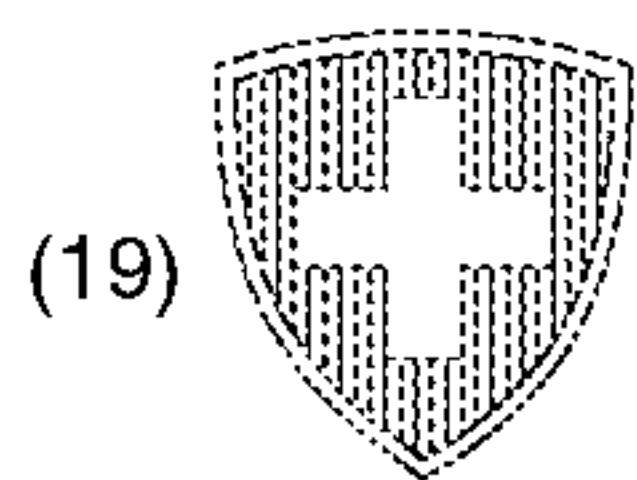




CONFÉDÉRATION SUISSE
INSTITUT FÉDÉRAL DE LA PROPRIÉTÉ INTELLECTUELLE

(11) **CH** **709 795 B1**

(51) Int. Cl.: **H04M** 1/667 (2006.01)
H04M 3/436 (2006.01)

Brevet d'invention délivré pour la Suisse et le Liechtenstein
Traité sur les brevets, du 22 décembre 1978, entre la Suisse et le Liechtenstein

(12) **FASCICULE DU BREVET**

(21) Numéro de la demande: 00925/14

(22) Date de dépôt: 18.06.2014

(43) Demande publiée: 31.12.2015

(24) Brevet délivré: 26.02.2021

(45) Fascicule du brevet publié: 26.02.2021

(73) Titulaire(s):
KATIA SA, c/o Maxime Winkler Avenue du Léman 14
1920 Martigny (CH)

(72) Inventeur(s):
Maxime Winkler, 1005 Lausanne (CH)

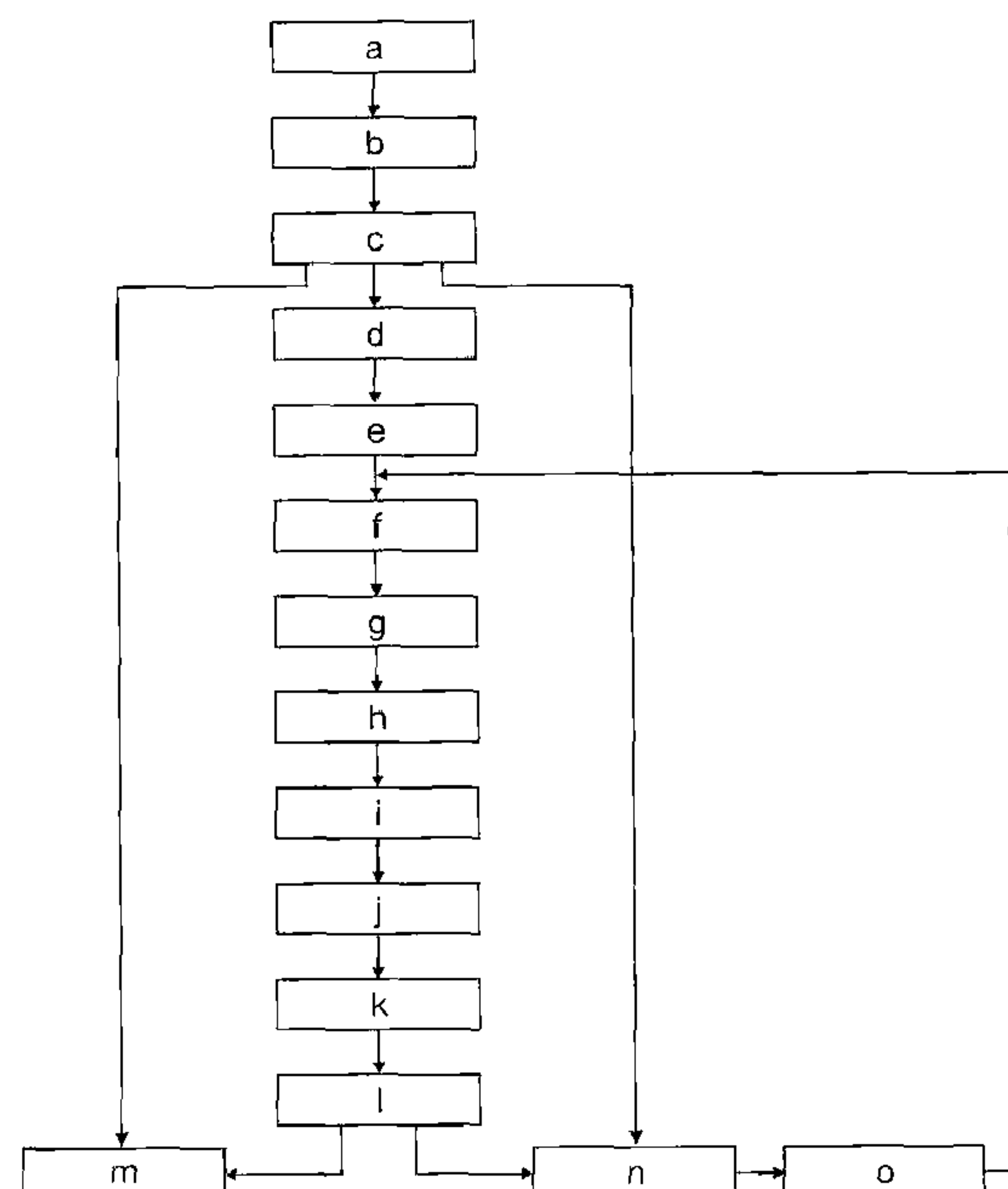
(74) Mandataire:
P&TS SA, Av. J.-J. Rousseau 4 P.O. Box 2848
2001 Neuchâtel (CH)

(54) **Procédé et système de filtrage d'appels téléphoniques entrants indésirables.**

(57) L'invention concerne un procédé de filtrage d'appels téléphoniques entrants indésirables, dans lequel une décision de bloquer un appel ou de le transmettre est basée à la fois sur le numéro d'appelant et sur une analyse de la voix de l'appelant. Le procédé comporte les étapes suivantes:

- (a) détermination du numéro d'appelant
- (b) en fonction du numéro d'appelant, un dispositif de filtrage décide soit de transmettre l'appel, soit de rejeter l'appel, soit d'inviter l'appelant à parler ;
- (c) lorsque l'appelant est invité à parler, il parle sans que son message vocal ne soit restitué à l'appelé ;
- (d) le système de filtrage analyse la voix de l'appelant, et
- (e) le système de filtrage décide en fonction de cette analyse si l'appel doit être transmis à l'appelé, ou s'il doit être bloqué.

L'invention concerne également un système de filtrage d'appels téléphoniques entrants indésirables adapté pour exécuter ledit procédé.



Description

Domaine technique

[0001] L'invention concerne un procédé et un système de filtrage d'appels téléphoniques entrants indésirables, notamment un procédé et un système pour détecter et prévenir les appels indésirables et criminels.

Etat de la technique

[0002] Les systèmes de communication téléphonique d'aujourd'hui permettent de perpétrer facilement des appels indésirables, souvent en toute impunité. Par exemple, de nombreux abonnés se plaignent de recevoir des appels provenant de campagnes de publicité ou de sondages d'opinions. Plus grave, certains appels peuvent même être criminels, par exemple en cas de harcèlement, d'arnaque téléphonique, d'escroquerie, ou d'appel pédophile par exemple.

[0003] De nombreuses solutions existent dans l'état de la technique pour bloquer des appels téléphoniques indésirables.

[0004] US2008292085A décrit un appareil qui permet de bloquer les appels téléphoniques provenant d'un numéro figurant sur une liste noire. L'appareil a la possibilité d'ajouter des numéros dans sa liste. Cet appareil ne fournit cependant aucune protection contre les appels indésirables provenant d'un numéro hors de la liste noire, par exemple les appels provenant d'une cabine, ou ceux dont le numéro d'appelant a été falsifié.

[0005] GB200614708A décrit un dispositif de filtrage d'appels entrants qui permet à l'utilisateur de programmer les numéros d'appelants autorisés et de bloquer les autres appels. Les utilisateurs qui ne figurent pas sur cette liste peuvent entrer un code NIP pour être autorisés à appeler. Ce dispositif offre une protection efficace, mais risque de créer un nombre important de „faux positifs“, c'est-à-dire d'appels bloqués à tort bien qu'ils ne soient pas indésirables. En outre, l'obligation d'introduire un code NIP est contraignant pour les appelants de bonne foi.

