avec le boîtier maître (figure 6). Ce mode dégradé fait donc
10 appel à une transmission une par une. Il se distingue du mode nominal par le fait qu'on ne fait pas appel à l'association de sécurité de contrôle.

Le plan des données comprend le format des paquets IP, les en-têtes des divers types de paquets et les fonctions et
15 algorithmes utilisés.

La figure 5 représente un paquet IP classique qui comporte, d'une part, une partie de données 70 et, d'autre part un en-tête IP 72.

Comme indiqué ci-dessus, pour assurer une transmission
20 sécurisée des paquets dans le réseau 20, on fait appel au mode tunnel dans lequel un nouveau paquet IP est créé à partir du paquet initial, le paquet initial étant sécurisé, c'est-à-dire que son en-tête et ses données sont chiffrées.

Comme montré sur la figure 5, le paquet 70, 72 est
25 chiffré pour former le paquet 74 auquel on ajoute, d'une part, un en-tête IP'76 pour l'adressage et le routage, et d'autre part, un en-tête SatIPsec 78 pour la sécurisation des données à transmettre, et nécessaire pour leur déchiffrement.

La transmission peut s'effectuer en mode tunnel pur,
30 dans lequel l'adresse IP source du nouveau paquet IP formé est l'adresse IP du boîtier émetteur, et l'adresse IP destinataire est celle du (des) boîtier(s) destinataire(s). Autrement dit, les adresses IP de la source d'origine et du destinataire final peuvent être cachées dans ce cas.

On peut également faire appel au mode tunnel transport dans lequel les adresses de la source et du destinataire du paquet IP formé pour le transport sont celles du paquet initial.

L'en-tête SatIPsec 78 dédié aux mécanismes et
5 fonctions de sécurité appliqués au paquet IP initial peut comporter un ou plusieurs des champs suivants:

- Un identifiant de l'association de sécurité appliquée au paquet. Ce champ permet à chaque boîtier d'identifier pour un paquet IP reçu les fonctions et les clés à
10 utiliser pour lui rendre sa forme initiale.

- Un champ d'authentification qui fournit une valeur résultant de l'application d'une fonction de hachage sur le paquet 74,76,78.

- Un paramètre indiquant, d'une part, la longueur
15 du paquet et, d'autre part, si ce dernier a été segmenté avant d'être transmis en mode tunnel. Dans ce cas, le paramètre indique si on a affaire au premier ou au dernier segment, ou à un segment intermédiaire. Ce champ permet au boîtier récepteur d'effectuer l'assemblage du paquet initial.

20 - La durée de vie de l'association de sécurité avec la date de début et la date de fin. Ce champ indique si une nouvelle clé de session est utilisée ou si la clé actuelle arrive en fin de vie.

- Un compteur qui est incrémenté à chaque paquet
25 IP envoyé. Le nombre ainsi affecté à chaque paquet permet d'éviter les attaques par rejeu. Dans le cas où plusieurs sources sont prévues pour émettre des paquets IP, chacune de ces sources dispose de son propre compteur et les récepteurs doivent alors identifier la source du paquet IP avec l'adresse IP
30 source.

Les fonctions et algorithmes utilisés sont, par exemple, ceux du protocole de la norme IPSec, c'est-à-dire, pour le chiffrement des données, le protocole 3DES en mode CBC, et pour la vérification de l'intégrité, de l'authenticité et de

l'origine d'un paquet, des fonctions de hachage telles que HMAC-MD5 ou HMAC-SHA.

L'algorithme de chiffrement est appliqué sur le paquet IP initial, c'est-à-dire sur les en-têtes et les données.

5 Pour l'authentification, les fonctions de hachage sont appliquées sur l'ensemble du paquet, c'est-à-dire sur l'en-tête IP', sur l'en-tête SatIPsec et sur les données sécurisées. Il est ainsi possible de détecter toute modification sur les paramètres mentionnés en clair qui sont indispensables au
10 récepteur pour déchiffrer les paquets et réaliser les différentes vérifications ainsi que pour réassembler le paquet initial.

De façon générale, l'encapsulation des paquets IP dépend des associations de sécurité définies pour le trafic de
15 ces paquets . On peut ainsi utiliser l'encapsulation définie ci-dessus, les encapsulations normalisées IPSec AH/ESP ou une encapsulation IP dans IP. On peut aussi faire appel à une modification du paquet IP que l'on peut envoyer sans encapsulation.

20 Quel que soit son mode de réalisation, l'invention assure de façon simple une sécurisation des données multidestinations ou monodestinations transmises notamment sous le protocole IP par système hertzien et plus particulièrement par satellite. Elle est adaptée aux réseaux dits VPN ("Virtual
25 Private Network").

Le coût d'installation et de réalisation des divers équipements est modéré.

Dans un mode de réalisation les diverses phases de l'établissement d'une session sont fiabilisées de façon à
30 s'assurer que l'ensemble des configurations envoyées par le boîtier maître soit implanté dans les boîtiers destinataires et afin de s'assurer que le renouvellement des clés et les mises à jour soient réalisées dans l'ensemble des boîtiers clients prévus.

Pour la phase 1 (figure 6), au cours de laquelle les messages sont échangés selon un ordre prédéterminé, la fiabilité est assurée en imposant les contraintes suivantes : un seul message est envoyé à la fois ; l'ordre des messages est immuable et à chaque envoi est associé une durée de temporisation : si le message suivant n'est pas reçu avant l'expiration de cette durée, le message est transmis de nouveau.