[0006] US2004131164 décrit un appareil qui permet de dévier vers un répondeur les appels lorsque l'identifiant d'appelant figure sur une liste.

[0007] US8472599 décrit un dispositif qui permet de rejeter automatiquement les appels entrants lorsque l'identificateur d'appel ne peut pas être déterminé.

[0008] US2002018546A décrit un dispositif de filtrage d'appel qui peut être programmé pour définir des règles différentes selon l'heure de la journée ou pour différents appelants.

[0009] US2004086101A décrit un système de filtrage d'appels téléphoniques adapté notamment à des fax.

[0010] EP0559047 décrit un appareil de filtrage d'appels téléphonique qui peut être employé avec un récepteur téléphonique.

[0011] US8548149 décrit un répondeur téléphonique capable de détecter les appels indésirables, en se basant notamment sur des motifs d'appels et sur des listes noires d'appelants indésirables.

[0012] W011014103 décrit un système de télécommunication capable de filtrer les appels au niveau d'un central téléphonique. Les appelants peuvent être identifiés au moyen d'un code d'identification.

[0013] JP2011010078 décrit un autre dispositif de filtrage d'appels indésirable qui se base sur des listes noires d'appelants indésirables.

[0014] US2010278325A décrit une méthode qui permet de prédire si un appel entrant va ennuyer l'appelé, et pour empêcher un tel appel. La prédiction se base sur les caractéristiques temporelles des appels précédents de l'appelant.

[0015] EP2153637 décrit une méthode pour détecter des campagnes d'appels téléphoniques indésirables, en analysant par exemple le nombre d'appels émis depuis chaque numéro. Cette méthode est difficile ou impossible à appliquer depuis un emplacement d'abonné.

[0016] WO07144310A1 décrit un système de gestion d'appels entrants qui emploie une liste noire, une liste blanche, et une liste grise d'appelants.

[0017] JP2007336001 décrit une méthode qui permet d'interrompre un appel indésirable en détériorant progressivement la qualité de l'appel.

[0018] W007134810 décrit un procédé permettant de déterminer la probabilité qu'un appel entrant soit indésirable, en se basant sur l'heure d'arrivée de l'appel.

[0019] W007118851 décrit une méthode impliquant la création d'une liste noire d'appelants ayant effectué au moins un appel indésirable.

[0020] US2009238345A décrit un système permettant de bloquer des appels indésirables avant même la première sonnerie.

[0021] US2009238345A décrit un dispositif qui permet d'ajouter un numéro de téléphone dans une liste noire ou dans une liste blanche.

[0022] US5930700 décrit un système de gestion de listes noires et blanches depuis un PDA.

[0023] La plupart de ces solutions connues se basent donc avant tout sur l'identification d'appelant, ou parfois sur d'autres paramètres comme l'heure d'appel. Aucun de ces critères n'offre cependant une sécurité suffisante.

[0024] En effet, à l'heure actuelle, une personne peut, sans autre, appeler une autre personne sans pour autant être autorisée, identifiée ou même authentifiée. Par exemple, la plupart des opérateurs permettent de masquer le numéro d'appelant. N'importe qui peut aussi utiliser une cabine téléphonique publique ou plus simplement effectué un appel par VoIP (ex : Skype) terminé sur le réseau afin de ne pas révéler son identité. Il est en outre possible de modifier simplement le numéro d'appelant ; de nombreux centraux téléphoniques privés offrent cette possibilité.

[0025] Par conséquent, les numéros téléphoniques qui s'affichent sont parfois fantaisistes, ou masqués, et n'aident pas vraiment les appelés à prendre la bonne décision avant de décrocher. Certains spammeurs téléphoniques utilisent même des numéros d'appelants correspondant à des organismes gouvernementaux dont les appels ne doivent en aucun cas, ou ne peuvent légalement, être bloqués.

Bref résumé de l'invention

[0026] Un but de la présente invention est de proposer un procédé et un dispositif qui permettent de résoudre ou en tout cas de réduire les problèmes décrits ci-dessus.

[0027] En particulier, un but de la présente invention est de contrôler les accès téléphoniques entrants pour filtrer efficacement les appels non désirés.

[0028] Un but de la présente invention est de proposer un procédé qui soit transparent pour les appelants habilités et habitués à communiquer avec un usager donné.

[0029] Selon l'invention, ces buts sont atteints notamment au moyen d'un procédé de filtrage d'appels téléphoniques entrants indésirables, dans lequel une décision de bloquer un appel ou de le transmettre est basée à la fois sur le numéro d'appelant et sur une analyse de la voix de l'appelant.

[0030] Ce procédé utilise donc au moins deux indicateurs, l'un sur le numéro d'appelant et l'autre qui modélise l'appelant lui-même grâce à une analyse de sa voix.

[0031] Dans un mode de réalisation, le procédé comporte les étapes suivantes :

a) détermination du numéro d'appelant;

b) en fonction du numéro d'appelant, un système de filtrage décide soit de transmettre l'appel, soit de rejeter l'appel, soit d'inviter l'appelant à parler ;

c) lorsque l'appelant est invité à parler, il parle sans que son message vocal ne soit restitué à l'appelé ;

d) le système de filtrage analyse la voix de l'appelant ;

e) le système de filtrage décide en fonction de cette analyse si l'appel doit être transmis à l'appelé, ou s'il doit être bloqué.

[0032] Ce procédé permet donc de bloquer immédiatement les appels entrants qui peuvent avec une certitude quasi absolue être qualifiés comme indésirables ; ce blocage peut même être effectué sans que la sonnerie du téléphone appelé ne sonne. A l'inverse, le procédé est transparent pour les appels dont on peut, notamment sur la base du numéro d'appelant, exclure qu'il s'agisse de spam téléphonique. Entre les deux, une procédure spéciale est mise en place pour les appels qui ne peuvent pas facilement être classifiés comme indésirables ou comme souhaitables ; dans cette zone grise, l'appelant est invité par le système à parler au système afin d'analyser sa voix et de déterminer, sur la base de cette voix, si l'appel doit être transmis ou non. Le message vocal de l'appelant n'est de préférence pas transmis à l'appelé durant cette phase de test ; il est même possible d'analyser automatiquement la voix de l'appelant avant que le téléphone de l'appelé ne sonne.

[0033] Ce procédé permet ainsi d'empêcher les appels de nature criminelle avant même que ceux-ci n'atteignent leurs victimes.

[0034] Le procédé peut comprendre une analyse sémantique de la conversation, la décision de transmettre un appel ou la décision de bloquer un appel dépendant de cette analyse sémantique.

[0035] Dans un mode de réalisation, un score décrit la confiance que le système attribue à un identifiant d'appel tandis qu'une deuxième mesure vérifie que c'est bien la bonne personne qui est en ligne en vérifiant l'empreinte biométrique, par exemple l'empreinte vocale, l'empreinte faciale, l'empreinte multimodale (voix plus visage), et éventuellement l'empreinte sémantique de l'appelant.

[0036] L'analyse du numéro d'appelant peut par exemple employer des listes noires, des listes blanches et/ou des listes grises d'appelant. Ces listes peuvent propres à chaque appelés : un appelant donné sera en effet peut-être indésirable pour certains appelés mais pas pour d'autres. D'autres listes noires, blanches et/ou grises peuvent aussi être partagées entre plusieurs appelés, par exemple en les stockant de manière centralisée dans un serveur partagé.

[0037] Des mécanismes de synchronisation peuvent être mis en place pour synchroniser les listes partagées avec les listes individuelles. Dans un mode de réalisation, un appelant est mis sur une liste noire, respectivement blanche ou grise, partagée dès qu'un nombre et/ou un pourcentage donné d'appelés l'ont classé ainsi.

[0038] L'analyse du numéro d'appelant peut aussi se baser sur la plausibilité du numéro d'appelant, afin par exemple de bloquer les numéros d'appelants inexistantes ou dont le format (par exemple le nombre de chiffres, l'indicatif, etc.) ne correspond pas à une structure de numéro existante.

[0039] L'analyse du numéro d'appelant peut aussi se baser sur l'origine géographique associée à l'indicatif du numéro d'appelant transmis ; pour un appelé donné, les appels provenant de l'étranger, ou d'une région ou pays autre que ceux avec lesquels il a l'habitude de communiquer, peuvent être bloqués ou générer une invitation à parler avant que l'appel ne soit transmis.

[0040] L'analyse vocale de la voix des appelants permet par exemple d'identifier la personne en ligne et de la reconnaître sur la base de son empreinte vocale. Ainsi, un spammeur téléphonique connu (par exemple un employé d'un call center) peut être reconnu sur la base de son empreinte vocale même s'il emploie différents numéros d'appelants. Les empreintes vocales des appelants indésirables peuvent être partagées entre plusieurs appelés.

[0041] L'analyse vocale permet aussi d'authentifier l'appelant et de vérifier qu'il correspond au numéro d'appelant transmis, lorsque la ou les empreintes associées à ce numéro d'appelant sont connus, par exemple sur la base d'appels précédents.

[0042] L'analyse vocale permet aussi de classer l'appelant dans un groupe parmi plusieurs groupes, par exemple dans un groupe „bloqué“, „admis“, etc.

[0043] Un algorithme de reconnaissance de parole et une analyse sémantique peuvent être mis en oeuvre pour classer les appelés et pour rejeter des appels indésirables ou accepter des appels souhaitables. Par exemple, certains termes ou expressions fréquemment employés par des importuns, ou par un appelant spécifique, peuvent contribuer à déclencher une décision de blocage ou d'acceptation.

[0044] L'algorithme de reconnaissance de parole peut aussi comparer les paroles de l'appelant avec des données endogènes (par exemple des contenus de dialogues précédents avec cet appelant connus du système) ou exogènes (par exemple des données sur un réseau social de l'appelant ou de l'appelé). Cette comparaison peut être utilisée pour classer l'appelant et/ou pour l'authentifier.

[0045] Le système de filtrage peut continuer d'analyser la voix de l'appelant après que l'appel ait été transmis à l'appelé. Cette analyse permet par exemple de préciser la signature vocale des appelants autorisés dont l'appel a été transmis, afin de mieux les reconnaître dans le futur. Il est aussi possible de bloquer l'appel ou de proposer de le bloquer lorsque cette analyse révèle, après l'établissement de l'appel avec l'appelé, qu'il est indésirable, par exemple s'il provient d'un importun reconnu tardivement dans la discussion, ou lorsque l'analyse sémantique de ses paroles révèle un contenu inacceptable.

[0046] Un score de confiance peut être attribué à l'appel en fonction du numéro d'appelant, la décision de rejeter l'appel ou d'inviter l'appelant à parler étant prise au cours de l'étape b lorsque ce score est en-dessous d'un seuil prédéterminé.

[0047] Ce score de confiance attribué à un appelant est déterminé indépendamment pour chaque appelé. Un numéro d'appelant très connu d'un appelé donné, et ayant souvent téléphoné avec lui, générera par exemple un score de confiance plus élevé qu'un numéro d'appelant inédit pour cet appelé. Ce score de confiance individuel peut aussi dépendre des listes blanches, noires ou grises individuelles propres à chaque appelé ainsi que des listes partagées.

[0048] Un deuxième score de confiance peut aussi être attribué à l'appel en fonction de l'analyse biométrique, par exemple vocale, faciale, vocale plus faciale, et/ou sémantique. Ce deuxième score de confiance peut être combiné au premier score de confiance.

[0049] Le score de confiance, et la décision de rejeter l'appel ou d'inviter l'appelant à parler peut dépendre de l'historique des appels effectués avec ledit numéro d'appelant vers d'autres appelés. Par exemple, un numéro d'appelant notoirement associé à des appels importuns peut être mentionné dans des listes noires de numéros qui peuvent être partagées, ou à l'inverse un numéro d'agence gouvernementale peut figurer sur des listes blanches partagées. Par ailleurs, un numéro d'appelant associé à un très grand nombre d'appels provient peut-être d'un call center, auquel un score de confiance plus bas sera probablement attribué.

[0050] Le procédé peut comprendre une étape d'identification de l'appelant grâce à l'analyse biométrique, le score de confiance dépendant de l'historique des appels effectués par l'appelant ainsi identifié vers d'autres appelés. Par exemple, un appelant notoirement associé à des appels importuns peut être mentionné dans des listes noires d'appelant qui peuvent être partagées. Par ailleurs, un appelant associé à un très grand nombre d'appels travaille peut-être dans un call center, auquel un score de confiance plus bas sera probablement attribué.

[0051] L'appelé peut de préférence signaler un appel indésirable, par exemple au moyen d'un bouton sur un appareil, d'une commande vocale ou via un site web. Cette indication peut par exemple être effectuée pendant l'appel, ou après cet appel. Le numéro d'appelant peut ensuite être mis dans une liste noire de l'appelé, ou associé à un score de confiance plus bas qu'à l'origine. De la même façon, l'empreinte biométrique, par exemple vocale et/ou faciale, de l'appelant peut être mise dans une liste noire de l'appelé, ou associée à un score de confiance plus bas qu'à l'origine. Cette décision peut aussi être utilisée dans la décision de rejeter les futurs appels de l'appelant vers d'autres appelés, ou d'inviter cet appelant à parler.

[0052] Le procédé peut employer une modélisation des appelants autorisés, et une autre modélisation des appelants non autorisés. Cette modélisation peut se baser à la fois sur le numéro d'appelant et sur l'analyse biométrique de l'appelant. Elle peut être individuelle pour chaque appelé. Par exemple, un modèle d'appelant autorisé pour un appelé donné peut contenir les appelants habituels de cet appelé, alors qu'un modèle d'appelant non autorisé peut contenir les appelants sur une liste noire ainsi que ceux dont le numéro d'appelant ou l'analyse vocale trahissent un appel depuis un call center à l'étranger. La modélisation des appelants peut aussi être collective et identique pour tous les appelés.

[0053] La décision d'accepter un appel puis de le transmettre peut être prise lorsque les paramètres de cet appel se rapprochent suffisamment du modèle d'appelant autorisé. La décision de bloquer un appel sera prise lorsque les paramètres de cet appel se rapprochent suffisamment du modèle d'appelant non autorisé.

[0054] Un algorithme de type machine learning peut être mise en place pour classer les appels entrants dans la catégorie des appels autorisés ou non autorisés.

Brève description des figures

[0055] Des exemples de mise en oeuvre de l'invention sont indiqués dans la description illustrée par les figures annexées dans lesquelles :

- La figure 1 illustre un réseau de télécommunications incluant un système de filtrage selon un premier mode de réalisation de l'invention.
- La figure 2 illustre un réseau de télécommunications incluant un système de filtrage selon un deuxième mode de réalisation de l'invention.
- La figure 3 illustre un réseau de télécommunications incluant un système de filtrage selon un troisième mode de réalisation de l'invention.
- La figure 4 illustre un réseau de télécommunications incluant un système de filtrage selon un quatrième mode de réalisation de l'invention.
- La figure 5 est un diagramme de flux illustrant un exemple de procédé selon l'invention.

Exemple(s) de mode de réalisation de l'invention

[0056] Les figures 1 à 4 illustrent quatre variantes de système de filtrage dans un réseau de télécommunications.

[0057] Dans l'exemple de la figure 1, le réseau de télécommunications comporte un réseau téléphonique 4, par exemple un réseau analogique (POTS), ISDN, cellulaire, de type VoIP, et/ou une combinaison entre plusieurs de ces réseaux. La référence 3 correspond à un dispositif terminal d'un appelant désirant établir un appel téléphonique avec un dispositif terminal d'un appelé 2 au travers de ce réseau téléphonique 4. Le système de filtrage 1, 5 inclut dans ce cas un module 1 sous la forme d'un boîtier branché entre le dispositif terminal d'appelé 2 et le réseau téléphonique 4, par exemple sur la prise téléphonique du terminal. Les fonctionnalités du module 1 peuvent aussi être réalisées par logiciel. Dans un mode de réalisation, ce module est intégré au dispositif terminal d'appelé 2, par exemple sous la forme de firmware ou d'une application, par exemple d'une application exécutée par-dessus un système d'exploitation dans le cas d'un dispositif terminal sous la forme d'un téléphone cellulaire, d'une tablette ou d'un ordinateur notamment. Le module 1 peut contenir un processeur ainsi qu'une base de données personnelle de numéros d'appelants, une base de données personnelle d'appelants et une base de données personnelle d'empreintes biométriques des appelants, par exemple d'empreintes vocales et/ou faciales. Les bases de données de numéros d'appelants et d'appelants indiquent par exemple quels numéros et quels appelants figurent sur des listes noires, blanches ou grises.