La figure 6 est un schéma représentant un exemple d'échange de messages pour cette phase 1 entre un boîtier maître et un boîtier client. Sur cette figure, on a représenté six messages qui sont destinés à effectuer une authentification mutuelle du boîtier maître et du boîtier client et une mise en place d'un tunnel chiffré. Ces messages sont effectués, dans cet exemple, en faisant appel au protocole IKE et, de façon plus précise, au protocole ISAKMP contenu dans la norme RFC 2408. Les lignes 1 à 6 de la figure 6 utilisent le formalisme de ce protocole ISAKMP. Ainsi :

HDR est un en-tête générique suivi de données.
 SA est une association de sécurité.
 P est une proposition.
 T est une transformation.
 KE est un échange de clés.
 NONCE est une valeur aléatoire.
 HASH est une valeur de hachage.
 IDi est une identification.
 SEQ est un numéro de séquence.
 SIG est une signature numérique.
 HDR* signifie que l'ensemble des données du message est chiffré.

Au cours de la seconde phase, ou phase 2, représentée sur la figure 7, le serveur envoie à chaque boîtier client des messages de configuration en mode monodestination. Le nombre des messages de configuration varie suivant les sessions. Pour garantir la fiabilité de cette seconde phase, on prévoit une procédure d'acquiescement basée sur un numéro de séquence présent

dans un des champs du message, les messages non acquittés étant retransmis.

Dans cet exemple, les acquittements sont sélectifs : le récepteur précise les numéros de séquences de messages déjà
5 reçus. Ainsi le boîtier client envoie périodiquement un message d'acquittement mentionnant jusqu'à quel numéro de séquence il a reçu l'ensemble des messages. Par exemple, si le boîtier client a reçu correctement les numéros de séquences de 1 à 9 et de 11 à 15, il enverra un accusé de réception mentionnant cette
10 situation et le boîtier maître comprendra qu'il faut renvoyer le message correspondant au numéro de séquence 10 qui manque. Dans ces conditions, comme l'acquittement intervient alors que d'autres messages sont déjà parvenus au boîtier client, cet acquittement sélectif permet de limiter les renvois de messages
15 à ceux qui n'ont pas été reçus. Comme pour la première phase tout message qui n'est pas acquitté lorsque sa durée de temporisation arrive à expiration est retransmis.

Cette phase 2 constitue une phase de mise à niveau des boîtiers clients par rapport aux boîtiers déjà connectés et
20 fournit des instructions pour le chiffrement des paquets. Dans l'exemple représenté sur la figure 7, on fait également appel au protocole ISAKMP avec le même formalisme.

Cependant, on a indiqué dans les lignes 1, 2 et 6 une indication SA/P/T SatIPSec qui correspond à l'envoi de données
25 spécifiques à l'invention. Ainsi, aux lignes 1 et 2, la partie des données contient n_1 Param et n_2 Param qui signifient " n_1 paramètres" et " n_2 paramètres" et ces paramètres correspondent à ceux de blocs fonctionnels prévus dans chaque association de sécurité comme décrit plus loin.

30 À la ligne 6, on prévoit des paramètres de contrôle.

Le suffixe ack, par exemple SEQ_ack, signifie un accusé de réception de SEQ (numéro de séquence).

Au cours de la phase 2 bis (figure 8), le boîtier maître envoie des messages de configuration de type
35 multidestinations à plusieurs boîtiers clients. Pour fiabiliser

cette phase on prévoit un acquittement négatif avec retransmission, c'est-à-dire qu'un boîtier client n'ayant pas reçu un message demandera sa retransmission en envoyant un message de non acquittement. Dans ce cas aussi chaque message
5 comporte un numéro de séquence. Chaque boîtier client connaît le premier numéro de séquence que le boîtier maître utilisera et, de façon régulière, le boîtier maître envoie un message mentionnant le dernier numéro de séquence utilisé. Lorsqu'un boîtier client détermine qu'il n'a pas reçu un ou plusieurs
10 messages il déclenche une temporisation. A l'expiration de cette durée de temporisation le boîtier client envoie un message de non acquittement mentionnant les numéros de séquence manquants, ce qui déclenche la retransmission, en mode multide destinations, des messages correspondants.

15 Autrement dit, contrairement aux acquittements ou accusés de réception sélectifs, prévus au cours de la phase 2 de type mono-destination, au cours de cette phase 2bis de type multide destinations, les boîtiers clients n'envoient pas systématiquement d'accusé de réception. C'est seulement
20 lorsqu'il manque un numéro de séquence que le boîtier client envoie un accusé de réception négatif. Dans ces conditions, le trafic des boîtiers clients vers le boîtier maître est limité.

La durée de temporisation peut être différente d'un boîtier client à un autre afin d'éviter la congestion du boîtier
25 maître.

La figure 8 représente un exemple de messages envoyés par le boîtier maître en mode multide destinations et un message (ligne 5) envoyé par l'un des boîtiers clients vers le boîtier maître.

30 Sur cette figure, les indications portées à chaque ligne ont la même signification que sur les figures 6 et 7. Cependant, le suffixe Nack correspond à un accusé de réception de type négatif comme expliqué ci-dessus et HDR** signifie que le chiffrement de l'ensemble des données du message correspond à
35 une autre clé et/ou à un algorithme de chiffrement différent de

celle et/ou celui utilisé(e) pour la phase 1 ou la phase 2 (figure 6 et figure 7).

Selon un mode de réalisation on prévoit que le protocole de sécurisation offre des fonctions et des services
5 supplémentaires par rapport au protocole normalisé IPsec.

En effet dans le protocole connu IPsec une association de sécurité est utilisée seulement pour définir les paramètres qui serviront à sécuriser des paquets IPsec. Ainsi le protocole IPsec constitue un bloc fonctionnel unique permettant de
10 protéger des flux de données. Au cours de l'utilisation de ce bloc aucun paramètre ne peut être modifié, à l'exception des clés qui sont renouvelées régulièrement. Si l'utilisateur souhaite modifier une des caractéristique de l'association de sécurité celle-ci doit être renégociée.

15 Dans une réalisation du protocole selon l'invention des services supplémentaires sont définis dans chaque association de sécurité et constituent des blocs fonctionnels séparés, chaînés entre eux.

Ainsi alors que dans le protocole IPsec la
20 compression, le chiffrement et l'authentification forment un seul bloc fonctionnel, il est possible, conformément à l'invention, de séparer la compression du chiffrement IPsec.

Les blocs fonctionnels que l'on peut prévoir dans chaque association de sécurité sont compris par exemple dans le
25 groupe comportant : le protocole de chiffrement IPsec ESP (défini par la norme RFC 2406), le protocole d'authentification IPsec AH (défini par la norme RFC 2402), le chiffrement, l'authentification, le mode tunnel, un protocole TCP "spoofer" (modifications des paquets TCP qui évitent les limitations de
30 débit dues au temps de transmission par satellite), un protocole IGMP proxy (modifications des paquets IGMP, "Internet Group Management Protocol", pour une optimisation du trafic sur le lien satellite) et un protocole Drop (filtre basé sur une description de paquets, ne laissant passer que les paquets ayant
35 un gabarit autorisé).

Le chaînage des blocs fonctionnels permet une flexibilité du protocole. Ainsi au cours de l'utilisation d'une association de sécurité il est possible de modifier les paramètres de cette chaîne en supprimant un bloc, en ajoutant un
5 bloc ou en remplaçant un bloc par un autre.

REVENDICATIONS

1. Système de télécommunication comprenant une pluralité de terminaux (12, 14, 18) répartis selon des groupes tels qu'à l'intérieur de chaque groupe chaque terminal puisse émettre des messages multide destinations vers les autres membres du groupe, caractérisé en ce qu'à chaque terminal d'un groupe sont associés des moyens de chiffrement et déchiffrement (12₁, 14₁, 18₁) de façon que chacun de ces terminaux puisse émettre des messages multide destinations déchiffrables uniquement par les autres terminaux du groupe, et en ce que le système comporte un serveur central (16₁) pour distribuer à chacun des moyens de chiffrement et de déchiffrement des clés pour la transmission sécurisée des communications à l'intérieur de chaque groupe.

2. Système selon la revendication 1, caractérisé en ce que les messages transmis sont selon un protocole réseau.

3. Système selon la revendication 2, caractérisé en ce que le protocole réseau est choisi dans le groupe comprenant les protocoles IP, ATM, MPLS, Ethernet, PEP, PPPoE.

4. Système selon l'une des revendications précédentes, caractérisé en ce que les terminaux sont reliés à un réseau terrestre filaire et fournissent les messages déchiffrés à ce réseau filaire.

5. Système selon l'une des revendications précédentes, caractérisé en ce que les terminaux sont reliés les uns aux autres par un réseau à diffusion, par exemple de type hertzien, notamment par satellite, ou local, par exemple du type ethernet.

6. Système selon la revendication 5, caractérisé en ce que les terminaux sont aptes à fournir des messages chiffrés au réseau à diffusion ou au réseau local.

7. Système selon la revendication 5 ou 6, caractérisé en ce que le serveur central est relié aux terminaux par l'intermédiaire du réseau à diffusion.

8. Dispositif de chiffrement et de déchiffrement caractérisé en ce qu'il comporte une interface pour recevoir et émettre, à travers un premier réseau de télécommunication, des

messages chiffrés, une interface connectée à un second réseau pour recevoir de ce second réseau des messages à chiffrer à transmettre par le premier réseau et pour délivrer sur ce second réseau des messages déchiffrés et provenant du premier réseau, et une interface pour recevoir d'un serveur des clés de chiffrement et déchiffrement, les clés de chiffrement permettant de chiffrer un message multide destinations vers des destinataires sélectionnés faisant partie d'un même groupe qu'un terminal auquel le dispositif est associé.

9. Dispositif selon la revendication 8, caractérisé en ce que le premier réseau est du type hertzien ou filaire, notamment par satellite, et en ce que le second réseau est de type filaire.

10. Dispositif selon la revendication 8 ou 9, caractérisé en ce que le plan de contrôle et le plan de données du dispositif sont séparés.

11. Dispositif selon l'une des revendications 8 à 10 caractérisé en ce que les messages sont des paquets d'un protocole réseau.

12. Dispositif selon la revendication 11, caractérisé en ce qu'il comporte des moyens pour émettre des paquets IP sécurisés en mode tunnel.

13. Dispositif selon la revendication 12 caractérisé en ce qu'il comporte un moyen pour transmettre les paquets IP chiffrés avec un premier en-tête de routage et d'adresse et un second en-tête concernant les données de sécurité de ce paquet.

14. Dispositif selon la revendication 12 ou 13 caractérisé en ce qu'il comporte un moyen pour émettre et recevoir des seconds en-têtes avec des données de sécurité comprises dans le groupe comportant : des données d'identification permettant au(x) récepteur(s) de déterminer les fonctions et clés à utiliser pour rendre sa forme initiale à chaque paquet et vérifier son intégrité et son origine, des données relatives à la segmentation des paquets, des données de durée de vie de clés de session, et un numéro de paquet.

15. Dispositif selon l'une des revendications 8 à 14 caractérisé en ce que son interface pour la connexion au premier réseau est connectée directement à une interface d'un terminal de ce réseau.

5 16. Dispositif selon l'une des revendications 8 à 14 caractérisé en ce qu'il est réalisé sous la forme d'un logiciel intégré à la pile de logiciels réseau d'un terminal du premier réseau.

10 17. Serveur pour système de télécommunication permettant la transmission et la réception de messages multi-destinations, caractérisé en ce qu'il comprend des moyens pour transmettre à chacun des émetteurs et récepteurs de messages multi-destinations des éléments de sécurité pour permettre que
15 chacun des émetteurs puisse chiffrer les messages multi-destinations et chacun des récepteurs puisse déchiffrer les messages reçus afin que tous les destinataires faisant partie d'un groupe puissent recevoir simultanément les messages chiffrés reçus.