[0058] Le système de filtrage 1, 5 inclut en outre un serveur 5 accessible depuis le réseau téléphonique 4 et contenant un processeur ainsi qu'une base de données partagée de numéros d'appelants 50, une base de données partagée d'appelants 51 et une base de données partagée d'empreintes biométriques 52 des appelants, par exemple d'empreintes vocales et/ou faciales. Les bases de données de numéros d'appelants et d'appelants indiquent par exemple quels numéros et quels appelants figurent sur des listes noires, blanches ou grises.

[0059] Le serveur 5 peut aussi contenir des historiques d'appels passés par différents appelants et/ou à différents appelés, des signatures vocales et/ou biométriques et/ou sémantiques d'appelants, etc.

[0060] Le serveur 5 peut aussi être réalisé sous la forme d'un serveur virtuel ou d'un groupe de serveurs interconnectés, par exemple dans le cloud. D'autres organisations peuvent être imaginées.

[0061] Le boîtier de filtrage 1 peut se connecter à ce serveur 5 par exemple au moyen d'un modem intégré 10 permettant d'établir une communication de données avec ce serveur, par exemple pendant un intervalle sans dialogue ou dans une bande de fréquence non utilisée pour la communication vocale.

[0062] La configuration de la figure 1 offre un confort d'installation maximal et évite aux appelé la tâche de devoir configurer une connexion internet; elle est aussi appropriée lorsqu'il n'y a pas de connexion internet disponible. Typiquement, tous les téléphones fixes et mobiles peuvent ainsi être utilisés par l'invention. Dans ce cas une partie seulement de l'information est communiquée par la ligne téléphonique ou par la connexion voix du téléphone mobile ; typiquement la voix de l'auteur présumé d'un appel abusif. La grande partie du traitement de la modélisation des locuteurs est effectuée sur le dispositif 1 lui-même. La modélisation spam elle aussi s'effectue directement sur le dispositif 1.

[0063] Dans l'exemple de la figure 2, le boîtier 1 est connecté au serveur 5 au travers du réseau Internet IP, par exemple au travers d'une interface Internet du boîtier 1. Les autres éléments peuvent être identiques aux éléments correspondants de la figure 1. La connexion IP élargit les possibilités d'utilisation et améliore l'ergonomie d'utilisation. Il est par exemple possible de configurer le système de filtrage via un serveur Web, de stocker des paramètres dans le serveur 5 (ou dans un cloud), et de partager des informations avec d'autres utilisateurs.

[0064] Dans l'exemple de la figure 3, le système de filtrage 5 est entièrement intégré dans le réseau téléphonique 40, par exemple sous la forme d'un module software et/ou hardware 5 qui peut être connecté à un noeud 40 du réseau, par exemple un noeud SSF d'un réseau intelligent. Les autres éléments peuvent être identiques aux éléments correspondants de la figure 1.

[0065] Dans ce mode de réalisation, le service peut aussi être réalisé par déviation des appels au niveau du réseau téléphonique classique ou par déviation des appels vers un autre réseau de type VoIP. L'utilisateur n'a plus besoin d'installer un boîtier chez lui et l'interaction s'effectue par un accès web ou par avec une application logicielle sur le smartphone. Le service peut être géré par des opérateurs téléphoniques ou des opérateurs de service voix, réseaux sociaux, etc.

[0066] Dans l'exemple de la figure 4, le dispositif terminal 2 de l'appelé est connecté au serveur 5 via une liaison de type Internet, afin de permettre à l'appelé par exemple de signaler des appels indésirables. Les autres éléments peuvent être identiques aux éléments correspondants de la figure 1 ou de la figure 3.

[0067] Nous allons maintenant décrire en relation avec la figure 5 un exemple de procédé mis en oeuvre par le système de filtrage 1,5 selon l'invention.

[0068] Au cours de l'étape a, un appel téléphonique provenant du réseau téléphonique 4 est reçu, et le numéro d'appelant (CLI - Caller Line Identity) est déterminé, par exemple dans le dispositif (ou application) 1 s'il est présent, ou dans le serveur 5 dans les modes de réalisation des figures 3 et 4. L'appel est intercepté et n'est pas immédiatement transmis au dispositif terminal 2, qui ne sonne donc pas encore.

[0069] Au cours de l'étape b, le numéro d'appelant ainsi déterminé est analysé. Cette analyse peut par exemple comporter une comparaison avec une liste de numéro d'appelant dans une liste noire de numéros d'appelants indésirables, et/ou une comparaison avec une liste de numéro d'appelant dans une liste blanche de numéros d'appelants.

[0070] La comparaison peut être effectuée avec des listes blanches et/ou noires individuelles à l'appelé, qui peuvent par exemple être stockées localement dans son dispositif 1 ou dans un espace mémoire dédié du serveur 5 ; ces listes locales contiennent par exemple des numéros qui sont indésirables (respectivement acceptables) pour un appelé donné mais qui ne le sont pas nécessairement pour un autre appelé. En addition, ou alternativement, la comparaison peut être effectuée avec des listes blanches et/ou noires qui peuvent être stockées de manière centralisée dans le serveur 5 et qui contiennent des numéros d'appelants indésirables (respectivement acceptables) pour tous ou la plupart des appelés. Des mécanismes de synchronisation peuvent être mis en place pour synchroniser les listes locales et les listes centralisées ; par exemple, un numéro d'appelant marqué comme indésirable dans un nombre supérieur à un seuil prédéterminé de dispositifs 1, ou dans un pourcentage prédéterminé de dispositifs 1, pourra être incorporé automatiquement dans une liste centralisée dans le serveur 5.

[0071] L'analyse de numéro d'appelant effectuée au cours de l'étape b peut aussi inclure une analyse de plausibilité du numéro d'appelant, par exemple afin d'exclure des numéros dont le format, le nombre de chiffres ou l'indicatif ne correspond pas un numéro possible, ou correspond à un numéro dans une tranche de numéros interdits.

[0072] L'analyse de numéro d'appelant effectuée au cours de l'étape b peut inclure une vérification de l'historique des appels passés depuis ce numéro, tel que stocké dans le serveur 5 ; ainsi un numéro d'appelant associés à des appels fréquents durant un intervalle bref aura une probabilité plus d'élévée d'être classé comme indésirable qu'un numéro d'appelant utilisé de façon plus conventionnelle.

[0073] L'analyse de numéro d'appelant effectuée au cours de l'étape b peut inclure une vérification d'un profil associé à ce numéro d'appelant, par exemple un profil disponible à partir de ce numéro dans un annuaire téléphonique, sur le Web, dans un réseau social comme Facebook, Twitter, LinkedIn etc, dans un site de chat, etc et permettant de classer ce numéro d'appelant. Par exemple, un numéro d'appelant associé à une société, ou un type de société, connu pour

son harcèlement téléphonique, sera associé à une probabilité élevée d'être indésirable. Un appelé particulier peut aussi décider de bloquer par exemple tous les appels entrants dont le numéro est associé dans un annuaire ou sur le Web à des compagnies d'assurances.

[0074] L'analyse de numéro d'appelant peut aussi recourir à une entité de certification externe et spécialisée, par exemple une PKI („public-key infrastructure“) capable de certifier certains numéros d'appelants

[0075] Au cours de l'étape c (optionnelle), un score est attribué à l'appel en fonction des résultats de l'analyse de numéro d'appelant effectuée au cours de l'étape b. Ce score est lié à la probabilité que l'appel soit indésirable pour l'appelé 2 donné.

[0076] Si le score est inférieur à un premier seuil donné, l'appel entrant est bloqué (étape m) ; en option, un message vocal préenregistré ou généré synthétiquement peut être restitué à l'appelant 3 pour lui indiquer que l'appel est refusé. Si en revanche ce score est supérieur à un deuxième seuil donné (supérieur au premier seuil), l'appel est transmis au dispositif 2 (étape n) qui se met à sonner (ou à vibrer), afin que l'appelé puisse répondre. Ces appels sûrs sont donc établis de manière entièrement transparente pour l'appelant et pour l'appelé.

[0077] Dans le cas où le score est entre le premier seuil et le deuxième seuil, une procédure particulière est mise en place, et illustrée par les étapes d à l sur la figure. Ces étapes sont donc effectuées lorsque l'analyse du numéro d'appelant ne permet pas à elle seule de classer l'appel comme appel désirable ou comme appel à accepter sans condition, par exemple en cas de numéro d'appel inconnu ou pour lequel aucune information n'est disponible.

[0078] Les niveaux de seuils 1 et 2 peuvent en option être ajustés par l'utilisateur afin d'ajuster le taux de faux positifs et de faux négatifs.