20 18. Serveur selon la revendication 17, caractérisé en ce que les messages sont des paquets selon un protocole réseau.

25 19. Serveur selon la revendication 17 ou 18, caractérisé en ce qu'il comporte des moyens de connexion à un réseau pour transmettre de façon confidentielle et sécurisée les éléments de sécurité à chacun des émetteurs et récepteurs de messages selon un mode mono et/ou multide destinations.

30 20. Serveur selon la revendication 19, caractérisé en ce que les éléments de sécurité à transmettre sont compris dans le groupe comportant : des fonctions et clés à utiliser pour protéger des paquets, c'est-à-dire pour chiffrer, déchiffrer et authentifier les paquets, ou pour modifier les paquets, des formats d'encapsulation des paquets, notamment IP, des données de filtrage définissant le groupe destinataire des paquets, et des données de durées de vie des éléments de sécurité.

21. Serveur selon la revendication 20, caractérisé en que les fonctions de sécurité et les modifications apportées aux paquets réseau sont séparées et forment des blocs chaînés.

22. Serveur selon la revendication 21, caractérisé en
5 ce qu'il comporte des moyens pour supprimer, ajouter ou remplacer au moins un bloc.

23. Serveur selon la revendication 21 ou 22, caractérisé en ce que les blocs chaînés sont compris dans le groupe incluant : le protocole IPSec ESP, le protocole IPSec AH,
10 le chiffrement, l'authentification, le mode tunnel, un protocole TCP spoofer, un protocole IGMP proxy et un protocole Drop.

24. Serveur selon l'une des revendications 17 à 23, caractérisé en ce que les moyens de transmission du serveur vers les émetteurs et récepteurs comportent des moyens pour, qu'au
15 cours d'une première phase, le serveur communique par des messages mono-destination avec les émetteurs et récepteurs afin de réaliser une authentification mutuelle et mettre en place un tunnel chiffré.

25. Serveur selon la revendication 24, caractérisé en
20 ce qu'il comporte des moyens pour, qu'au cours d'une seconde phase, il puisse envoyer à chaque émetteur et récepteur des messages de configuration en mode mono-destination.

26. Serveur selon la revendication 24 ou 25, caractérisé en ce qu'il comporte des moyens pour, qu'au cours
25 d'une autre phase, il puisse envoyer des messages de configuration de type multidestinations à plusieurs émetteurs et récepteurs.

27. Serveur selon l'une des revendications 17 à 26, caractérisé en ce qu'il comprend des moyens pour fiabiliser
30 l'envoi des éléments de sécurité vers chacun des émetteurs et récepteurs de messages multi-destinations ou monodestinations.

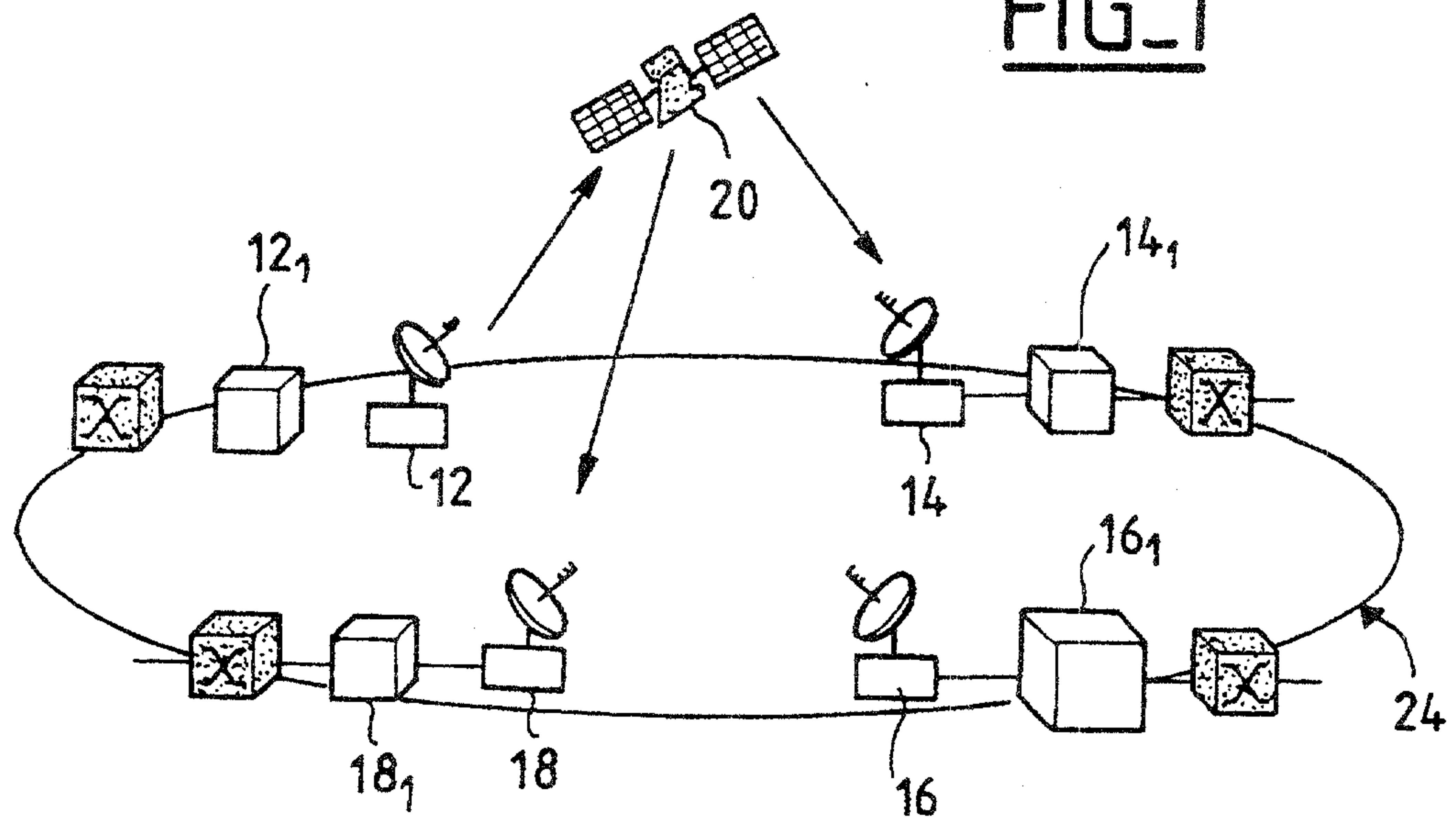
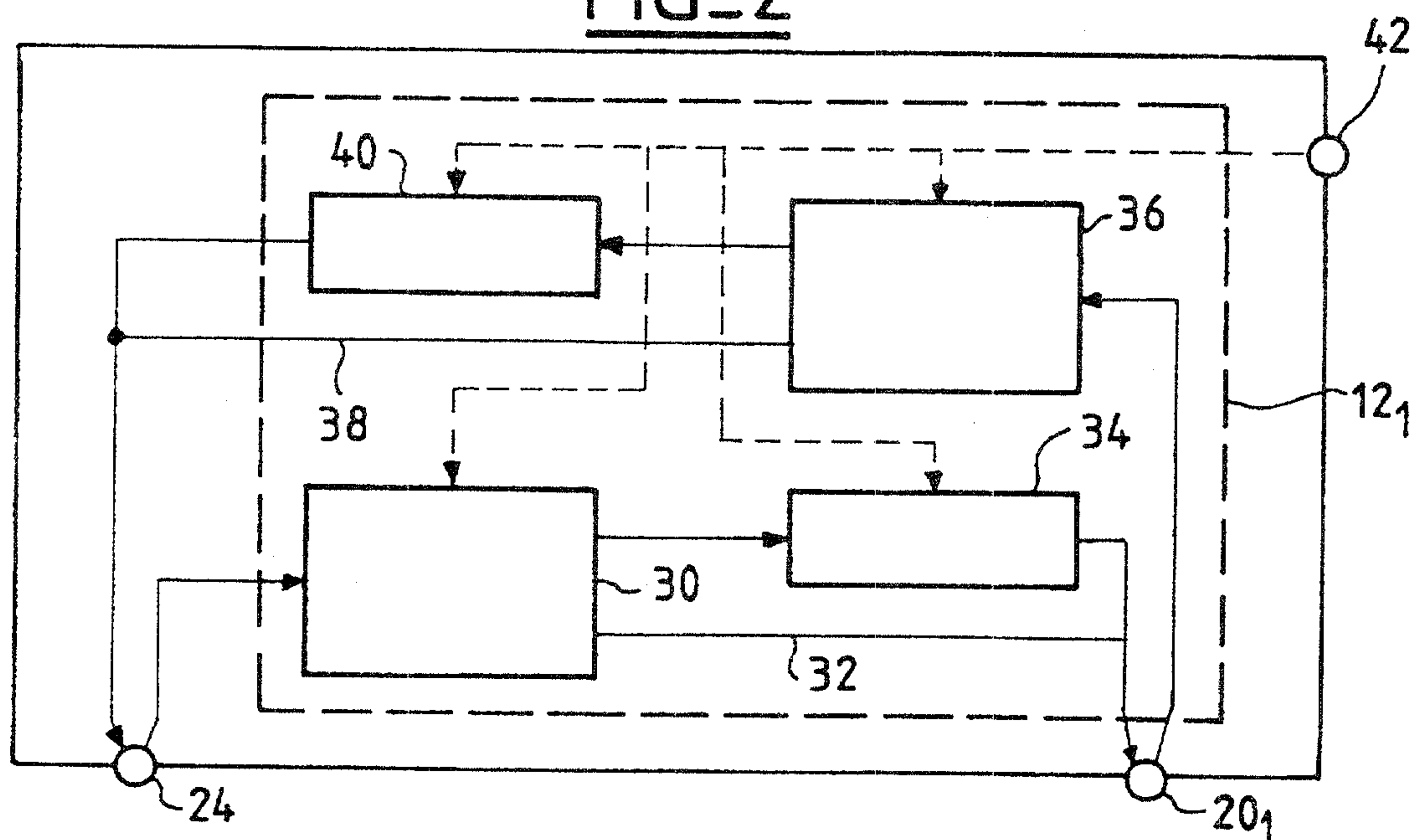
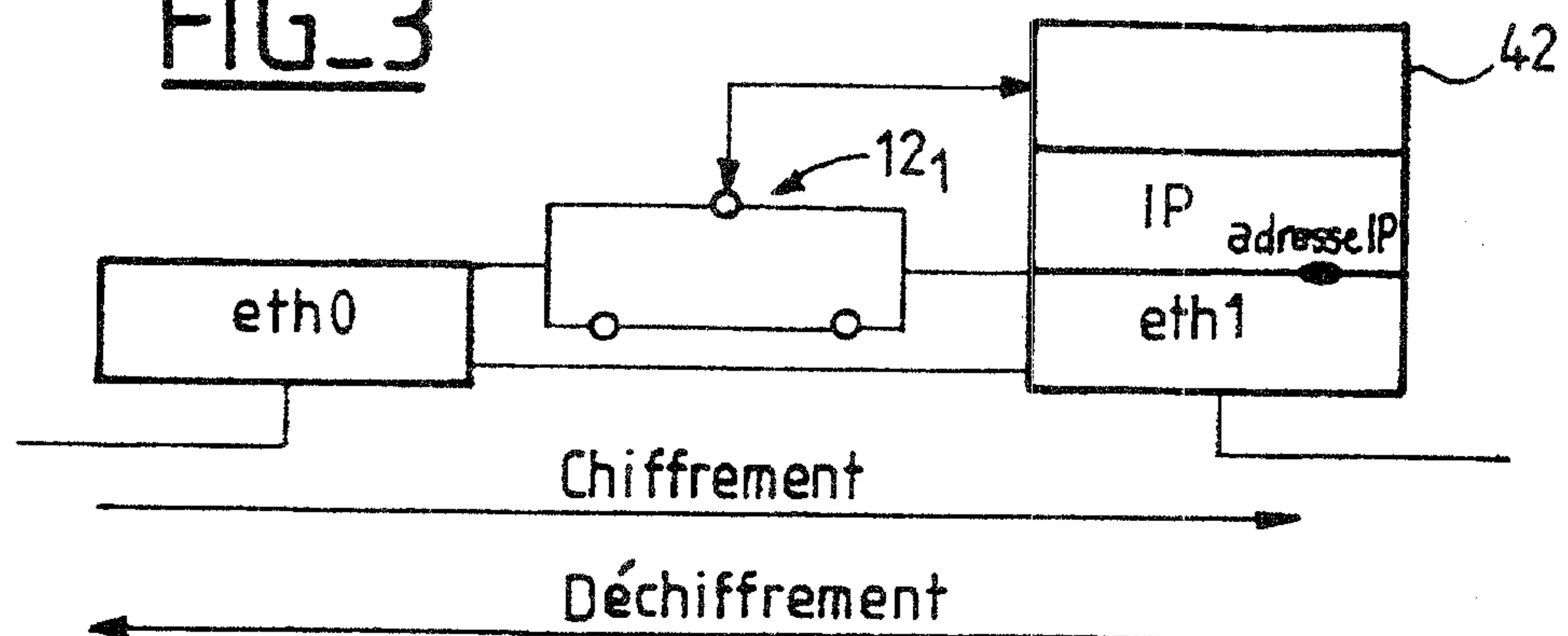
28. Serveur selon la revendication 27, caractérisé en ce que les moyens de fiabilisation comprennent un moyen pour retransmettre un message non acquitté par son destinataire après
35 un temps prédéterminé.