[0079] Au cours de l'étape d, l'appelant est invité à parler, par exemple au moyen d'une invite vocale synthétisée par le dispositif 1 respectivement par le serveur 5. L'appelant peut par exemple être invité à indiquer son nom et le nom de la personne souhaitée. L'invitation peut être restituée de manière à ce que l'appelant ne puisse que difficilement se rendre compte qu'il parle à une machine de dialogue vocal.

[0080] Au cours de l'étape e, l'appelant répond au système de filtrage 1, 5, par exemple en indiquant son nom et la personne désirée.

[0081] Au cours de l'étape f, la voix de l'appelant est analysée par le système de filtrage 1 respectivement 5. Le but de cette analyse est de classer l'appelant comme personne indésirable ou non.

[0082] En cas de communication multimodale, par exemple de communication incluant l'image en plus de la voix, il est possible en option d'analyser également l'image de l'appelant, et d'effectuer une analyse faciale. D'autres paramètres biométriques peuvent être employés en sus de la voix, y compris par exemple les empreintes digitales si disponibles.

[0083] Au cours de l'étape g (optionnelle), une analyse sémantique de la voix de l'appelant est effectuée, par exemple sur la base d'une conversion voix en texte des mots dits par l'appelant. L'empreinte sémantique dépend de l'ensemble des couches du langage : le discours, la pragmatique, la sémantique, la syntaxe, le niveau lexical.

[0084] Au cours de l'étape h (optionnelle), l'appelant est modélisé sur la base de sa voix et de cette analyse sémantique. Cette étape permet d'une part de créer une signature vocale de l'appelant, afin de le reconnaître lors d'appels ultérieurs, et d'autre part de le comparer à des modèles préexistants d'utilisateurs indésirables et d'utilisateurs acceptables. Cette modélisation peut par exemple inclure une détection de la langue parlée par l'appelant ; il est ainsi possible d'associer un score dépendant de cette langue. Le modèle peut aussi indiquer des caractéristiques émotionnelles de l'appelant (par exemple un état de stress, un ton agressif, un langage commercial, etc.). Le modèle peut encore inclure une détermination de l'âge approximatif de l'appelant, et de son sexe. L'ensemble de ces paramètres du modèle peuvent être utilisés pour calculer plus tard, au cours de l'étape k, un score attribué à l'appelant et lié à la probabilité que cet appelant soit indésirable.

[0085] Au cours de l'étape i, l'appelant est identifié sur la base de l'analyse vocale. L'identification peut utiliser des algorithmes de reconnaissance de locuteur („speaker recognition“) et/ou des algorithmes de reconnaissance vocale pour identifier l'appelant sur la base de ses paroles.

[0086] L'identification correspond à une détermination de l'identité de l'appelant, par exemple sous la forme d'un identifiant unique telle qu'un nom, un numéro, etc. L'identification peut exploiter le numéro d'appelant préalablement déterminée au cours de l'étape a ; toutefois, plusieurs appelants peuvent partager un même numéro d'appelant, et un appelant peut employer différents numéros d'appelants à différentes occasions. Cette identification d'appelant permet donc par exemple de distinguer entre les différents membres d'une famille ou d'une entreprise employant la même ligne téléphonique et le même numéro d'appelant.

[0087] Alternativement, ou en addition, l'étape i peut aussi inclure une authentification (ou vérification) de l'appelant afin de vérifier s'il correspond bien au numéro d'appelant indiqué, à l'identité prétendue dans sa réponse vocale, et/ou à un groupe d'appelant prétendu. Par exemple, l'authentification peut consister à vérifier si la signature vocale et/ou faciale de l'appelant appartient au groupe d'utilisateurs qui partagent un numéro d'appelant ou un groupe de numéros d'appelants. Dans une option, l'algorithme modélise de manière combinée (reconnaissance multimodale des locuteurs) en utilisant, par exemple, la cohérence de la représentation 3D du visage avec les visèmes de la parole prononcée.

[0088] Alternativement, ou en addition, l'étape i peut aussi inclure une classification de l'appelant parmi des groupes d'appelants prédéterminés. Cette classification peut se baser par exemple sur des modèles de groupes d'appelants prédéterminés. Dans un mode de réalisation, au moins un premier modèle est établi pour modéliser les appelants indésirables et au moins un deuxième modèle est établi pour modéliser les appelants acceptés. La classification peut alors impliquer un calcul de la distance entre le modèle d'appelant déterminé au cours de l'étape h et ces deux modèles d'appelants prédéterminés, afin de classer le nouvel appelant dans l'une ou l'autre classe.

[0089] La classification peut aussi impliquer une classification dans un groupe d'inconnus, c'est-à-dire un groupe réunissant tous les locuteurs en dehors du set de N identifiants des appelants connus par le système.

[0090] Des technologies d'apprentissages automatiques Machine Learning connues peuvent être utilisées pour cette classification (GMM, Bayesian network, Support Vector Machine), en utilisant aussi bien des paramètres biométriques que textuels/sémantiques.

[0091] Des algorithmes de modélisation biométrique indépendants du texte prononcé et qui ne permettent pas de connaître le contenu du texte peuvent aussi être utilisés, par exemple dans une approche respectueuse de la vie privée et afin d'éviter une analyse du contenu des conversations. Les approches dépendantes du texte et impliquant une conversion voix en texte ont cependant en général une fiabilité supérieure.

[0092] Des données associées à l'appelant préalablement identifié peuvent être vérifiées au cours de l'étape j optionnelle. Par exemple, des données associées à cet appelant et stockées dans le dispositif 1, dans le serveur 5 ou dans des bases de données ou des sites web externes peuvent être exploitées. Dans un mode de réalisation, des données relatives à cet appelant sont extraites d'annuaires ou de réseaux sociaux et peuvent être utilisées pour attribuer au cours de l'étape l un score à cet appelant.

[0093] Au cours de l'étape k optionnelle, des données associées à l'appelé peuvent être vérifiées, par exemple des données introduites à cet effet par l'appelé lui-même dans le dispositif 1, dans le serveur 5, dans un site web dédié, sur un site de réseau social, un site de chat, etc. Ces données peuvent par exemple inclure des listes d'appelés refusés, des caractéristiques d'appelés refusés (par exemple en fonction de la langue, de l'âge, du sexe, etc.), ou des points d'intérêts ou des caractéristiques de l'appelé. Il est ainsi possible de vérifier une éventuelle corrélation entre ces données propres à l'appelé et les données propres à l'appelant, ainsi que le contenu sémantique des paroles parlées par l'appelant.

[0094] Au cours de l'étape l, (optionnelle), un score est attribué à l'appelant en fonction des résultats des étapes f à k. Ce score est lié à la probabilité que l'appelant soit indésirable pour l'appelé 2 donné. Il peut être combiné au score de numéro d'appel déterminé au cours de l'étape c afin de calculer un score combiné.

[0095] Si le score est inférieur à un troisième seuil donné, l'appel entrant est bloqué (étape m) ; en option, un message vocal préenregistré ou généré synthétiquement peut être restitué à l'appelant 3 pour lui indiquer que l'appel est refusé. Si en revanche ce score est supérieur à un quatrième seuil donné (supérieur au premier seuil), l'appel est transmis au dispositif terminal 2 (étape n) qui se met à sonner (ou à vibrer), afin que l'appelé puisse répondre.

[0096] Lorsque l'appel est établi au cours de l'étape n, l'appelant et l'appelé peuvent converser normalement. L'appelé peut cependant signaler en tout temps, au cours de l'étape o, que l'appelant est indésirable, par exemple en appuyant sur un bouton sur le module 1, par une commande vocale, etc. Dans ce cas, l'appel est interrompu et le numéro d'appelant, ainsi que la signature vocale ou biométrique de l'appelant, sont enregistrées comme indésirables dans la liste noire personnelle de l'appelé.

[0097] Au cours du dialogue entre l'appelant et l'appelé, l'analyse vocale et sémantique des paroles de l'appelant se poursuit (étapes f à l), et le score est recalculé en permanence ; la conversation peut ainsi être interrompue automatiquement par le système 1, 5 si ce score descend au-dessous d'une valeur donnée. Dans une variante, le système de filtrage propose seulement à l'appelé d'interrompre la conversation, par exemple au moyen d'un message visuel affiché sur un smartphone ou sur un écran du module 1, ou d'un message vocal restitué. La décision d'interrompre la conversation, ou de proposer une telle interruption, peut aussi dépendre d'une analyse des émotions dans la voix de l'appelant et/ou de l'appelé, et d'une analyse sémantique du dialogue.

[0098] Cette analyse à la volée, au cours de la conversation, permet aussi d'améliorer le modèle vocal et sémantique des appelants.

[0099] Dans le cas où le dispositif terminal 2 est constitué par un smartphone, une tablette ou un ordinateur, la confiance que le système place dans l'appel ou dans l'authenticité de la conversation peut être visualisée en permanence sur l'écran ou en faisant appels aux fonctionnalités du système utilisé (vibreur, notification sonore, ...)

[0100] Dans le cas d'une communication asymétrique smartphone vers téléphone, les paramètres biométriques de l'appelant peuvent tout de même inclure la modélisation visuelle de l'appelant effectuée sur le smartphone. Les paramètres sont alors transmis par une autre connexion réseau vers le système de filtrage 1, 5.

[0101] Le système offre en outre l'avantage de sauvegarder les données biométriques de l'appelant, par exemple son empreinte vocale et/ou faciale. Les auteurs d'appels criminels ou indésirables laissant leurs traces biométriques derrière eux, ces données peuvent être partagées avec les autres membres de la communauté d'utilisateurs du système, ou avec la police. Le système biométrique peut ainsi bénéficier et modéliser ces personnes.

[0102] Nous allons maintenant décrire un exemple de dialogue dans un système selon l'invention. Le système fait appel à un dispositif qui se présente sous le nom de Katia. Dans ce scénario, l'appelant 3 est Alice et l'appelé 2 est Bob.

[0103] Dans cet exemple, le dialogue est initié par Alice qui compose le numéro de l'appelé Bob. Bob a installé un boîtier de filtrage „Katia“ 1 entre son terminal 2 et le réseau téléphonique 4, qui intercepte cet appel entrant. Alternativement, Bob a installé une application dans son smartphone qui intercepte cet appel entrant.

[0104] Le système 1, 5 détecte que le score associé au numéro est inférieur au premier seuil de confiance. Dans ce cas, le système décroche l'appel à la place de Bob et procède à un contrôle d'accès non transparent pour l'appelant. Plus précisément, le boîtier 1 décroche avec le message suivant: Votre numéro n'est pas reconnu par Katia, la suite de la conversation sera enregistrée, si vous ne désirez pas être enregistré raccrochez maintenant. Katia vous écoute !

[0105] Un tel message a souvent déjà pour effet de dissuader les appelants indésirables ou criminels s'ils apprennent que leur appel est enregistré.

[0106] Alice répond avec la phrase : Bonjour Katia, je t'appelle depuis New York. J'ai besoin de l'aide de Bob, peux-tu me le passer ?

[0107] Le système 1, 5 reconnaît Alice grâce à l'empreinte vocale stockée et aussi grâce à l'empreinte sémantique créée par la page Facebook où Alice avait décrit son voyage à New York. Avec un résultat favorable du calcul de probabilité (score du numéro d'appel combiné avec les probabilités qui résultent de la vérification des empreintes), le système accorde l'accès et fait sonner le téléphone de Bob. Une musique d'attente est restituée à Alice en attendant que Bob réponde.

[0108] L'accès est ensuite accordé par Bob qui décroche. Dans un mode de réalisation préférentiel, Bob a écouté le message d'Alice qui lui est restitué, ce qui permet un filtrage manuel par Bob. Bob peut communiquer au dispositif 1 sa décision de prendre l'appel par exemple avec une commande vocale du type „Katia, je prends l'appel“. La communication est alors établie entre Alice et Bob.

[0109] Alice parle alors à Bob. Dans cet exemple, elle demande „Bonjour Bob, peux-tu m'envoyer de l'argent sur mon compte ? C'est urgent !“. Le système 1, 5 enregistre la conversation et segmente le discours de chaque locuteur. L'empreinte sémantique d'Alice est analysée en continu pour vérifier le spam. Bob répond et la conversation se poursuit.

[0110] Alice termine ensuite son appel. Le système de filtrage 1, 5 met à jour les modèles vocaux, biométriques et sémantiques de l'appelant Alice.

[0111] Un support de données informatique tangible contient un programme qui peut être exécuté par un système informatique 1, 5 pour exécuter tout ou partie du procédé ci-dessus.

Revendications

1. Procédé de filtrage d'appels téléphoniques entrants indésirables, dans lequel une décision de bloquer un appel ou de le transmettre est basée à la fois sur le numéro d'appelant et sur une analyse de la voix de l'appelant, le procédé comportant les étapes suivantes :
 - a) détermination du numéro d'appelant;
 - b) en fonction du numéro d'appelant, un dispositif de filtrage (1, 5) décide soit de transmettre l'appel, soit de rejeter l'appel, soit d'inviter l'appelant à parler;
 - c) lorsque l'appelant est invité à parler, il parle sans que son message vocal ne soit restitué à l'appelé ;
 - d) le système de filtrage analyse la voix de l'appelant, et
 - e) le système de filtrage décide en fonction de cette analyse si l'appel doit être transmis à l'appelé, ou s'il doit être bloqué.
2. Procédé selon la revendication 1, dans lequel une décision de bloquer un appel ou de le transmettre est basée à la fois sur le numéro d'appelant, sur l'analyse la voix de l'appelant et sur une analyse du visage de l'appelant.
3. Procédé selon la revendication 1 ou 2, dans lequel le système de filtrage continue d'analyser la voix de l'appelant après que l'appel ait été transmis à l'appelé, et bloque l'appel ou propose de le bloquer lorsque cette analyse révèle que l'appel est indésirable.
4. Procédé selon l'une des revendications précédentes, comprenant en outre une étape succédant l'étape a) et précédant l'étape b) et au cours de laquelle un score de confiance est attribué en fonction du numéro d'appelant, la décision de rejeter l'appel ou d'inviter l'appelant à parler étant prise au cours de l'étape b) lorsque ce score est en-dessous d'un seuil prédéterminé.
5. Procédé selon la revendication 4, dans lequel ledit score de confiance attribué à un appelant est déterminé indépendamment pour chaque appelé.
6. Procédé selon l'une des revendications 4 et 5, dans lequel ledit score de confiance, ou un autre score de confiance, est attribué à chaque appelant en fonction de ladite analyse de voix.
7. Procédé selon l'une des revendications 4 à 6, dans lequel ladite décision de rejeter l'appel ou d'inviter l'appelant à parler dépend de l'historique des appels effectués avec ledit numéro d'appelant vers d'autres appelés.

8. Procédé selon l'une des revendications 4 à 7, comprenant en outre une étape d'identification dudit appelant grâce à ladite analyse vocale succédant à l'étape d) et précédant l'étape e), le score de confiance dépendant de l'historique des appels effectués par ledit appelant ainsi identifié vers d'autres appelés.
9. Procédé selon l'une des revendications 4 à 8, comprenant en outre une étape d'authentification dudit appelant grâce à ladite analyse vocale et de vérification que ladite authentification corresponde au numéro d'appelant,
10. Procédé selon l'une des revendications 4 à 9, comprenant en outre une étape de vérification de données relatives à l'appelant et/ou à l'appelé dans un réseau social, ladite décision de rejeter l'appel ou d'inviter l'appelant à parler dépendant de ces données.
11. Procédé selon l'une des revendications précédentes, comprenant en outre une étape au cours de laquelle l'appelé signale un appel indésirable, cette indication étant ensuite utilisée dans la décision de rejeter les futurs appels de l'appelant vers d'autres appelés, ou d'inviter cet appelant à parler.
12. Procédé selon l'une des revendications précédentes, comprenant une étape (g) d'analyse sémantique de la conversation, la décision de transmettre un appel ou la décision de bloquer un appel dépendant de cette analyse sémantique.
13. Procédé selon la revendication 12, la décision de transmettre un appel ou la décision de bloquer un appel en fonction de l'analyse sémantique dépendant de chaque appelé.
14. Procédé selon l'une des revendications précédentes, dans lequel ladite décision de transmettre l'appel, de rejeter l'appel, ou d'inviter l'appelant à parler est basée sur un procédé de machine learning.
15. Procédé selon l'une des revendications précédentes, dans lequel ledit système de filtrage (1) effectue une analyse de plausibilité du numéro d'appelant et tient compte de cette analyse de plausibilité dans sa décision soit de transmettre l'appel, soit de rejeter l'appel, soit d'inviter l'appelant à parler.
16. Système de filtrage d'appels téléphoniques entrants indésirables adapté pour exécuter le procédé selon l'une des revendications précédentes, le système de filtrage comportant :
 - un module de détermination du numéro d'appelant ;
 - un dispositif de filtrage (1, 5) apte à décider, en fonction du numéro d'appelant, si l'appel doit être transmis, rejeté, ou si l'appelant doit être invité à parler;
 - un module d'analyse pour l'analyse de la voix de l'appelant;
 - le dispositif de filtrage étant en outre agencé pour décider en fonction de cette analyse si l'appel doit être transmis à l'appelé, ou s'il doit être bloqué.