29. Serveur selon la revendication 28, caractérisé en ce que les éléments de sécurité étant envoyés vers chacun des émetteurs/récepteurs par un message multidestinations, à chaque émetteur/récepteur destinataire est associé une durée
5 prédéterminée d'acquiescement qui diffère d'un destinataire à un autre afin que le serveur ne reçoive pas simultanément plusieurs signaux de non acquiescement.

30. Serveur selon la revendication 27, 28 ou 29, caractérisé en ce que les moyens de fiabilisation comportent un
10 moyen pour associer à chaque message un numéro de séquence.

31. Serveur selon la revendication 30, caractérisé en ce que les moyens de fiabilisation comprennent un moyen pour recevoir des messages d'acquiescement comportant les numéros de séquence des messages émis correspondants et pour renvoyer les
15 messages correspondant aux numéros de séquence non acquiescés.

32. Serveur selon la revendication 30, caractérisé en ce que les moyens de fiabilisation comportent, pour les messages multidestinations, un moyen pour détecter des acquiescements négatifs provenant d'émetteurs/récepteurs indiquant que ces
20 derniers n'ont pas reçu de messages pour un numéro de séquence donné et des moyens pour retransmettre les messages correspondant aux acquiescements négatifs.

FIG_1FIG_2FIG_3

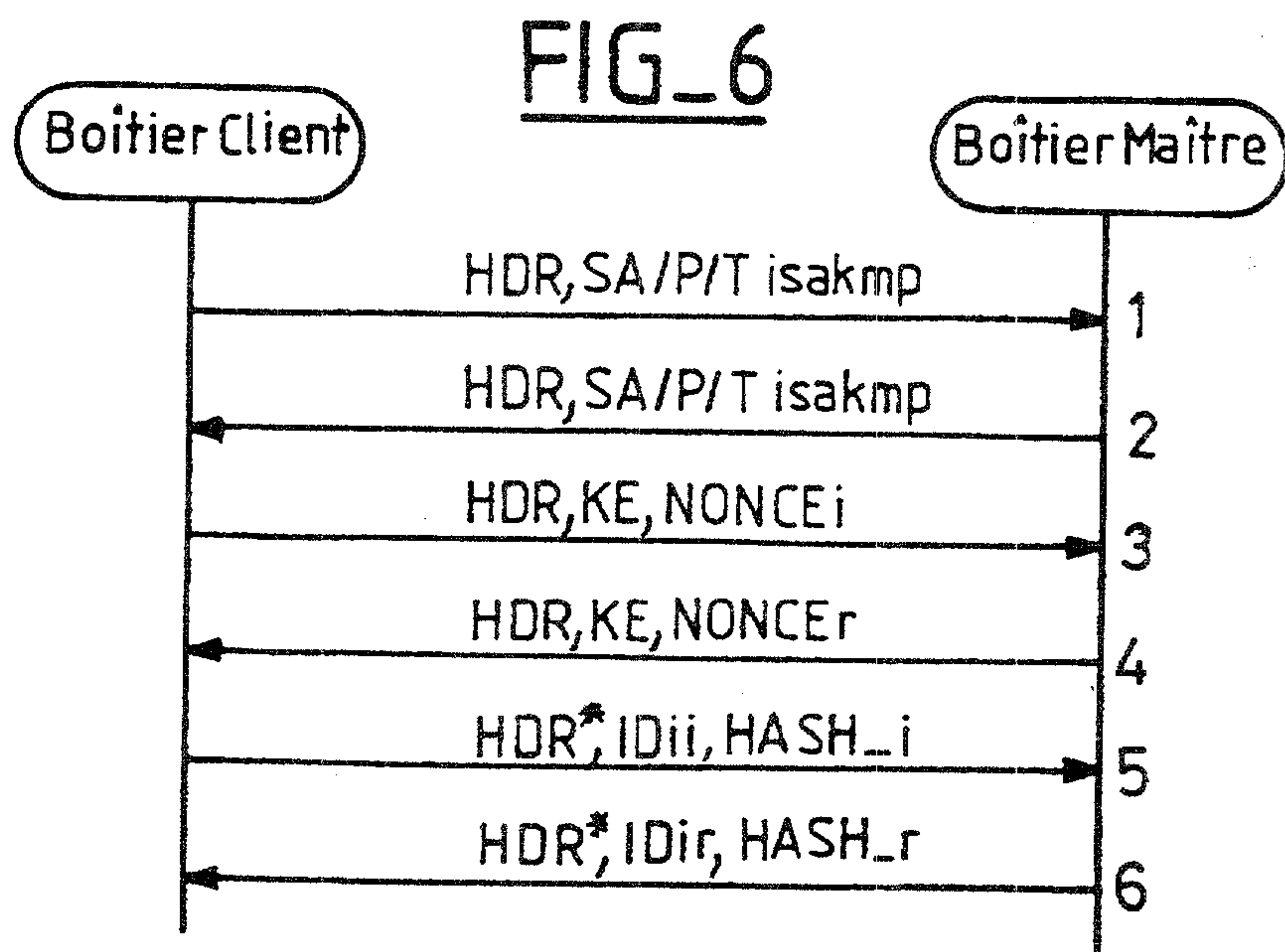
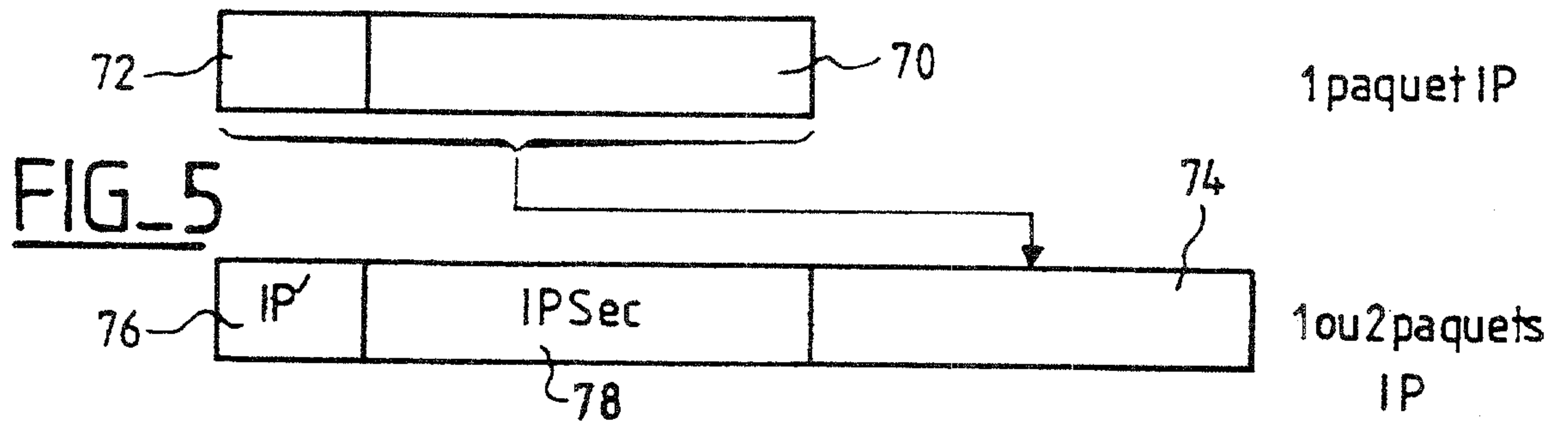
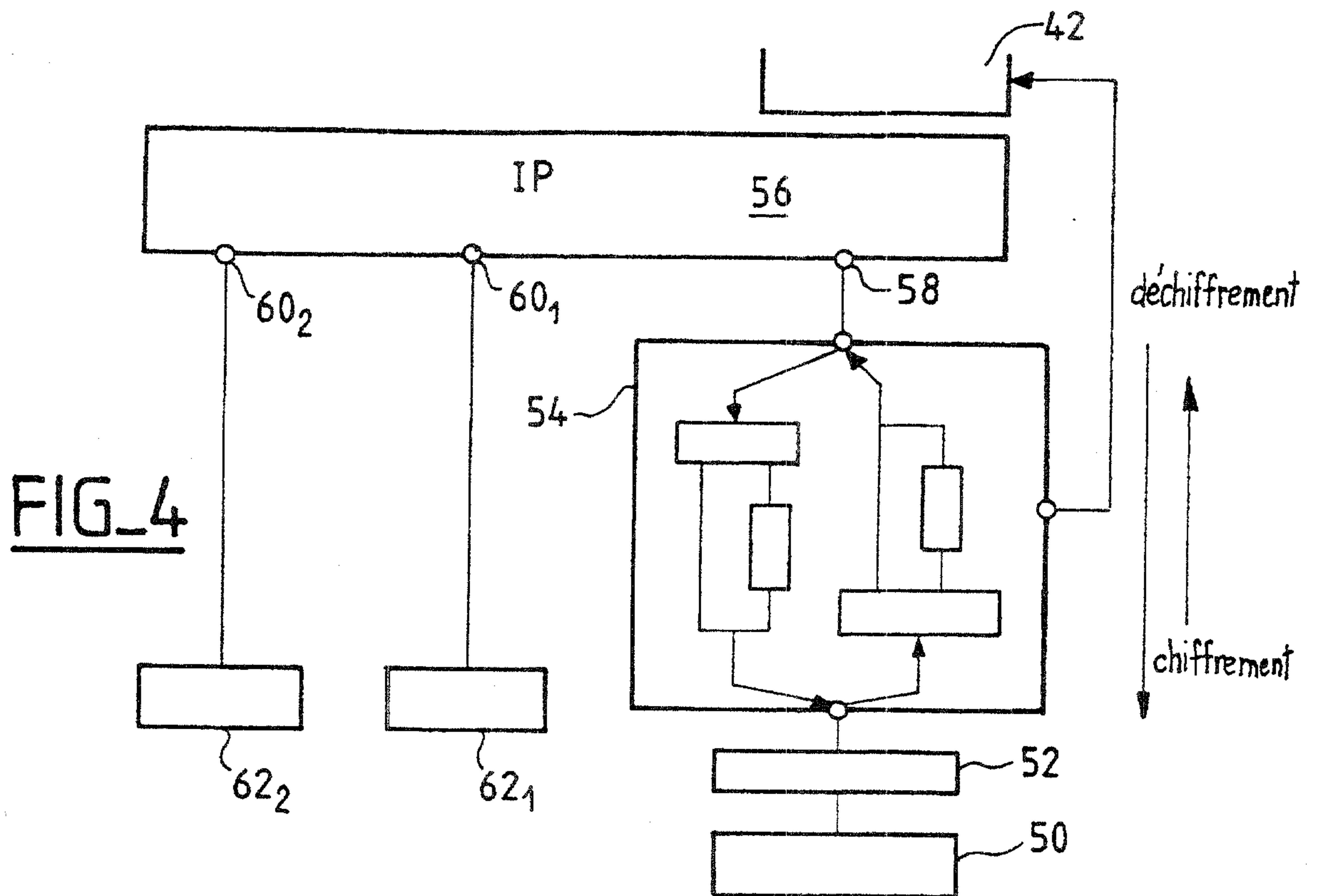
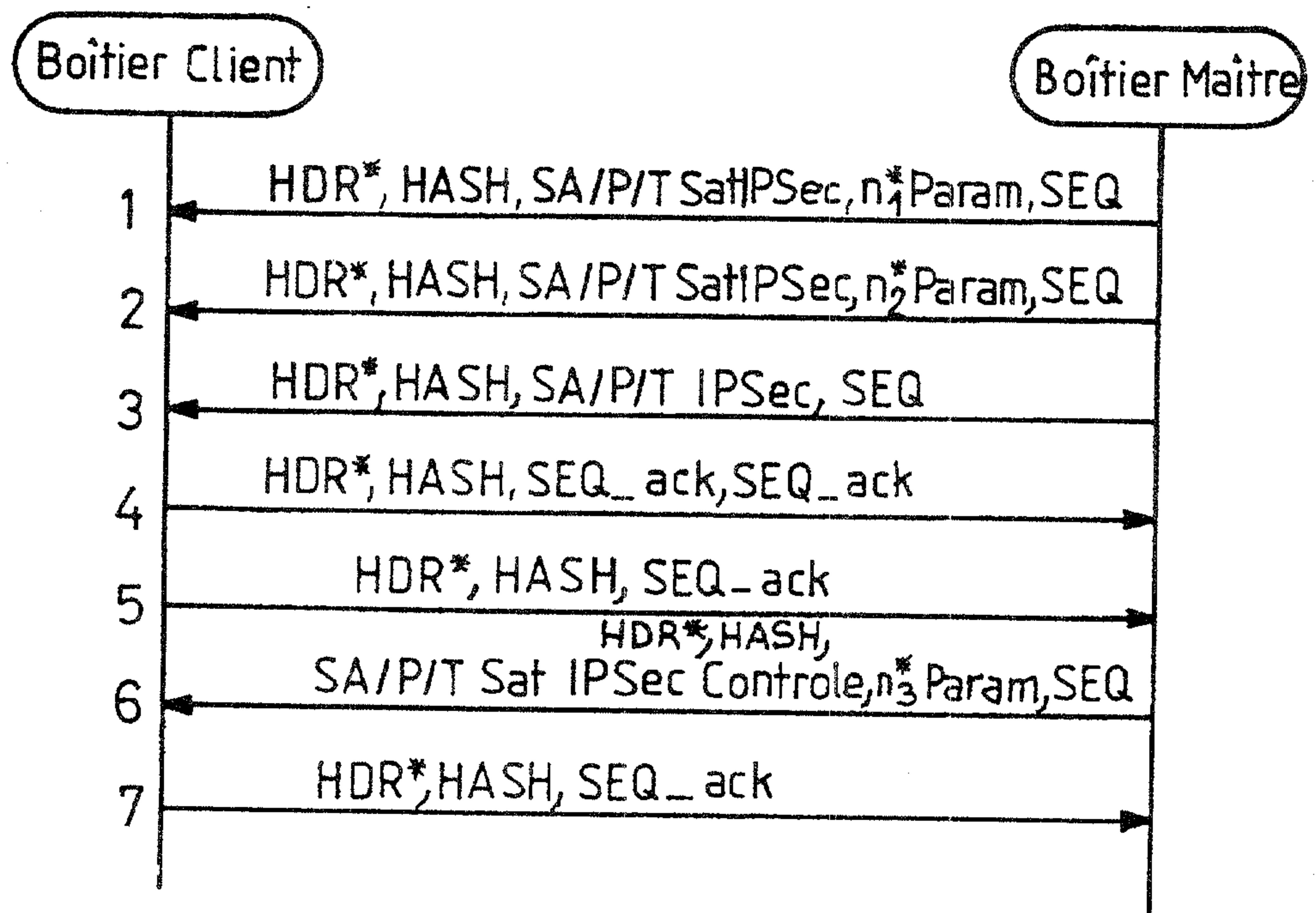


FIG_7FIG_8