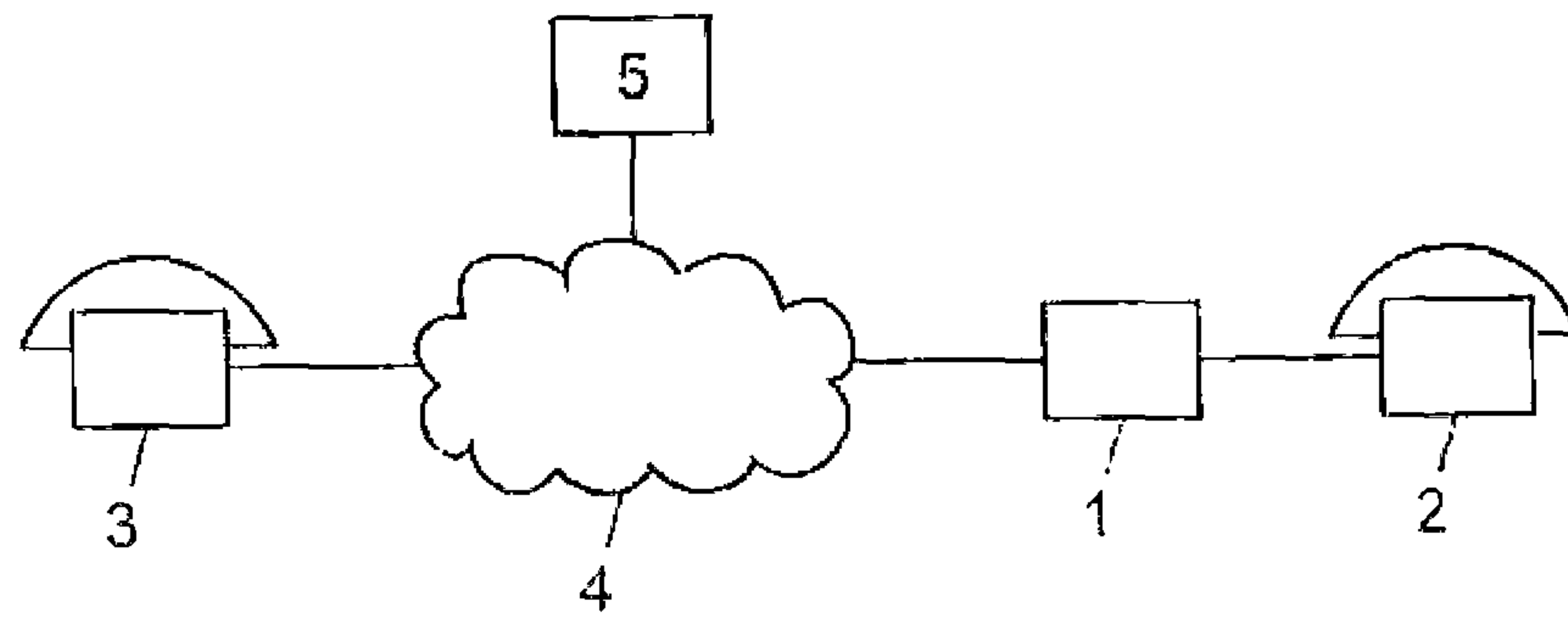


Fig.1

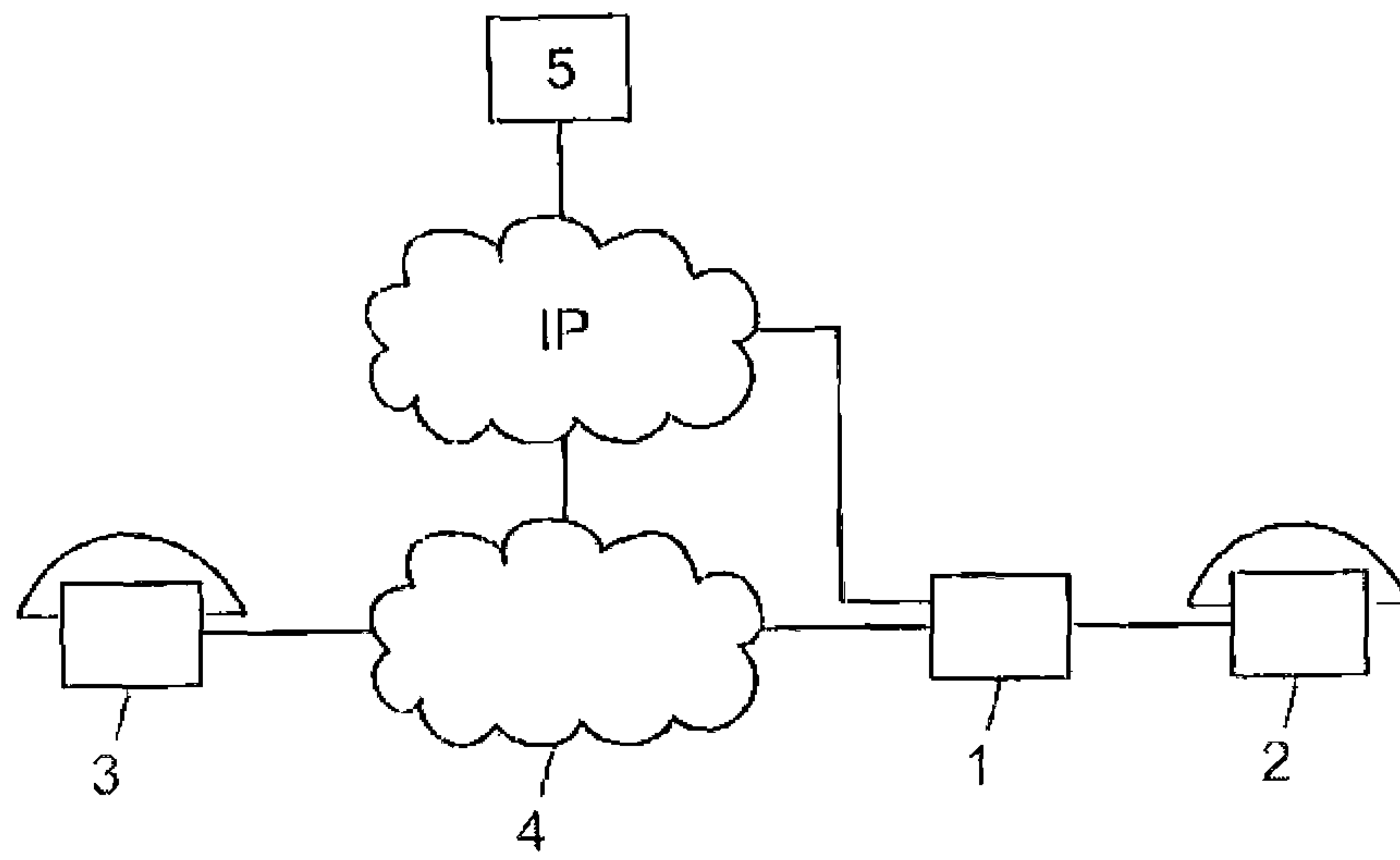


Fig.2

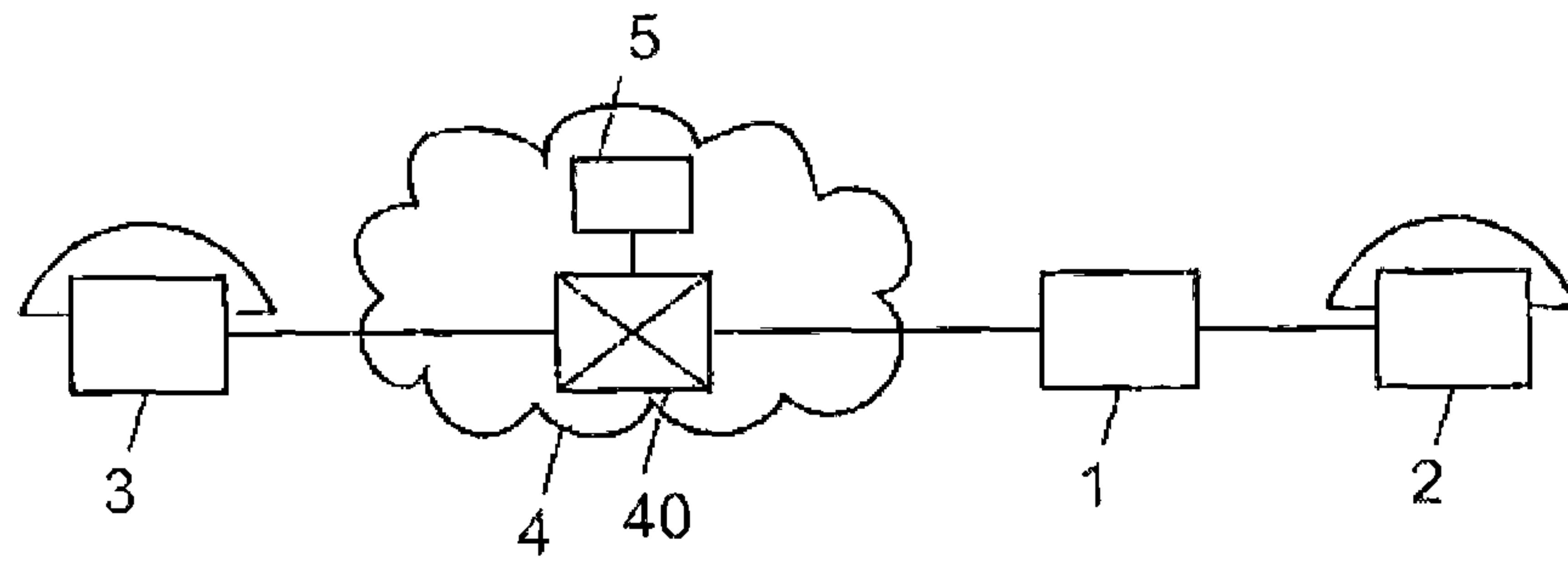


Fig.3

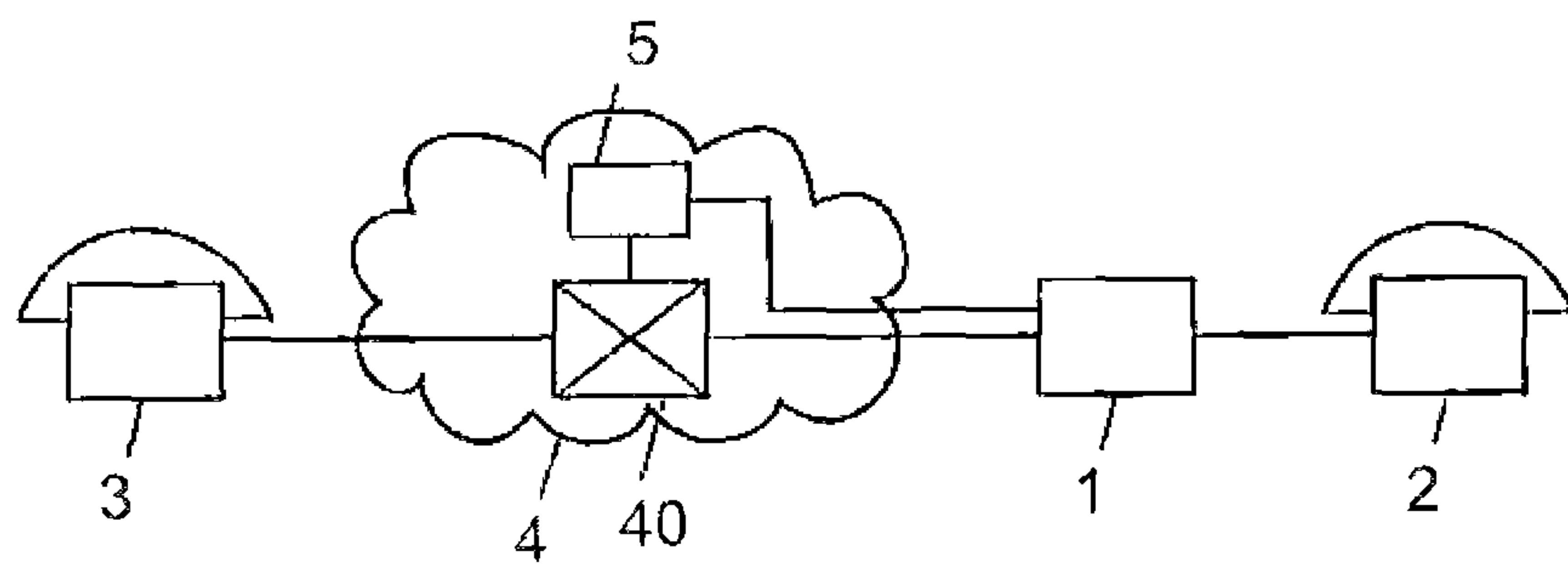


Fig.4

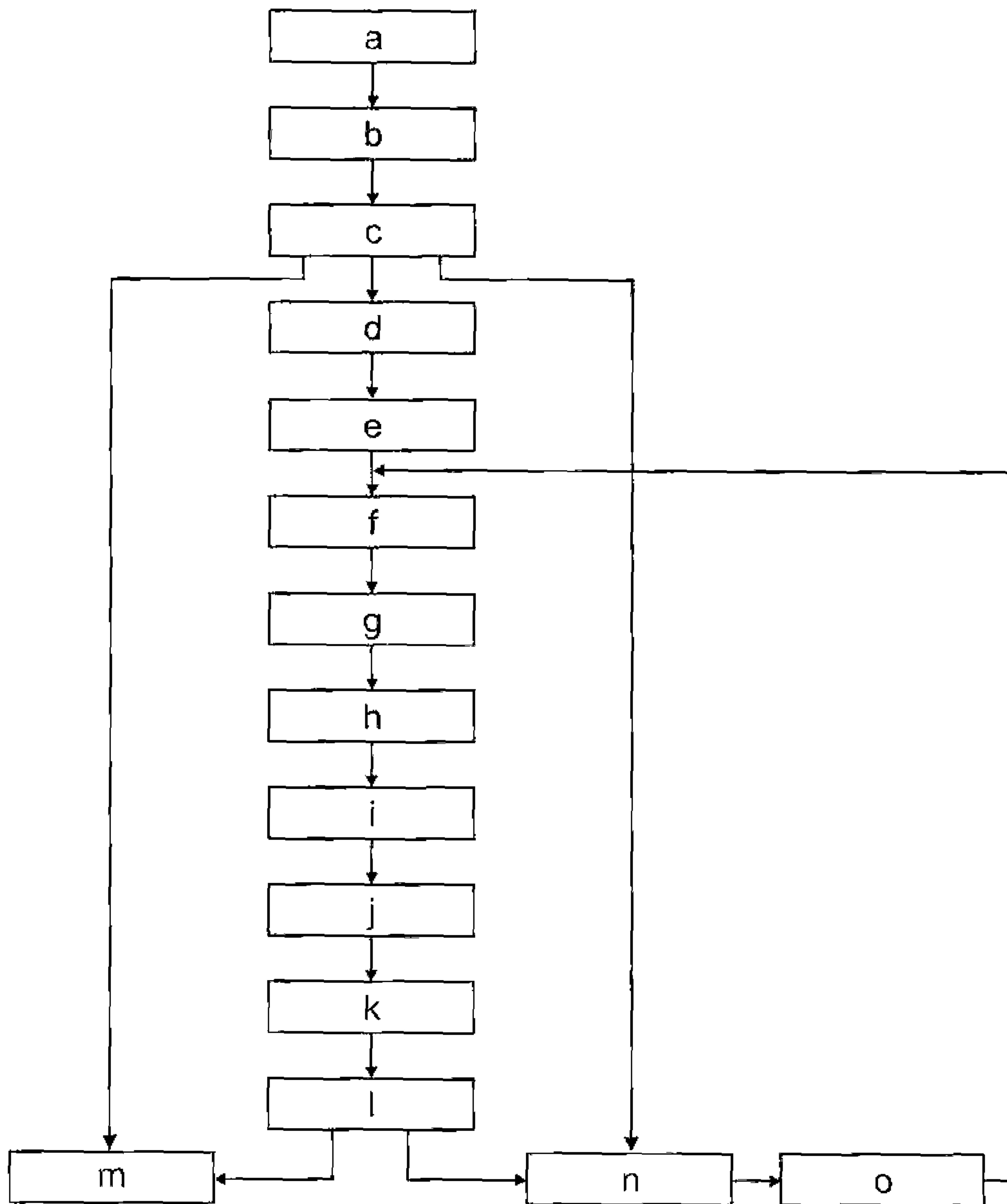


Fig.5